Google Cloud Platform: PCI DSS v3.2.1 Shared Responsibility Matrix

December 2021

Introduction

Google Cloud Platform (GCP) was designed with security as a core design component. Google uses a variety of technologies and processes to secure information stored on Google servers. Google has performed independent validation on Payment Card Industry Data Security Standard (PCI DSS) requirements that apply to GCP technologies and infrastructure managed by Google. Google offers customers a great deal of control over their instances running on Google's infrastructure. Google does not control security on the operating system, packages or applications that are deployed by customers on GCP. It is the customer's responsibility to comply with the requirements of PCI DSS that relate to operating systems packages and applications deployed by customer, or to customer's configurations in multi-cloud or hybrid cloud models outside the GCP boundary. GCP adheres to the PCI DSS requirements set forth for a level 1 Service Provider. This document outlines each requirement that Google complies with on behalf of customers that use GCP to deliver PCI-compliant products and services. If a requirement is not included in this document, that indicates that GCP is not performing the requirement on behalf of its clients. With respect to the cloud hosting services which GCP delivers to its customers, responsibility for the various requirements associated with PCI DSS varies. Some requirements are the sole responsibility of GCP, some requirements are the sole responsibility of the customer, and some requirements are a shared responsibility between both parties. GCP's support for PCI DSS does not apply to customer's activities outside the GCP boundary. We recommend that customers reference the responsibility matrix in this document as they pursue PCI compliance and find it a useful tool when conducting their own PCI audits.

Definitions

Term	Description
Google	The service provider
Google Cloud Platform (GCP) responsibility	**The requirement in question is the responsibility of, and implemented by, Google.** A Qualified Security Assessor has assessed and validated these requirements and found GCP to be compliant with PCI-DSS v3.2.1. These requirements, which support the Customer's PCI-DSS efforts but the Customer cannot manage directly, are the sole responsibility of GCP
Customer responsibility	**The requirement in question is the responsibility of, and implemented by, the customer.** These requirements were not applicable to Google Cloud services as they are designed and these are the customer responsibilities. Customers of GCP bear sole responsibility to meet their own PCI DSS compliance for these requirements.
Shared responsibility	**Both the customer and Google are responsible for implementing parts of the requirement.** A Qualified Security Assessor has assessed and validated these specific requirements and found GCP to be compliant with PCI-DSS v3.2.1. However, Customers of GCP share some responsibility and must take action in order to meet their own PCI DSS compliance for these requirements.
Service Provider	The Service Provider, as defined by the requirement, is Google
POS	Point of Sale
PCI DSS	Payment Card Industry Data Security Standard

			Customers Responsibility Summary				
PCI DSS v3.2.1 Requirements	**GCP**	**Customer**	**Compute** App Engine Bare Metal Compute Engine Cloud Run Preemptible VMs Shielded VMs	**Networking** Cloud Armor Cloud NAT Hybrid Connectivity Network Intelligence Center Network Telemetry Service Directory Traffic Director Virtual Private Cloud (VPC)	**Storage** Archive Storage Cloud Storage Filestore Local SSD Persistent Disk	**Security** Access Transparency Assured Workloads Binary Authorization Chronicle Cloud Asset Inventory Cloud Data Loss Prevention Cloud Key Management Firewalls Secret Manager Security Command Center Shielded VMs VPC Service Controls **Identity and Access** Cloud Identity Identity and Access Management Identity-Aware Proxy Identity Platform Managed Service for Microsoft Active Directory Policy Intelligence Resource Manager Titan Security Key	**Google Responsibility Summary**
Requirement 1: Install and maintain a firewall configuration to protect cardholder data							
1.1 Establish and implement firewall and router configuration standards that include the following:	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 and GCE.	Customers are responsible for formalizing change control processes around approval and testing of network connections, i.e. GCP firewall rules that impact their VPC and GCE.	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 and GCE.	Google's internal production network and systems have been assessed against and comply with this requirement.
1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations.	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 and GCE.	Customers are responsible for formalizing change control processes around approval and testing of network connections, i.e. GCP firewall rules that impact their VPC and GCE.	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 and GCE.	Google's internal production network and systems have been assessed against and comply with this requirement.
1.1.2 Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks**.**		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 are responsible for maintaining their own network diagrams specific to their CDE that identify all connections between their CDE and any other networks.	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.	Not Applicable
1.1.3 Current diagram that shows all cardholder data flows across systems and networks.		x	Customers are responsible for maintaining their own dataflow diagrams specific to their CDE.	Customers are responsible for maintaining their own dataflow diagrams specific to their CDE.	Not Applicable	Customers are responsible for maintaining their own dataflow diagrams specific to their CDE.	Not Applicable

1.1.4 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone.	x	x	GCP customers implementing GCE are responsible for implementing perimeter firewalls and configuring security groups and ACLs through any API's and other user interfaces for their in-scope services. GCP customers are responsible for developing appropriate firewall rules or using additional firewall technologies to develop appropriate DMZ and internal networks. GCP customers are responsible for reviewing the connectivity models and exposure of their GCE instances to these data stores, for ensuring that appropriate zones are created, and that access mechanisms to the data stores that have cardholder data are not directly exposed to the Internet.	GCP customers implementing GCE are responsible for implementing perimeter firewalls and configuring security groups and ACLs through any API's and other user interfaces for their in-scope services. GCP customers are responsible for developing appropriate firewall rules or using additional firewall technologies to develop appropriate DMZ and internal networks. GCP customers are responsible for reviewing the connectivity models and exposure of their GCE instances to these data stores, for ensuring that appropriate zones are created, and that access mechanisms to the data stores that have cardholder data are not directly exposed to the Internet.	Not Applicable	GCP customers implementing GCE are responsible for implementing perimeter firewalls and configuring security groups and ACLs through any API's and other user interfaces for their in-scope services. GCP customers are responsible for developing appropriate firewall rules or using additional firewall technologies to develop appropriate DMZ and internal networks. GCP customers are responsible for reviewing the connectivity models and exposure of their GCE instances to these data stores, for ensuring that appropriate zones are created, and that access mechanisms to the data stores that have cardholder data are not directly exposed to the Internet.	Firewalls that comply with this requirement have been implemented by Google to control access to the Google production network and to GCP products and services implemented by Google.
1.1.5 Description of groups, roles, and responsibilities for management of network components.	x	x	Customers are responsible for defining responsibilities for management of GCP firewall rules and any other network configurations.	Customers are responsible for defining responsibilities for management of GCP firewall rules and any other network configurations.	Not Applicable	Customers are responsible for defining responsibilities for management of GCP firewall rules and any other network configurations.	Google's internal production network and systems have been assessed against and comply with this requirement.
1.1.6 Documentation of business justification and approval for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.	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.
1.1.7 Requirement to review firewall and router rule sets at least every six months.	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 GCE and GCS, and GCP 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 GCE and GCS, and GCP 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 GCE and GCS, and GCP 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 Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.	x	x	Customers are responsible for implementing firewall rules and limiting ingress and egress traffic to defined ports and protocols necessary for GCE instances and denying all other traffic.	Customers are responsible for implementing firewall rules and limiting ingress and egress 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 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 GCP GCE and GCS, and GCP VPCs. Customers are responsible for denying any traffic that is not explicitly required for the GCP Product to function.	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.
1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	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 GCP GCE and GCS, and GCP VPCs. 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 GCP GCE and GCS, and GCP VPCs. 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 GCP GCE and GCS, and GCP VPCs. Customers are responsible for denying any traffic that is not explicitly required for the GCP Product to function.	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.
1.2.2 Secure and synchronize router configuration files.	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.
1.2.3 Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.	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.
1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.	x	x	Customers are responsible for implementing firewall rules and limiting ingress traffic to defined ports and protocols necessary for GCE instances within their DMZ.	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.	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.

1.3.1 Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	x	x	Customers are responsible for implementing firewall rules and limiting ingress traffic to defined ports and protocols necessary for GCE instances within their DMZ.	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.	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.
1.3.2 Limit inbound Internet traffic to IP addresses within the DMZ.	x	x	Customers are responsible for implementing firewall rules and limiting ingress traffic to defined ports and protocols necessary for GCE instances within their DMZ.	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.	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.
1.3.3 Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network.	x		Not Applicable	Not Applicable	Not Applicable	Not Applicable	GCP firewalls perform anti-spoofing by default. As such, customers can rely on the GCP AOC for compliance with anti-spoofing controls.
1.3.4 Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.	x	x	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.	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.	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.	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.
1.3.5 Permit only “established” connections into the network.	x		Not Applicable	Not Applicable	Not Applicable	Not Applicable	GCP firewalls perform stateful packet inspection by default and customers can rely on the GCP AOC for compliance with stateful packet inspection controls.
1.3.6 Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.		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.	Not Applicable	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
1.3.7 Do not disclose private IP addresses and routing information to unauthorized parties.	x	x	Customers are responsible for developing appropriate configuration on GCP GCE to prevent the disclosure of IP Addresses and routing information.	Customers are responsible for developing appropriate configuration on GCP GCE to prevent the disclosure of IP Addresses and routing information.	Not Applicable	Customers are responsible for developing appropriate configuration on GCP GCE 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.

1.4 Install personal firewall software or equivalent functionality on any portable computing devices (including company and/or employee-owned) that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the CDE.		x	Customers are responsible for implementing personal firewall rules for systems with direct connectivity to the Internet for systems used to manage the CDE within GCP.	Customers are responsible for implementing personal firewall rules for systems with direct connectivity to the Internet for systems used to manage the CDE 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 the CDE within GCP.	Not Applicable
1.5 Ensure that security policies and operational procedures for managing firewalls are documented, in use, and known to all affected parties.		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

			Customers Responsibility Summary				
PCI DSS v3.2.1 Requirements	**GCP**	**Customer**	**Compute** App Engine Bare Metal Compute Engine Cloud Run Preemptible VMs Shielded VMs	**Networking** Cloud Armor Cloud NAT Hybrid Connectivity Network Intelligence Center Network Telemetry Service Directory Traffic Director Virtual Private Cloud (VPC)	**Storage** Archive Storage Cloud Storage Filestore Local SSD Persistent Disk	**Security** Access Transparency Assured Workloads Binary Authorization Chronicle Cloud Asset Inventory Cloud Data Loss Prevention Cloud Key Management Firewalls Secret Manager Security Command Center Shielded VMs VPC Service Controls **Identity and Access** Cloud Identity Identity and Access Management Identity-Aware Proxy Identity Platform Managed Service for Microsoft Active Directory Policy Intelligence Resource Manager Titan Security Key	**Google Responsibility Summary**
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.							
2.1 Always change vendor-supplied defaults and remove or disable unnecessary default accounts **before** installing a system on the network.	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.
2.1.1 For wireless environments connected to the cardholder data environment or transmitting cardholder data, change ALL wireless vendor defaults at installation, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.		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 Cardholder Data Environment relating to GCP.
2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. *Sources of industry-accepted system hardening standards may include, but are not limited to:* *• Center for Internet Security (CIS)* *• International Organization for Standardization (ISO)* *• SysAdmin Audit Network Security (SANS) Institute* *• National Institute of Standards Technology (NIST).*	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 GCE, VPC, and GCS based on industry standards and hardening guidelines.	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 GCE, VPC, and GCS based on industry standards and hardening guidelines.	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 GCE, VPC, and GCS based on industry standards and hardening guidelines.	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 GCE, VPC, and GCS based on industry standards and hardening guidelines.	Google has implemented configuration standards for the infrastructure underlying GCP products in scope that comply with this PCI DSS requirement .

2.2.1 Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.) ***Note:*** *Where virtualization technologies are in use, implement only one primary function per virtual system component.*	x	x	Customers are responsible for ensuring that only one primary function is implemented per customer-managed GCP products.	Customers are responsible for ensuring that only one primary function is implemented per customer-managed GCP products.	Not Applicable	Customers are responsible for ensuring that only one primary function is implemented per customer-managed GCP products.	Google has implemented configuration standards for the infrastructure underlying GCP products in scope that comply with this PCI DSS requirement .
2.2.2 Enable only necessary services, protocols, daemons, etc., as required for the function of the system.	x	x	GCP 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.	GCP 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.	GCP 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.	GCP 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 .
2.2.3 Implement additional security features for any required services, protocols, or daemons that are considered to be insecure.		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. The GCP product does not implement services, protocols or daemons deemed insecure.
2.2.4 Configure system security parameters to prevent misuse.	x	x	GCP 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.	GCP 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.	GCP 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.	GCP 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 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.	x	x	GCP 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.	GCP 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.	GCP 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.	GCP 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 .
2.3 Encrypt all non-console administrative access using strong cryptography.	x	x	GCP customers are 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.	GCP customers are 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.	GCP customers are 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.	GCP customers are 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.
2.4 Maintain an inventory of system components that are in scope for PCI DSS.		x	Customers are responsible for maintaining an inventory of GCP GCE instances that are in scope for their compliance.	Customers are responsible for maintaining an inventory of GCP GCE instances that are in scope for their compliance.	Customers are responsible for maintaining an inventory of GCP GCE instances that are in scope for their compliance.	Customers are responsible for maintaining an inventory of GCP GCE instances that are in scope for their compliance.	Not Applicable
2.5 Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties.		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

2.6 Shared hosting providers must protect each entity's hosted environment and cardholder data. These providers must meet specific requirements as detailed in Appendix A1: Additional PCI DSS Requirements for Shared Hosting Providers.		x	Customers may also be considered a shared hosting provider, if they run applications or store data for their customers. In this case, customers are responsible for protecting their customer's data within GCP services.	Customers may also be considered a shared hosting provider, if they run applications or store data for their customers. In this case, customers are responsible for protecting their customer's data within GCP services.	Customers may also be considered a shared hosting provider, if they run applications or store data for their customers. In this case, customers are responsible for protecting their customer's data within GCP services.	Customers may also be considered a shared hosting provider, if they run applications or store data for their customers. In this case, customers are responsible for protecting their customer's data within GCP services.	Not Applicable

			Customers Responsibility Summary				
PCI DSS v3.2.1 Requirements	**GCP**	**Customer**	**Compute** App Engine Bare Metal Compute Engine Cloud Run Preemptible VMs Shielded VMs	**Networking** Cloud Armor Cloud NAT Hybrid Connectivity Network Intelligence Center Network Telemetry Service Directory Traffic Director Virtual Private Cloud (VPC)	**Storage** Archive Storage Cloud Storage Filestore Local SSD Persistent Disk	**Security** Access Transparency Assured Workloads Binary Authorization Chronicle Cloud Asset Inventory Cloud Data Loss Prevention Cloud Key Management Firewalls Secret Manager Security Command Center Shielded VMs VPC Service Controls **Identity and Access** Cloud Identity Identity and Access Management Identity-Aware Proxy Identity Platform Managed Service for Microsoft Active Directory Policy Intelligence Resource Manager Titan Security Key	**Google Responsibility Summary**
Requirement 3: Protect stored cardholder data.							
3.1 Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all cardholder data (CHD) storage: • Limiting data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements • Specific retention requirements for cardholder data • Processes for secure deletion of data when no longer needed • A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention.		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.	Not Applicable
3.2 Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process.		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.	Not Applicable

3.2.1 Do not store the full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere) after authorization. This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data. *Note: In the normal course of business, the following data elements from the magnetic stripe may need to be retained:* *• The cardholder's name* *• Primary account number (PAN)* *• Expiration date* *• Service code* *To minimize risk, store only these data elements as needed for business.*		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.	Not Applicable
3.2.2 Do not store the card verification code or value (three-digit or four-digit number printed on the front or back of a payment card used to verify card-not-present transactions) after authorization.		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.	Not Applicable
3.2.3 Do not store the personal identification number (PIN) or the encrypted PIN block after authorization.		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.	Not Applicable
3.3 Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see more than the first six/last four digits of the PAN. *Note: This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, legal or payment card brand requirements for point-of-sale (POS) receipts.*		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.	Not Applicable
3.4 Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: • One-way hashes based on strong cryptography, (hash must be of the entire PAN) • Truncation (hashing cannot be used to replace the truncated segment of PAN) • Index tokens and pads (pads must be securely stored) • Strong cryptography with associated key-management processes and procedures. *Note: It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN. Where hashed and truncated versions of the same PAN are present in an entity's environment, additional controls must be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN.*		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 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts. *Note: This requirement applies in addition to all other PCI DSS encryption and key-management requirements.*		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
3.5 Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse.	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.
3.5.1 *Additional requirement for service providers only:* Maintain a documented description of the cryptographic architecture that includes: • Details of all algorithms, protocols, and keys used for the protection of cardholder data, including key strength and expiry date • Description of the key usage for each key. • Inventory of any HSMs and other SCDs used for key management	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.
3.5.2 Restrict access to cryptographic keys to the fewest number of custodians necessary.	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.

3.5.3 Store secret and private keys used to encrypt/decrypt cardholder data in one (or more) of the following forms at all times: • Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key • Within a secure cryptographic device (such as a hardware (host) security module (HSM) or PTS-approved point-of-interaction device) • As at least two full-length key components or key shares, in accordance with an industry-accepted method *Note: It is not required that public keys be stored in one of these forms.*	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.
3.5.4 Store cryptographic keys in the fewest possible locations.	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 Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following:	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.
3.6.1 Generation of strong cryptographic keys	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.

3.6.2 Secure cryptographic key distribution	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.
3.6.3 Secure cryptographic key storage	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.
3.6.4 Cryptographic key changes for keys that have reached the end of their cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57).	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.
3.6.5 Retirement or replacement (for example, archiving, destruction, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key component), or keys are suspected of being compromised. *Note: If retired or replaced cryptographic keys need to be retained, these keys must be securely archived (for example, by using a key-encryption key). Archived cryptographic keys should only be used for decryption/verification purposes.*	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.
3.6.6 If manual clear-text cryptographic key-management operations are used, these operations must be managed using split knowledge and dual control.		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	Google does not use clear text cryptographic key management. This is a customer responsibility.

						creation, usage, and management of customer encryption keys in accordance with PCI DSS controls for these GCP Products.	
3.6.7 Prevention of unauthorized substitution of cryptographic keys.	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.
3.6.8 Requirement for cryptographic key custodians to formally acknowledge that they understand and accept their key-custodian responsibilities.		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 Ensure that security policies and operational procedures for protecting stored cardholder data are documented, in use, and known to all affected parties.		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

			Customers Responsibility Summary				
PCI DSS v3.2.1 Requirements	**GCP**	**Customer**	**Compute** App Engine Bare Metal Compute Engine Cloud Run Preemptible VMs Shielded VMs	**Networking** Cloud Armor Cloud NAT Hybrid Connectivity Network Intelligence Center Network Telemetry Service Directory Traffic Director Virtual Private Cloud (VPC)	**Storage** Archive Storage Cloud Storage Filestore Local SSD Persistent Disk	**Security** Access Transparency Assured Workloads Binary Authorization Chronicle Cloud Asset Inventory Cloud Data Loss Prevention Cloud Key Management Firewalls Secret Manager Security Command Center Shielded VMs VPC Service Controls **Identity and Access** Cloud Identity Identity and Access Management Identity-Aware Proxy Identity Platform Managed Service for Microsoft Active Directory Policy Intelligence Resource Manager Titan Security Key	**Google Responsibility Summary**
Requirement 4: Encrypt transmission of cardholder data across open, public networks.							
4.1 Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: • Only trusted keys and certificates are accepted. • The protocol in use only supports secure versions or configurations. • The encryption strength is appropriate for the encryption methodology in use. *Examples of open, public networks include but are not limited to:* *• The Internet* *• Wireless technologies, including 802.11 and Bluetooth* *• Cellular technologies, for example, Global System for Mobile communications (GSM), Code division multiple access (CDMA)* *• General Packet Radio Service (GPRS).* *• Satellite communications.*	x	x	GCP 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 using web browsers and client endpoints that do not support TLS1.0 or ciphers that are weaker than AES128.	GCP 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 using web browsers and client endpoints that do not support TLS1.0 or ciphers that are weaker than AES128.	GCP 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 using web browsers and client endpoints that do not support TLS1.0 or ciphers that are weaker than AES128.	GCP 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 using web browsers and client endpoints that do not support TLS1.0 or ciphers that are weaker than AES128.	Google has implemented configuration standards that comply with requirements in section 4.1 for the infrastructure underlying GCP products in scope for PCI.
4.1.1 Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices to implement strong encryption for authentication and transmission.		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. Any transmission of Cardholder Data over wireless networks is Customer responsibility.

4.2 Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, SMS, chat, etc.).	x	x	GCP customers are responsible for the use of any end-user messaging technologies for transmitting PAN.	GCP customers are responsible for the use of any end-user messaging technologies for transmitting PAN.	GCP customers are responsible for the use of any end-user messaging technologies for transmitting PAN.	GCP customers are responsible for the use of any end-user messaging technologies for transmitting PAN.	Google has implemented configuration standards that comply with requirements in section 4.2 for the infrastructure underlying GCP products in scope for PCI.
4.3 Ensure that security policies and operational procedures for encrypting transmissions of cardholder data are documented, in use, and known to all affected parties.		x	GCP customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	GCP customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	GCP customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	GCP customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	Not Applicable.

			Customers Responsibility Summary				
PCI DSS v3.2.1 Requirements	**GCP**	**Customer**	**Compute** App Engine Bare Metal Compute Engine Cloud Run Preemptible VMs Shielded VMs	**Networking** Cloud Armor Cloud NAT Hybrid Connectivity Network Intelligence Center Network Telemetry Service Directory Traffic Director Virtual Private Cloud (VPC)	**Storage** Archive Storage Cloud Storage Filestore Local SSD Persistent Disk	**Security** Access Transparency Assured Workloads Binary Authorization Chronicle Cloud Asset Inventory Cloud Data Loss Prevention Cloud Key Management Firewalls Secret Manager Security Command Center Shielded VMs VPC Service Controls **Identity and Access** Cloud Identity Identity and Access Management Identity-Aware Proxy Identity Platform Managed Service for Microsoft Active Directory Policy Intelligence Resource Manager Titan Security Key	**Google Responsibility Summary**
Requirement 5: Use and regularly update anti-virus software or programs.							
5.1 Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).	x	x	GCP customers are responsible for managing anti-virus software or program for any customer-managed GCP GCE 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	GCP customers are responsible for managing anti-virus software or program for any customer-managed GCP GCE 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.
5.1.1 Ensure that anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.	x	x	GCP customers are responsible for managing anti-virus software or program for any customer-managed GCP GCE 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	GCP customers are responsible for managing anti-virus software or program for any customer-managed GCP GCE 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.

5.1.2 For systems considered to be not commonly affected by malicious software, perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software.	x	x	GCP customers are responsible for managing anti-virus software or program for any customer-managed GCP GCE 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	GCP customers are responsible for managing anti-virus software or program for any customer-managed GCP GCE 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 Ensure that all anti-virus mechanisms are maintained as follows: • Are kept current. • Perform periodic scans. • Generate audit logs which are retained per PCI DSS Requirement 10.7.	x	x	GCP customers are responsible for managing anti-virus software or program for any customer-managed GCP GCE 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	GCP customers are responsible for managing anti-virus software or program for any customer-managed GCP GCE 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 Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period. ***Note:*** *Anti-virus solutions may be temporarily disabled only if there is legitimate technical need, as authorized by management on a case-by-case basis. If anti-virus protection needs to be disabled for a specific purpose, it must be formally authorized. Additional security measures may also need to be implemented for the period of time during which anti-virus protection is not active.*	x	x	GCP customers are responsible for managing anti-virus software or program for any customer-managed GCP GCE instances.	Not Applicable	Not Applicable	GCP customers are responsible for managing anti-virus software or program for any customer-managed GCP GCE 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 Ensure that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties.		x	GCP customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	GCP customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	GCP customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	GCP customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	Not Applicable

			Customers Responsibility Summary				
PCI DSS v3.2.1 Requirements	**GCP**	**Customer**	**Compute** App Engine Bare Metal Compute Engine Cloud Run Preemptible VMs Shielded VMs	**Networking** Cloud Armor Cloud NAT Hybrid Connectivity Network Intelligence Center Network Telemetry Service Directory Traffic Director Virtual Private Cloud (VPC)	**Storage** Archive Storage Cloud Storage Filestore Local SSD Persistent Disk	**Security** Access Transparency Assured Workloads Binary Authorization Chronicle Cloud Asset Inventory Cloud Data Loss Prevention Cloud Key Management Firewalls Secret Manager Security Command Center Shielded VMs VPC Service Controls **Identity and Access** Cloud Identity Identity and Access Management Identity-Aware Proxy Identity Platform Managed Service for Microsoft Active Directory Policy Intelligence Resource Manager Titan Security Key	**Google Responsibility Summary**
Requirement 6: Develop and maintain secure systems and applications.							
6.1 Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as "high," "medium," or "low") to newly discovered security vulnerabilities. ***Note:*** *Risk rankings should be based on industry best practices as well as consideration of potential impact. For example, criteria for ranking vulnerabilities may include consideration of the CVSS base score, and/or the classification by the vendor, and/or type of systems affected.* *Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organization's environment and risk-assessment strategy. Risk rankings should, at a minimum, identify all vulnerabilities considered to be a "high risk" to the environment. In addition to the risk ranking, vulnerabilities may be considered "critical" if they pose an imminent threat to the environment, impact critical systems, and/or would result in a potential compromise if not addressed. Examples of critical systems may include security systems, public-facing*	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 GCE 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 VPCs.	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 GCS and in-scope 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.

devices and systems, databases, and other systems that store, process, or transmit cardholder data.							
6.2 Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release.	x	x	Customers are responsible for managing the security patches of their GCE instances and installing all applicable security patches within one month of release.	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.
6.3 Develop internal and external software applications (including web-based administrative access to applications) securely, as follows: • In accordance with PCI DSS (for example, secure authentication and logging) • Based on industry standards and/or best practices. • Incorporating information security throughout the software-development life cycle	x	x	Customers are responsible to maintain software development standards aligned with PCI requirements for applications developed and deployed on customer-managed GCP GCE 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 GCP GCE instances.	Google is responsible for protecting the systems and infrastructure underlying GCP from vulnerabilities in compliance with this requirement.
6.3.1 Remove development, test and/or custom application accounts, user IDs, and passwords before applications become active or are released to customers.	x	x	Customers are responsible to maintain software development standards aligned with PCI requirements for applications developed and deployed on customer-managed GCP GCE 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 GCP GCE instances.	Google is responsible for protecting the systems and infrastructure underlying GCP from vulnerabilities in compliance with this requirement.
6.3.2 Review custom code prior to release to production or customers in order to identify any potential coding vulnerability (using either manual or automated processes) to include at least the following: • Code changes are reviewed by individuals other than the originating code author, and by individuals knowledgeable about code-review techniques and secure coding practices. • Code reviews ensure code is developed according to secure coding guidelines • Appropriate corrections are implemented prior to release. • Code-review results are reviewed and approved by management prior to release.	x	x	Customers are responsible to maintain software development standards aligned with PCI requirements for applications developed and deployed on customer-managed GCP GCE 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 GCP GCE instances.	Google is responsible for protecting the systems and infrastructure underlying GCP from vulnerabilities in compliance with this requirement.
6.4 Follow change control processes and procedures for all changes to system components. The processes must include the following:		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	Customers must designate separate VPCs for development/test and production and enforce appropriate firewall rules ingress and egress with appropriate access controls.	Customers must designate different GCP buckets for development/test and production. They cannot use the GCS buckets for both dev/test and production.	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 GCE instances. IAM roles and permissions can be used to separate development and test environments.	Not Applicable

			customer-managed GCE instances.				
6.4.1 Separate development/test environments from production environments, and enforce the separation with access controls.		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 GCE instances.	Customers must designate separate VPCs for development/test and production and enforce appropriate firewall rules ingress and egress with appropriate access controls.	Customers must designate different GCP buckets for development/test and production. They cannot use the GCS buckets for both dev/test and production.	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 GCE instances. IAM roles and permissions can be used to separate development and test environments.	Not Applicable
6.4.2 Separation of duties between development/test and production environments.		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 GCE instances.	Customers must designate separate VPCs for development/test and production and enforce appropriate firewall rules ingress and egress with appropriate access controls.	Customers must designate different GCP buckets for development/test and production. They cannot use the GCS buckets for both dev/test and production.	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 GCE instances. IAM roles and permissions can be used to separate development and test environments.	Not Applicable
6.4.3 Production data (live PANs) are not used for testing or development		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 GCE instances.	Customers are responsible for ensuring production data is not used for development or testing in non-production VPCs.	Customers are responsible for ensuring production data is not used for development or testing in non-production GCS buckets.	Customers are responsible to maintain software development standards, change control processes, and vulnerability management standards aligned with PCI requirements	Not Applicable
6.4.4 Removal of test data and accounts from system components before the system becomes active/goes into production.		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 GCE instances.	Customers are responsible for removing all test data and accounts from VPCs prior to going live in production.	Customers are responsible for removing all test data and accounts from GCS buckets and objects prior to going live in production.	Customers are responsible to maintain software development standards, change control processes, and vulnerability management standards aligned with PCI requirements	Not Applicable

6.4.5 Change control procedures must include the following:	x	x	Customers are responsible for configuration changes and change control processes, including documentation of impact for all changes made to GCE instances.	Customers are responsible for configuration changes and change control processes, including documentation of impact for all changes made to in-scope VPCs.	Customers are responsible for configuration changes and change control processes, including documentation of impact for all changes made to GCS buckets.	Customers are responsible for any custom configurations and all changes to GCP product configurations are subject to customer change control procedures. Customers are responsible to maintain software development standards, change control processes, and vulnerability management standards aligned with PCI requirements for systems components and applications developed and deployed on GCP products.	Google is responsible for protecting the systems and infrastructure underlying GCP from vulnerabilities in compliance with this requirement.
6.4.5.1 Documentation of impact.	x	x	Customers are responsible for configuration changes and change control processes, including documentation of impact for all changes made to GCE instances.	Customers are responsible for configuration changes and change control processes, including documentation of impact for all changes made to in-scope VPCs.	Customers are responsible for configuration changes and change control processes, including documentation of impact for all changes made to GCS buckets.	Customers are responsible for any custom configurations and all changes to GCP product configurations are subject to customer change control procedures. Customers are responsible to maintain software development standards, change control processes, and vulnerability management standards aligned with PCI requirements for systems components and applications developed and deployed on GCP products.	Google is responsible for protecting the systems and infrastructure underlying GCP from vulnerabilities in compliance with this requirement.
6.4.5.2 Documented change approval by authorized parties.	x	x	Customers are responsible for configuration changes and change control processes, including documented approval for all changes made to GCE instances.	Customers are responsible for configuration changes and change control processes, including documented approval for all changes made to in-scope VPCs.	Customers are responsible for configuration changes and change control processes, including documented approval for all changes made to GCS buckets.	Customers are responsible for any custom configurations and all changes to GCP product configurations are subject to customer change control procedures. Customers are responsible to maintain software development standards, change control processes, and vulnerability management standards aligned with PCI requirements for systems components and applications developed and deployed on GCP products.	Google is responsible for protecting the systems and infrastructure underlying GCP from vulnerabilities in compliance with this requirement.
6.4.5.3 Functionality testing to verify that the change does not adversely impact the security of the system.	x	x	Customers are responsible for configuration changes and change control processes, including functionality testing for all changes made to GCE instances.	Customers are responsible for configuration changes and change control processes, including functionality testing for all changes made to in-scope VPCs.	Customers are responsible for configuration changes and change control processes, including functionality testing for all changes made to GCS buckets.	Customers are responsible for any custom configurations and all changes to GCP product configurations are subject to customer change control procedures. Customers are responsible to maintain software development standards, change control processes, and vulnerability management standards aligned with PCI requirements for systems components and applications developed and deployed on GCP products.	Google is responsible for protecting the systems and infrastructure underlying GCP from vulnerabilities in compliance with this requirement.
6.4.5.4 Back-out procedures.	x	x	Customers are responsible for configuration changes and change control processes, including backout procedures for all changes made to GCE instances.	Customers are responsible for configuration changes and change control processes, including backout procedures for all changes made to in-scope VPCs.	Customers are responsible for configuration changes and change control processes, including backout procedures for all changes made to GCS buckets.	Customers are responsible for any custom configurations and all changes to GCP product configurations are subject to customer change control procedures. Customers are responsible to maintain software development standards, change control processes, and vulnerability management standards aligned with PCI requirements for systems components and applications developed and deployed on GCP products.	Google is responsible for protecting the systems and infrastructure underlying GCP from vulnerabilities in compliance with this requirement.

6.4.6 Upon completion of a significant change, all relevant PCI DSS requirements must be implemented on all new or changed systems and networks, and documentation updated as applicable.	x	x	Customers are responsible for configuration changes and change control processes, including significant changes made to GCE instances.	Customers are responsible for configuration changes and change control processes, including significant changes made to in-scope VPCs.	Customers are responsible for configuration changes and change control processes, including significant changes made to GCS buckets.	Customers are responsible for any custom configurations and all changes to GCP product configurations are subject to customer change control procedures. Customers are responsible to maintain software development standards, change control processes, and vulnerability management standards aligned with PCI requirements for systems components and applications developed and deployed on GCP products.	Google is responsible for protecting the systems and infrastructure underlying GCP from vulnerabilities in compliance with this requirement.
6.5 Address common coding vulnerabilities in software-development processes as follows: • Train developers at least annually in up-to-date secure coding techniques, including how to avoid common coding vulnerabilities. • Develop applications based on secure coding guidelines.		x	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 GCP GCE 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 GCP GCE instances.	Not Applicable
6.5.1 Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws.		x	Customers are responsible to maintain software development standards aligned with PCI requirements for applications developed and deployed on customer-managed GCP GCE 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 GCP GCE instances.	Not Applicable
6.5.2 Buffer overflows		x	Customers are responsible to maintain software development standards aligned with PCI requirements for applications developed and deployed on customer-managed GCP GCE 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 GCP GCE instances.	Not Applicable
6.5.3 Insecure cryptographic storage		x	Customers are responsible to maintain software development standards aligned with PCI requirements for applications developed and deployed on customer-managed GCP GCE 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 GCP GCE instances.	Not Applicable

6.5.4 Insecure communications		x	Customers are responsible to maintain software development standards aligned with PCI requirements for applications developed and deployed on customer-managed GCP GCE 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 GCP GCE instances.	Not Applicable
6.5.5 Improper error handling		x	Customers are responsible to maintain software development standards aligned with PCI requirements for applications developed and deployed on customer-managed GCP GCE 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 GCP GCE instances.	Not Applicable
6.5.6 All “high risk” vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.1).		x	Customers are responsible to maintain software development standards aligned with PCI requirements for applications developed and deployed on customer-managed GCP GCE 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 GCP GCE instances.	Not Applicable
6.5.7 Cross-site scripting (XSS)		x	Customers are responsible to maintain software development standards aligned with PCI requirements for applications developed and deployed on customer-managed GCP GCE 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 GCP GCE instances.	Not Applicable
6.5.8 Improper access control (such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access to functions).		x	Customers are responsible to maintain software development standards aligned with PCI requirements for applications developed and deployed on customer-managed GCP GCE 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 GCP GCE instances.	Not Applicable
6.5.9 Cross-site request forgery (CSRF)		x	Customers are responsible to maintain software development standards aligned with PCI requirements for applications developed and	Not Applicable	Not Applicable	Customers are responsible to maintain software development standards aligned with PCI requirements for applications developed and deployed on customer-managed GCP GCE instances.	Not Applicable

			deployed on customer-managed GCP GCE instances.				
6.5.10 Broken authentication and session management		x	Customers are responsible to maintain software development standards aligned with PCI requirements for applications developed and deployed on customer-managed GCP GCE 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 GCP GCE instances.	Not Applicable
6.6 For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods: • Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes • Installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) in front of public-facing web applications, to continually check all traffic.		x	Customers are responsible for Web Application Filtering or application security reviews for web applications deployed on customer-managed GCE instances.	Not Applicable	Not Applicable	Customers are responsible for Web Application Filtering or application security reviews for web applications deployed on customer-managed GCE instances.	Not Applicable
6.7 Ensure that security policies and operational procedures for developing and maintaining secure systems and applications are documented, in use, and known to all affected parties.		x	GCP customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	GCP customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	GCP customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	GCP customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	Not Applicable

			Customers Responsibility Summary				
PCI DSS v3.2.1 Requirements	**GCP**	**Customer**	**Compute** App Engine Bare Metal Compute Engine Cloud Run Preemptible VMs Shielded VMs	**Networking** Cloud Armor Cloud NAT Hybrid Connectivity Network Intelligence Center Network Telemetry Service Directory Traffic Director Virtual Private Cloud (VPC)	**Storage** Archive Storage Cloud Storage Filestore Local SSD Persistent Disk	**Security** Access Transparency Assured Workloads Binary Authorization Chronicle Cloud Asset Inventory Cloud Data Loss Prevention Cloud Key Management Firewalls Secret Manager Security Command Center Shielded VMs VPC Service Controls **Identity and Access** Cloud Identity Identity and Access Management Identity-Aware Proxy Identity Platform Managed Service for Microsoft Active Directory Policy Intelligence Resource Manager Titan Security Key	**Google Responsibility Summary**
Requirement 7: Restrict access to cardholder data by business need to know.							
7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.	x	x	GCP Customers are responsible for managing access to all GCP products (GCE, VPC, GCS) 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.	GCP Customers are responsible for managing access to all GCP products (GCE, VPC, GCS) 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.	GCP Customers are responsible for managing access to all GCP products (GCE, VPC, GCS) 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.	GCP Customers are responsible for managing access to all GCP products (GCE, VPC, GCS) 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.
7.1.1 Define access needs for each role, including: - System components and data resources that each role needs to access for their job function - Level of privilege required (for example, user, administrator, etc.) for accessing resources.	x	x	GCP Customers are responsible for managing access to all GCP products (GCE, VPC, GCS) 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.	GCP Customers are responsible for managing access to all GCP products (GCE, VPC, GCS) 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.	GCP Customers are responsible for managing access to all GCP products (GCE, VPC, GCS) 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.	GCP Customers are responsible for managing access to all GCP products (GCE, VPC, GCS) 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.

7.1.2 Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.	x	x	GCP Customers are responsible for managing access to all GCP products (GCE, VPC, GCS) 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.	GCP Customers are responsible for managing access to all GCP products (GCE, VPC, GCS) 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.	GCP Customers are responsible for managing access to all GCP products (GCE, VPC, GCS) 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.	GCP Customers are responsible for managing access to all GCP products (GCE, VPC, GCS) 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.
7.1.3 Assign access based on individual personnel's job classification and function.	x	x	GCP Customers are responsible for managing access to all GCP products (GCE, VPC, GCS) 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.	GCP Customers are responsible for managing access to all GCP products (GCE, VPC, GCS) 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.	GCP Customers are responsible for managing access to all GCP products (GCE, VPC, GCS) 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.	GCP Customers are responsible for managing access to all GCP products (GCE, VPC, GCS) 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.
7.1.4 Require documented approval by authorized parties specifying required privileges.	x	x	GCP Customers are responsible for managing access to all GCP products (GCE, VPC, GCS) 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.	GCP Customers are responsible for managing access to all GCP products (GCE, VPC, GCS) 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.	GCP Customers are responsible for managing access to all GCP products (GCE, VPC, GCS) 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.	GCP Customers are responsible for managing access to all GCP products (GCE, VPC, GCS) 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 Establish an access control system for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system must include the following:	x	x	GCP Customers are responsible for managing access to all GCP products (GCE, VPC, GCS) 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.	GCP Customers are responsible for managing access to all GCP products (GCE, VPC, GCS) 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.	GCP Customers are responsible for managing access to all GCP products (GCE, VPC, GCS) 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.	GCP Customers are responsible for managing access to all GCP products (GCE, VPC, GCS) 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.
7.2.1 Coverage of all system components	x	x	GCP Customers are responsible for managing access to all GCP products (GCE, VPC, GCS) 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.	GCP Customers are responsible for managing access to all GCP products (GCE, VPC, GCS) 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.	GCP Customers are responsible for managing access to all GCP products (GCE, VPC, GCS) 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.	GCP Customers are responsible for managing access to all GCP products (GCE, VPC, GCS) 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 Assignment of privileges to individuals based on job classification and function.	x	x	GCP Customers are responsible for managing access to all GCP products (GCE, VPC, GCS) 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.	GCP Customers are responsible for managing access to all GCP products (GCE, VPC, GCS) 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.	GCP Customers are responsible for managing access to all GCP products (GCE, VPC, GCS) 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.	GCP Customers are responsible for managing access to all GCP products (GCE, VPC, GCS) 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 Default "deny-all" setting.	x	x	GCP Customers are responsible for managing access to all GCP products (GCE, VPC, GCS) 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.	GCP Customers are responsible for managing access to all GCP products (GCE, VPC, GCS) 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.	GCP Customers are responsible for managing access to all GCP products (GCE, VPC, GCS) 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.	GCP Customers are responsible for managing access to all GCP products (GCE, VPC, GCS) 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 Ensure that security policies and operational procedures for restricting access to cardholder data are documented, in use, and known to all affected parties.		x	GCP customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	GCP customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	GCP customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	GCP customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	Not Applicable

			Customers Responsibility Summary				
PCI DSS v3.2.1 Requirements	**GCP**	**Customer**	**Compute** App Engine Bare Metal Compute Engine Cloud Run Preemptible VMs Shielded VMs	**Networking** Cloud Armor Cloud NAT Hybrid Connectivity Network Intelligence Center Network Telemetry Service Directory Traffic Director Virtual Private Cloud (VPC)	**Storage** Archive Storage Cloud Storage Filestore Local SSD Persistent Disk	**Security** Access Transparency Assured Workloads Binary Authorization Chronicle Cloud Asset Inventory Cloud Data Loss Prevention Cloud Key Management Firewalls Secret Manager Security Command Center Shielded VMs VPC Service Controls **Identity and Access** Cloud Identity Identity and Access Management Identity-Aware Proxy Identity Platform Managed Service for Microsoft Active Directory Policy Intelligence Resource Manager Titan Security Key	**Google Responsibility Summary**
Requirement 8: Identify and authenticate access to system components.							
8.1 Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components as follows:	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, in-scope VPCs, GCS buckets and objects) as well as to the GCE compute instances and customer specific applications.	Customers are responsible for managing the creation of user accounts, including GCP accounts. This includes access controls to all in scope GCP products (GCE, in-scope VPCs, GCS buckets and objects) as well as to the GCE compute instances and customer specific applications.	Customers are responsible for managing the creation of user accounts, including GCP accounts. This includes access controls to all in scope GCP products (GCE, in-scope VPCs, GCS buckets and objects) as well as to the GCE compute instances and customer specific applications.	Customers are responsible for managing the creation of user accounts, including GCP accounts. This includes access controls to all in scope GCP products (GCE, in-scope VPCs, GCS buckets and objects) as well as to the GCE compute instances and customer specific applications.	Google is responsible for implementing access controls in compliance with this requirement for the systems and infrastructure underlying GCP.
8.1.1 Assign all users a unique ID before allowing them to access system components or cardholder data.	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, in-scope VPCs, GCS buckets and objects) as well as to the GCE compute instances and customer specific applications.	Customers are responsible for managing the creation of user accounts, including GCP accounts. This includes access controls to all in scope GCP products (GCE, in-scope VPCs, GCS buckets and objects) as well as to the GCE compute instances and customer specific applications.	Customers are responsible for managing the creation of user accounts, including GCP accounts. This includes access controls to all in scope GCP products (GCE, in-scope VPCs, GCS buckets and objects) as well as to the GCE compute instances and customer specific applications.	Customers are responsible for managing the creation of user accounts, including GCP accounts. This includes access controls to all in scope GCP products (GCE, in-scope VPCs, GCS buckets and objects) as well as to the GCE compute instances and customer specific applications.	Google is responsible for implementing access controls in compliance with this requirement for the systems and infrastructure underlying GCP.
8.1.2 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.	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, in-scope VPCs, GCS buckets and objects) as well as to the GCE compute instances and	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, in-scope VPCs, GCS buckets and objects) as well as to the GCE compute instances and 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, in-scope VPCs, GCS buckets and objects) as well as to the GCE compute instances and 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, in-scope VPCs, GCS buckets and objects) as well as to the GCE compute instances and customer	Google is responsible for implementing access controls in compliance with this requirement for the systems and infrastructure underlying GCP.

			customer specific applications.			specific applications.	
8.1.3 Immediately revoke access for any terminated users.	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, in-scope VPCs, GCS buckets and objects) as well as to the GCE compute instances and 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, in-scope VPCs, GCS buckets and objects) as well as to the GCE compute instances and 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, in-scope VPCs, GCS buckets and objects) as well as to the GCE compute instances and 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, in-scope VPCs, GCS buckets and objects) as well as to the GCE compute instances and customer specific applications.	Google is responsible for implementing access controls in compliance with this requirement for the systems and infrastructure underlying GCP.
8.1.4 Remove/disable inactive user accounts within 90 days.	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, in-scope VPCs, GCS buckets and objects) as well as to the GCE compute instances and 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, in-scope VPCs, GCS buckets and objects) as well as to the GCE compute instances and 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, in-scope VPCs, GCS buckets and objects) as well as to the GCE compute instances and 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, in-scope VPCs, GCS buckets and objects) as well as to the GCE compute instances and customer specific applications.	Google is responsible for implementing access controls in compliance with this requirement for the systems and infrastructure underlying GCP.
8.1.5 Manage IDs used by third parties to access, support, or maintain system components via remote access as follows: - Enabled only during the time period needed and disabled when not in use. - Monitored when in use.		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, in-scope VPCs, GCS buckets and objects) as well as to the GCE compute instances and 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, in-scope VPCs, GCS buckets and objects) as well as to the GCE compute instances and 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, in-scope VPCs, GCS buckets and objects) as well as to the GCE compute instances and 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, in-scope VPCs, GCS buckets and objects) as well as to the GCE compute instances and customer specific applications.	Not Applicable. Google does not allow any remote vendor access within the in-scope GCP environment.
8.1.6 Limit repeated access attempts by locking out the user ID after not more than six attempts.	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, in-scope VPCs, GCS buckets and objects) as well as to the GCE compute instances and 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, in-scope VPCs, GCS buckets and objects) as well as to the GCE compute instances and 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, in-scope VPCs, GCS buckets and objects) as well as to the GCE compute instances and 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, in-scope VPCs, GCS buckets and objects) as well as to the GCE compute instances and 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 six invalid access

							attempts.
8.1.7 Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.		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, in-scope VPCs, GCS buckets and objects) as well as to the GCE compute instances and 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, in-scope VPCs, GCS buckets and objects) as well as to the GCE compute instances and 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, in-scope VPCs, GCS buckets and objects) as well as to the GCE compute instances and 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, in-scope VPCs, GCS buckets and objects) as well as to the GCE compute instances and 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.	Not Applicable. Invalid logon attempts are prevented via the use of SSH public/private key pairs and Low Overhead Authentication Service (LOAS) certificates.
8.1.8 If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.	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, in-scope VPCs, GCS buckets and objects) as well as to the GCE compute instances and 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, in-scope VPCs, GCS buckets and objects) as well as to the GCE compute instances and 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, in-scope VPCs, GCS buckets and objects) as well as to the GCE compute instances and 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, in-scope VPCs, GCS buckets and objects) as well as to the GCE compute instances and 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.
8.2 In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users: - Something you know, such as a password or passphrase - Something you have, such as a token device or smart card - Something you are, such as a biometric.	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, in-scope VPCs, GCS buckets and objects) as well as to the GCE compute instances and 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, in-scope VPCs, GCS buckets and objects) as well as to the GCE compute instances and 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, in-scope VPCs, GCS buckets and objects) as well as to the GCE compute instances and 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, in-scope VPCs, GCS buckets and objects) as well as to the GCE compute instances and 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.

8.2.1 Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.	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.
8.2.2 Verify user identity before modifying any authentication credential—for example, performing password resets, provisioning new tokens, or generating new keys.	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, in-scope VPCs, GCS buckets and objects) as well as to the GCE compute instances and 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, in-scope VPCs, GCS buckets and objects) as well as to the GCE compute instances and 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, in-scope VPCs, GCS buckets and objects) as well as to the GCE compute instances and 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, in-scope VPCs, GCS buckets and objects) as well as to the GCE compute instances and 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.
8.2.3 Passwords/phrases must meet the following: - Require a minimum length of at least seven characters. - Contain both numeric and alphabetic characters. Alternatively, the passwords/phrases must have complexity and strength at least equivalent to the parameters specified above.	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, which the customer must enforce to 7 chacters minimum and mixed complexity. 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, which the customer must enforce to 7 chacters minimum and mixed complexity. 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, which the customer must enforce to 7 chacters minimum and mixed complexity. 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, which the customer must enforce to 7 characters minimum and mixed complexity. 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.
8.2.4 Change user passwords/passphrases at least once every 90 days.	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.

8.2.5 Do not allow an individual to submit a new password/phrase that is the same as any of the last four passwords/phrases he or she has used.	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 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 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 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 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.
8.2.6 Set passwords/phrases for first-time use and upon reset to a unique value for each user, and change immediately after the first use.	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.
8.3 Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication. Note: Multi-factor authentication requires that a minimum of two of the three authentication methods (see Requirement 8.2 for descriptions of authentication methods) be used for authentication. Using one factor twice (for example, using two separate passwords) is not considered multi-factor authentication.	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.
8.3.1 Incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access.	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.

8.3.2 Incorporate multi-factor authentication for all remote network access (both user and administrator, and including third-party access for support or maintenance) originating from outside the entity's network.	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 Document and communicate authentication procedures and policies and procedures to all users including: - Guidance on selecting strong authentication credentials - Guidance for how users should protect their authentication credentials - Instructions not to reuse previously used passwords - Instructions to change passwords if there is any suspicion the password could be compromised.	x	x	GCP customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	GCP customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	GCP customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	GCP 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.
8.5 Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows: - Generic user IDs are disabled or removed. - Shared user IDs do not exist for system administration and other critical functions. - Shared and generic user IDs are not used to administer any system components.	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, in-scope VPCs, GCS buckets and objects) as well as to the GCE compute instances and 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, in-scope VPCs, GCS buckets and objects) as well as to the GCE compute instances and 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, in-scope VPCs, GCS buckets and objects) as well as to the GCE compute instances and 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, in-scope VPCs, GCS buckets and objects) as well as to the GCE compute instances and 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.
8.5.1 Additional requirement for service providers only: Service providers with remote access to customer premises (for example, for support of POS systems or servers) must use a unique authentication credential (such as a password/phrase) for each customer. Note: This requirement is not intended to apply to shared hosting providers accessing their own hosting environment, where multiple customer environments are hosted.		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, in-scope VPCs, GCS buckets and objects) as well as to the GCE compute instances and 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, in-scope VPCs, GCS buckets and objects) as well as to the GCE compute instances and 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, in-scope VPCs, GCS buckets and objects) as well as to the GCE compute instances and 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, in-scope VPCs, GCS buckets and objects) as well as to the GCE compute instances and 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.

8.6 Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.), use of these mechanisms must be assigned as follows: - Authentication mechanisms must be assigned to an individual account and not shared among multiple accounts. - Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access.	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.
8.7 All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows: - All user access to, user queries of, and user actions on databases are through programmatic methods. - Only database administrators have the ability to directly access or query databases. - Application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes).		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. Google does not have access to customer data in a readable format.
8.8 Ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties.		x	GCP customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	GCP customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	GCP customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	GCP customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	Not Applicable

			Customers Responsibility Summary				
PCI DSS v3.2.1 Requirements	**GCP**	**Customer**	**Compute** App Engine Bare Metal Compute Engine Cloud Run Preemptible VMs Shielded VMs	**Networking** Cloud Armor Cloud NAT Hybrid Connectivity Network Intelligence Center Network Telemetry Service Directory Traffic Director Virtual Private Cloud (VPC)	**Storage** Archive Storage Cloud Storage Filestore Local SSD Persistent Disk	**Security** Access Transparency Assured Workloads Binary Authorization Chronicle Cloud Asset Inventory Cloud Data Loss Prevention Cloud Key Management Firewalls Secret Manager Security Command Center Shielded VMs VPC Service Controls **Identity and Access** Cloud Identity Identity and Access Management Identity-Aware Proxy Identity Platform Managed Service for Microsoft Active Directory Policy Intelligence Resource Manager Titan Security Key	**Google Responsibility Summary**
Requirement 9: Restrict physical access to cardholder data.							
9.1 Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.	x		Not Applicable	Not Applicable	Not Applicable	Not Applicable	GCP maintains the physical security and media handling controls for GCP data centers and colocations supporting the products included in the assessment.
9.1.1 Use either video cameras or access control mechanisms (or both) to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law. *Note: "Sensitive areas" refers to any data center, server room or any area that houses systems that store, process, or transmit cardholder data. This excludes public-facing areas where only point-of-sale terminals are present, such as the cashier areas in a retail store.*	x		Not Applicable	Not Applicable	Not Applicable	Not Applicable	GCP maintains the physical security and media handling controls for GCP data centers and colocations supporting the products included in the assessment.
9.1.2 Implement physical and/or logical controls to restrict access to publicly accessible network jacks. *For example, network jacks located in public areas and areas accessible to visitors could be disabled and only enabled when network access is explicitly authorized. Alternatively, processes could be implemented to ensure that visitors are*	x		Not Applicable	Not Applicable	Not Applicable	Not Applicable	GCP maintains the physical security and media handling controls for GCP data centers and colocations supporting the products included in the assessment.

escorted at all times in areas with active network jacks.							
9.1.3 Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines.	x		Not Applicable	Not Applicable	Not Applicable	Not Applicable	GCP maintains the physical security and media handling controls for GCP data centers and colocations supporting the products included in the assessment.
9.2 Develop procedures to easily distinguish between onsite personnel and visitors, to include: - Identifying onsite personnel and visitors (for example, assigning badges) - Changes to access requirements - Revoking or terminating onsite personnel and expired visitor identification (such as ID badges).	x		Not Applicable	Not Applicable	Not Applicable	Not Applicable	GCP maintains the physical security and media handling controls for GCP data centers and colocations supporting the products included in the assessment.
9.3 Control physical access for onsite personnel to the sensitive areas as follows: - Access must be authorized and based on individual job function. - Access is revoked immediately upon termination, and all physical access mechanisms, such as keys, access cards, etc., are returned or disabled.	x		Not Applicable	Not Applicable	Not Applicable	Not Applicable	GCP maintains the physical security and media handling controls for GCP data centers and colocations supporting the products included in the assessment.
9.4 Implement procedures to identify and authorize visitors. Procedures should include the following:	x		Not Applicable	Not Applicable	Not Applicable	Not Applicable	GCP maintains the physical security and media handling controls for GCP data centers and colocations supporting the products included in the assessment.
9.4.1 Visitors are authorized before entering, and escorted at all times within areas where cardholder data is processed or maintained.	x		Not Applicable	Not Applicable	Not Applicable	Not Applicable	GCP maintains the physical security and media handling controls for GCP data centers and colocations supporting the products included in the assessment.
9.4.2 Visitors are identified and given a badge or other identification that expires and that visibly distinguishes the visitors from onsite personnel.	x		Not Applicable	Not Applicable	Not Applicable	Not Applicable	GCP maintains the physical security and media handling controls for GCP data centers and colocations supporting the products included in the assessment.
9.4.3 Visitors are asked to surrender the badge or identification before leaving the facility or at the date of expiration.	x		Not Applicable	Not Applicable	Not Applicable	Not Applicable	GCP maintains the physical security and media handling controls for GCP data centers and colocations supporting the products included in the assessment.
9.4.4 A visitor log is used to maintain a physical audit trail of visitor activity to the facility as well as computer rooms and data centers where cardholder data is stored or transmitted. Document the visitor's name, the firm represented, and the onsite personnel authorizing physical access on the log. Retain this log for a minimum of three months, unless otherwise restricted by law.	x		Not Applicable	Not Applicable	Not Applicable	Not Applicable	GCP maintains the physical security and media handling controls for GCP data centers and colocations supporting the products included in the assessment.

9.5 Physically secure all media.	x	x	GCP customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	GCP customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	GCP customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	GCP customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	GCP maintains the physical security and media handling controls for GCP data centers and colocations supporting the products included in the assessment. GCP does not store customer data on removable media.
9.5.1 Store media backups in a secure location, preferably an off-site facility, such as an alternate or backup site, or a commercial storage facility. Review the location's security at least annually.	x	x	GCP customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	GCP customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	GCP customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	GCP customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	GCP maintains the physical security and media handling controls for GCP data centers and colocations supporting the products included in the assessment. GCP does not store customer data on removable media.
9.6 Maintain strict control over the internal or external distribution of any kind of media, including the following:	x	x	GCP customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	GCP customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	GCP customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	GCP customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	GCP maintains the physical security and media handling controls for GCP data centers and colocations supporting the products included in the assessment. GCP does not store customer data on removable media.
9.6.1 Classify media so the sensitivity of the data can be determined.	x	x	GCP customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	GCP customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	GCP customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	GCP customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	GCP maintains the physical security and media handling controls for GCP data centers and colocations supporting the products included in the assessment. GCP does not store customer data on removable media.

9.6.2 Send the media by secured courier or other delivery method that can be accurately tracked.	x	x	GCP customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	GCP customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	GCP customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	GCP customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	GCP maintains the physical security and media handling controls for GCP data centers and colocations supporting the products included in the assessment. GCP does not store customer data on removable media.
9.6.3 Ensure management approves any and all media that is moved from a secured area (including when media is distributed to individuals).	x	x	GCP customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	GCP customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	GCP customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	GCP customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	GCP maintains the physical security and media handling controls for GCP data centers and colocations supporting the products included in the assessment. GCP does not store customer data on removable media.
9.7 Maintain strict control over the storage and accessibility of media.	x	x	GCP customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	GCP customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	GCP customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	GCP customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	GCP maintains the physical security and media handling controls for GCP data centers and colocations supporting the products included in the assessment. GCP does not store customer data on removable media.
9.7.1 Properly maintain inventory logs of all media and conduct media inventories at least annually.	x	x	GCP customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	GCP customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	GCP customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	GCP customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	GCP maintains the physical security and media handling controls for GCP data centers and colocations supporting the products included in the assessment. GCP does not store customer data on removable media.

9.8 Destroy media when it is no longer needed for business or legal reasons as follows:	x	x	GCP customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	GCP customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	GCP customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	GCP customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	GCP maintains the physical security and media handling controls for GCP data centers and colocations supporting the products included in the assessment. GCP does not store customer data on removable media.
9.8.1 Shred, incinerate, or pulp hard-copy materials so that cardholder data cannot be reconstructed. Secure storage containers used for materials that are to be destroyed.	x	x	GCP customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	GCP customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	GCP customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	GCP customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	GCP maintains the physical security and media handling controls for GCP data centers and colocations supporting the products included in the assessment. GCP does not store customer data on removable media.
9.8.2 Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.	x	x	GCP customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	GCP customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	GCP customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	GCP customers are responsible for backup, compliance and destruction of media outside of the GCP environment.	GCP maintains the physical security and media handling controls for GCP data centers and colocations supporting the products included in the assessment. GCP does not store customer data on removable media.
9.9 Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution. *Note: These requirements apply to card-reading devices used in card-present transactions (that is, card swipe or dip) at the point of sale. This requirement is not intended to apply to manual key-entry components such as computer keyboards and POS keypads.*		x	Customer is responsible for all devices that capture payment card data via direct physical interaction with the card.	Customer is responsible for all devices that capture payment card data via direct physical interaction with the card.	Customer is responsible for all devices that capture payment card data via direct physical interaction with the card.	Customer is responsible for all devices that capture payment card data via direct physical interaction with the card.	Not Applicable
9.9.1 Maintain an up-to-date list of devices. The list should include the following: - Make, model of device - Location of device (for example, the address of the site or facility where the device is located) - Device serial number or other method of unique identification.		x	Customer is responsible for all devices that capture payment card data via direct physical interaction with the card.	Customer is responsible for all devices that capture payment card data via direct physical interaction with the card.	Customer is responsible for all devices that capture payment card data via direct physical interaction with the card.	Customer is responsible for all devices that capture payment card data via direct physical interaction with the card.	Not Applicable

9.9.2 Periodically inspect device surfaces to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device). *Note: Examples of signs that a device might have been tampered with or substituted include unexpected attachments or cables plugged into the device, missing or changed security labels, broken or differently colored casing, or changes to the serial number or other external markings*.		x	Customer is responsible for all devices that capture payment card data via direct physical interaction with the card.	Customer is responsible for all devices that capture payment card data via direct physical interaction with the card.	Customer is responsible for all devices that capture payment card data via direct physical interaction with the card.	Customer is responsible for all devices that capture payment card data via direct physical interaction with the card.	Not Applicable
9.9.3 Provide training for personnel to be aware of attempted tampering or replacement of devices. Training should include the following: - Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices. - Do not install, replace, or return devices without verification. - Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices). - Report suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer).		x	Customer is responsible for all devices that capture payment card data via direct physical interaction with the card.	Customer is responsible for all devices that capture payment card data via direct physical interaction with the card.	Customer is responsible for all devices that capture payment card data via direct physical interaction with the card.	Customer is responsible for all devices that capture payment card data via direct physical interaction with the card.	Not Applicable
9.10 Ensure that security policies and operational procedures for restricting physical access to cardholder data are documented, in use, and known to all affected parties.		x	GCP customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	GCP customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	GCP customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	GCP customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	Not Applicable

			Customers Responsibility Summary				
PCI DSS v3.2.1 Requirements	**GCP**	**Customer**	**Compute** App Engine Bare Metal Compute Engine Cloud Run Preemptible VMs Shielded VMs	**Networking** Cloud Armor Cloud NAT Hybrid Connectivity Network Intelligence Center Network Telemetry Service Directory Traffic Director Virtual Private Cloud (VPC)	**Storage** Archive Storage Cloud Storage Filestore Local SSD Persistent Disk	**Security** Access Transparency Assured Workloads Binary Authorization Chronicle Cloud Asset Inventory Cloud Data Loss Prevention Cloud Key Management Firewalls Secret Manager Security Command Center Shielded VMs VPC Service Controls **Identity and Access** Cloud Identity Identity and Access Management Identity-Aware Proxy Identity Platform Managed Service for Microsoft Active Directory Policy Intelligence Resource Manager Titan Security Key	**Google Responsibility Summary**
Requirement 10: Track and monitor all access to network resources and cardholder data.							
10.1 Implement audit trails to link all access to system components to each individual user.	x	x	GCP customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their GCE, and GKE instances, systems and applications in alignment with PCI DSS requirements.	GCP customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their GCE, and GKE instances, systems and applications in alignment with PCI DSS requirements.	GCP customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their GCE, and GKE instances, systems and applications in alignment with PCI DSS requirements.	GCP customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their GCE, and GKE instances, systems and applications in alignment with PCI DSS requirements.	Google has PCI DSS compliance responsibility for dedicated internal Google Production and management network systems.
10.2 Implement automated audit trails for all system components to reconstruct the following events:	x	x	GCP customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their GCE, and GKE instances, systems and applications in alignment with PCI DSS requirements.	GCP customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their GCE, and GKE instances, systems and applications in alignment with PCI DSS requirements.	GCP customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their GCE, and GKE instances, systems and applications in alignment with PCI DSS requirements.	GCP customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their GCE, and GKE instances, systems 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 All individual user accesses to cardholder data		x	GCP customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their GCE, and GKE instances, systems and applications in alignment with PCI DSS requirements.	GCP customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their GCE, and GKE instances, systems and applications in alignment with PCI DSS requirements.	GCP customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their GCE, and GKE instances, systems and applications in alignment with PCI DSS requirements.	GCP customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their GCE, and GKE instances, systems and applications in alignment with PCI DSS requirements.	Not Applicable. Google does not store PAN as such user access to cardholder data is the sole responsibility of the customer.

10.2.2 All actions taken by any individual with root or administrative privileges	x	x	GCP customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their GCE, and GKE instances, systems and applications in alignment with PCI DSS requirements.	GCP customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their GCE, and GKE instances, systems and applications in alignment with PCI DSS requirements.	GCP customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their GCE, and GKE instances, systems and applications in alignment with PCI DSS requirements.	GCP customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their GCE, and GKE instances, systems 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.
10.2.3 Access to all audit trails	x	x	GCP customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their GCE, and GKE instances, systems and applications in alignment with PCI DSS requirements.	GCP customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their GCE, and GKE instances, systems and applications in alignment with PCI DSS requirements.	GCP customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their GCE, and GKE instances, systems and applications in alignment with PCI DSS requirements.	GCP customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their GCE, and GKE instances, systems 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.
10.2.4 Invalid logical access attempts	x	x	GCP customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their GCE, and GKE instances, systems and applications in alignment with PCI DSS requirements.	GCP customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their GCE, and GKE instances, systems and applications in alignment with PCI DSS requirements.	GCP customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their GCE, and GKE instances, systems and applications in alignment with PCI DSS requirements.	GCP customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their GCE, and GKE instances, systems 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.
10.2.5 Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges.	x	x	GCP customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their GCE, and GKE instances, systems and applications in alignment with PCI DSS requirements.	GCP customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their GCE, and GKE instances, systems and applications in alignment with PCI DSS requirements.	GCP customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their GCE, and GKE instances, systems and applications in alignment with PCI DSS requirements.	GCP customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their GCE, and GKE instances, systems 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.
10.2.6 Initialization, stopping, or pausing of the audit logs	x	x	GCP customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their GCE, and GKE instances, systems and applications in alignment with PCI DSS requirements.	GCP customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their GCE, and GKE instances, systems and applications in alignment with PCI DSS requirements.	GCP customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their GCE, and GKE instances, systems and applications in alignment with PCI DSS requirements.	GCP customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their GCE, and GKE instances, systems 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.
10.2.7 Creation and deletion of system-level objects	x	x	GCP customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their GCE, and GKE instances, systems and applications in alignment with PCI DSS requirements.	GCP customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their GCE, and GKE instances, systems and applications in alignment with PCI DSS requirements.	GCP customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their GCE, and GKE instances, systems and applications in alignment with PCI DSS requirements.	GCP customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their GCE, and GKE instances, systems 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.
10.3 Record at least the following audit trail entries for all system components for each event:	x	x	GCP customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their GCE, and GKE instances, systems and applications in alignment with PCI DSS requirements.	GCP customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their GCE, and GKE instances, systems and applications in alignment with PCI DSS requirements.	GCP customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their GCE, and GKE instances, systems and applications in alignment with PCI DSS requirements.	GCP customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their GCE, and GKE instances, systems 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.

10.3.1 User identification	x	x	GCP customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their GCE, and GKE instances, systems and applications in alignment with PCI DSS requirements.	GCP customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their GCE, and GKE instances, systems and applications in alignment with PCI DSS requirements.	GCP customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their GCE, and GKE instances, systems and applications in alignment with PCI DSS requirements.	GCP customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their GCE, and GKE instances, systems 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.
10.3.2 Type of event	x	x	GCP customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their GCE, and GKE instances, systems and applications in alignment with PCI DSS requirements.	GCP customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their GCE, and GKE instances, systems and applications in alignment with PCI DSS requirements.	GCP customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their GCE, and GKE instances, systems and applications in alignment with PCI DSS requirements.	GCP customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their GCE, and GKE instances, systems 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.
10.3.3 Date and time	x	x	GCP customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their GCE, and GKE instances, systems and applications in alignment with PCI DSS requirements.	GCP customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their GCE, and GKE instances, systems and applications in alignment with PCI DSS requirements.	GCP customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their GCE, and GKE instances, systems and applications in alignment with PCI DSS requirements.	GCP customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their GCE, and GKE instances, systems 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.
10.3.4 Success or failure indication	x	x	GCP customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their GCE, and GKE instances, systems and applications in alignment with PCI DSS requirements.	GCP customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their GCE, and GKE instances, systems and applications in alignment with PCI DSS requirements.	GCP customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their GCE, and GKE instances, systems and applications in alignment with PCI DSS requirements.	GCP customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their GCE, and GKE instances, systems 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.
10.3.5 Origination of event	x	x	GCP customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their GCE, and GKE instances, systems and applications in alignment with PCI DSS requirements.	GCP customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their GCE, and GKE instances, systems and applications in alignment with PCI DSS requirements.	GCP customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their GCE, and GKE instances, systems and applications in alignment with PCI DSS requirements.	GCP customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their GCE, and GKE instances, systems 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.
10.3.6 Identity or name of affected data, system component, or resource.	x	x	GCP customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their GCE, and GKE instances, systems and applications in alignment with PCI DSS requirements.	GCP customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their GCE, and GKE instances, systems and applications in alignment with PCI DSS requirements.	GCP customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their GCE, and GKE instances, systems and applications in alignment with PCI DSS requirements.	GCP customers are responsible for configuring logging parameters, when available. Customers are responsible to log and monitor their GCE, and GKE instances, systems 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.
10.4 Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time. *Note: One example of time synchronization technology is Network Time Protocol (NTP).*	x	x	GCP customers are responsible for appropriately managing network time protocol (NTP) configuration for their GCE and GKE instances.	GCP customers are responsible for appropriately managing network time protocol (NTP) configuration for their GCE and GKE instances.	GCP customers are responsible for appropriately managing network time protocol (NTP) configuration for their GCE and GKE instances.	GCP customers are responsible for appropriately managing network time protocol (NTP) configuration for their GCE and GKE instances.	Google is responsible for controlling access, logging and monitoring of the systems and infrastructure underlying GCP in compliance with this requirement.

10.4.1 Critical systems have the correct and consistent time.	x	x	GCP customers are responsible for appropriately managing network time protocol (NTP) configuration for their GCE and GKE instances.	GCP customers are responsible for appropriately managing network time protocol (NTP) configuration for their GCE and GKE instances.	GCP customers are responsible for appropriately managing network time protocol (NTP) configuration for their GCE and GKE instances.	GCP customers are responsible for appropriately managing network time protocol (NTP) configuration for their GCE and GKE instances.	Google is responsible for controlling access, logging and monitoring of the systems and infrastructure underlying GCP in compliance with this requirement.
10.4.2 Time data is protected.	x	x	GCP customers are responsible for appropriately managing network time protocol (NTP) configuration for their GCE and GKE instances.	GCP customers are responsible for appropriately managing network time protocol (NTP) configuration for their GCE and GKE instances.	GCP customers are responsible for appropriately managing network time protocol (NTP) configuration for their GCE and GKE instances.	GCP customers are responsible for appropriately managing network time protocol (NTP) configuration for their GCE and GKE instances.	Google is responsible for controlling access, logging and monitoring of the systems and infrastructure underlying GCP in compliance with this requirement.
10.4.3 Time settings are received from industry-accepted time sources.	x	x	GCP customers are responsible for appropriately managing network time protocol (NTP) configuration for their GCE and GKE instances.	GCP customers are responsible for appropriately managing network time protocol (NTP) configuration for their GCE and GKE instances.	GCP customers are responsible for appropriately managing network time protocol (NTP) configuration for their GCE and GKE instances.	GCP customers are responsible for appropriately managing network time protocol (NTP) configuration for their GCE and GKE instances.	Google is responsible for controlling access, logging and monitoring of the systems and infrastructure underlying GCP in compliance with this requirement.
10.5 Secure audit trails so they cannot be altered.	x	x	GCP 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 GCE and GKE systems and instances in alignment with PCI DSS requirements.	GCP 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 GCE and GKE systems and instances in alignment with PCI DSS requirements.	GCP 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 GCE and GKE systems and instances in alignment with PCI DSS requirements.	GCP 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 GCE and GKE systems and 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 Limit viewing of audit trails to those with a job-related need.	x	x	GCP 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 GCE and GKE systems and instances in alignment with PCI DSS requirements.	GCP 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 GCE and GKE systems and instances in alignment with PCI DSS requirements.	GCP 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 GCE and GKE systems and instances in alignment with PCI DSS requirements.	GCP 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 GCE and GKE systems and 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.
10.5.2 Protect audit trail files from unauthorized modifications.	x	x	GCP 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	GCP 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	GCP 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	GCP 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	Google is responsible for controlling access, logging and monitoring of the systems and infrastructure underlying GCP in compliance with this requirement.

			monitor their GCE and GKE systems and instances in alignment with PCI DSS requirements.	monitor their GCE and GKE systems and instances in alignment with PCI DSS requirements.	monitor their GCE and GKE systems and instances in alignment with PCI DSS requirements.	monitor their GCE and GKE systems and instances in alignment with PCI DSS requirements.	
10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter.	x	x	GCP 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 GCE and GKE systems and instances in alignment with PCI DSS requirements.	GCP 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 GCE and GKE systems and instances in alignment with PCI DSS requirements.	GCP 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 GCE and GKE systems and instances in alignment with PCI DSS requirements.	GCP 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 GCE and GKE systems and 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.
10.5.4 Write logs for external-facing technologies onto a secure, centralized, internal log server or media device.	x	x	GCP 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 GCE and GKE systems and instances in alignment with PCI DSS requirements.	GCP 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 GCE and GKE systems and instances in alignment with PCI DSS requirements.	GCP 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 GCE and GKE systems and instances in alignment with PCI DSS requirements.	GCP 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 GCE and GKE systems and 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.
10.5.5 Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).	x	x	GCP 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 GCE and GKE systems and instances in alignment with PCI DSS requirements.	GCP 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 GCE and GKE systems and instances in alignment with PCI DSS requirements.	GCP 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 GCE and GKE systems and instances in alignment with PCI DSS requirements.	GCP 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 GCE and GKE systems and 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 Review logs and security events for all system components to identify anomalies or suspicious activity. ***Note:*** *Log harvesting, parsing, and alerting tools may be used to meet this Requirement.*	x	x	GCP customers are responsible for review (automated or manual) of audit logs, and for logging and monitoring their systems leveraging GCE, GKE services within their VPCs in alignment with PCI DSS requirements.	GCP customers are responsible for review (automated or manual) of audit logs, and for logging and monitoring their systems leveraging GCE, GKE services within their VPCs in alignment with PCI DSS requirements.	GCP customers are responsible for review (automated or manual) of audit logs, and for logging and monitoring their systems leveraging GCE, GKE services within their VPCs in alignment with PCI DSS requirements.	GCP customers are responsible for review (automated or manual) of audit logs, and for logging and monitoring their systems leveraging GCE, GKE services within their VPCs 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 Review the following at least 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, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS),	x	x	GCP customers are responsible for review (automated or manual) of audit logs, and for logging and monitoring their systems leveraging GCE, GKE services within their VPCs in alignment with PCI DSS requirements.	GCP customers are responsible for review (automated or manual) of audit logs, and for logging and monitoring their systems leveraging GCE, GKE services within their VPCs in alignment with PCI DSS requirements.	GCP customers are responsible for review (automated or manual) of audit logs, and for logging and monitoring their systems leveraging GCE, GKE services within their VPCs in alignment with PCI DSS requirements.	GCP customers are responsible for review (automated or manual) of audit logs, and for logging and monitoring their systems leveraging GCE, GKE services within their VPCs 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.

authentication servers, e-commerce redirection servers, etc.).							
10.6.2 Review logs of all other system components periodically based on the organization's policies and risk management strategy, as determined by the organization's annual risk assessment.	x	x	GCP customers are responsible for review (automated or manual) of audit logs, and for logging and monitoring their systems leveraging GCE, GKE services within their VPCs in alignment with PCI DSS requirements.	GCP customers are responsible for review (automated or manual) of audit logs, and for logging and monitoring their systems leveraging GCE, GKE services within their VPCs in alignment with PCI DSS requirements.	GCP customers are responsible for review (automated or manual) of audit logs, and for logging and monitoring their systems leveraging GCE, GKE services within their VPCs in alignment with PCI DSS requirements.	GCP customers are responsible for review (automated or manual) of audit logs, and for logging and monitoring their systems leveraging GCE, GKE services within their VPCs 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.
10.6.3 Follow up exceptions and anomalies identified during the review process.	x	x	GCP customers are responsible for review (automated or manual) of audit logs, and for logging and monitoring their systems leveraging GCE, GKE services within their VPCs in alignment with PCI DSS requirements.	GCP customers are responsible for review (automated or manual) of audit logs, and for logging and monitoring their systems leveraging GCE, GKE services within their VPCs in alignment with PCI DSS requirements.	GCP customers are responsible for review (automated or manual) of audit logs, and for logging and monitoring their systems leveraging GCE, GKE services within their VPCs in alignment with PCI DSS requirements.	GCP customers are responsible for review (automated or manual) of audit logs, and for logging and monitoring their systems leveraging GCE, GKE services within their VPCs 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.
10.7 Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup).	x	x	GCP customers are responsible for review (automated or manual) of audit logs, and for logging and monitoring their systems leveraging GCE, GKE services within their VPCs in alignment with PCI DSS requirements.	GCP customers are responsible for review (automated or manual) of audit logs, and for logging and monitoring their systems leveraging GCE, GKE services within their VPCs in alignment with PCI DSS requirements.	GCP customers are responsible for review (automated or manual) of audit logs, and for logging and monitoring their systems leveraging GCE, GKE services within their VPCs in alignment with PCI DSS requirements.	GCP customers are responsible for review (automated or manual) of audit logs, and for logging and monitoring their systems leveraging GCE, GKE services within their VPCs 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.
10.8 Additional requirement for service providers only: Implement a process for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of: • Firewalls • IDS/IPS • FIM • Anti-virus • Physical access controls • Logical access controls • Audit logging mechanisms • Segmentation controls (if used)	x	x	GCP customers are responsible for ensuring a process is implemented for timely detection and reporting of failures of critical security control systems.	GCP customers are responsible for ensuring a process is implemented for timely detection and reporting of failures of critical security control systems.	GCP customers are responsible for ensuring a process is implemented for timely detection and reporting of failures of critical security control systems.	GCP customers are responsible for ensuring a process is implemented for timely detection and reporting of failures of critical security control systems.	Google is responsible for controlling access, logging and monitoring of the systems and infrastructure underlying GCP in compliance with this requirement.
10.8.1 Additional requirement for service providers only: Respond to failures of any critical security controls in a timely manner. Processes for responding to failures in security controls must include: • Restoring security functions • Identifying and documenting the duration (date and time start to end) of the security failure • Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause • Identifying and addressing any security issues that arose during the failure • Performing a risk assessment to determine whether further actions are required as a result of the security failure • Implementing controls to prevent cause of failure from reoccurring • Resuming monitoring of security controls	x	x	GCP customers are responsible for ensuring a process is implemented for timely detection and reporting of failures of critical security control systems.	GCP customers are responsible for ensuring a process is implemented for timely detection and reporting of failures of critical security control systems.	GCP customers are responsible for ensuring a process is implemented for timely detection and reporting of failures of critical security control systems.	GCP customers are responsible for ensuring a process is implemented for timely detection and reporting of failures of critical security control systems.	Google is responsible for controlling access, logging and monitoring of the systems and infrastructure underlying GCP in compliance with this requirement.

10.9 Ensure that security policies and operational procedures for monitoring all access to network resources and cardholder data are documented, in use, and known to all affected parties.		x	GCP customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	GCP customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	GCP customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	GCP customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	Not Applicable

			Customers Responsibility Summary				
PCI DSS v3.2.1 Requirements	**GCP**	**Customer**	**Compute** App Engine Bare Metal Compute Engine Cloud Run Preemptible VMs Shielded VMs	**Networking** Cloud Armor Cloud NAT Hybrid Connectivity Network Intelligence Center Network Telemetry Service Directory Traffic Director Virtual Private Cloud (VPC)	**Storage** Archive Storage Cloud Storage Filestore Local SSD Persistent Disk	**Security** Access Transparency Assured Workloads Binary Authorization Chronicle Cloud Asset Inventory Cloud Data Loss Prevention Cloud Key Management Firewalls Secret Manager Security Command Center Shielded VMs VPC Service Controls **Identity and Access** Cloud Identity Identity and Access Management Identity-Aware Proxy Identity Platform Managed Service for Microsoft Active Directory Policy Intelligence Resource Manager Titan Security Key	**Google Responsibility Summary**
Requirement 11: Regularly test security systems and processes.							
11.1 Implement processes to test for the presence of wireless access points (802.11), and detect and identify all authorized and unauthorized wireless access points on a quarterly basis. ***Note:*** *Methods that may be used in the process include but are not limited to wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS.* *Whichever methods are used, they must be sufficient to detect and identify both authorized and unauthorized devices.*	x		Not Applicable	Not Applicable	Not Applicable	Not Applicable	Google is responsible for checking for the presence of unauthorized wireless access points and similar technologies within its own physical environment and in scope networks.
11.1.1 Maintain an inventory of authorized wireless access points including a documented business justification.	x		Not Applicable	Not Applicable	Not Applicable	Not Applicable	Google is responsible for checking for the presence of unauthorized wireless access points and similar technologies within its own physical environment and in scope networks.
11.1.2 Implement incident response procedures in the event unauthorized wireless access points are detected.	x		Not Applicable	Not Applicable	Not Applicable	Not Applicable	Google is responsible for its own incident response procedures for its environment.

11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades). ***Note:*** *Multiple scan reports can be combined for the quarterly scan process to show that all systems were scanned and all applicable vulnerabilities have been addressed. Additional documentation may be required to verify non-remediated vulnerabilities are in the process of being addressed.* *For initial PCI DSS compliance, it is not required that four quarters of passing scans be completed if the assessor verifies 1) the most recent scan result was a passing scan, 2) the entity has documented policies and procedures requiring quarterly scanning, and 3) vulnerabilities noted in the scan results have been corrected as shown in a re-scan(s). For subsequent years after the initial PCI DSS review, four quarters of passing scans must have occurred.*	x	x	GCP customers are responsible for all internal vulnerability scanning, and rescanning as needed for their GCE, GCS, and GKE instances and applications. GCP customers are responsible for all external vulnerability scanning for their GCE, GCS, and GKE instances and applications. (Note: External vulnerability scans should only include the customer endpoints, and not GCP endpoints as they are tested as part of the GCP compliance external vulnerability scans).	GCP customers are responsible for all internal vulnerability scanning, and rescanning as needed for their GCE, GCS, and GKE instances and applications. GCP customers are responsible for all external vulnerability scanning for their GCE, GCS, and GKE instances and applications. (Note: External vulnerability scans should only include the customer endpoints, and not GCP endpoints as they are tested as part of the GCP compliance external vulnerability scans).	GCP customers are responsible for all internal vulnerability scanning, and rescanning as needed for their GCE, GCS, and GKE instances and applications. GCP customers are responsible for all external vulnerability scanning for their GCE, GCS, and GKE instances and applications. (Note: External vulnerability scans should only include the customer endpoints, and not GCP endpoints as they are tested as part of the GCP compliance external vulnerability scans).	GCP customers are responsible for all internal vulnerability scanning, and rescanning as needed for their GCE, GCS, and GKE instances and applications. GCP customers are responsible for all external vulnerability scanning for their GCE, GCS, and GKE instances and applications. (Note: External vulnerability scans should only include the customer endpoints, and not GCP endpoints as they are tested as part of the GCP compliance external vulnerability scans).	Google has PCI DSS compliance responsibility for dedicated internal Google Production and management network systems. Google is also responsible for scanning of Google managed API endpoints and Cloud Load Balancer IP addresses.
11.2.1 Perform quarterly internal vulnerability scans, and rescans as needed, until all "high-risk" vulnerabilities (as identified in Requirement 6.1) are resolved. Scans must be performed by qualified personnel.	x	x	GCP customers are responsible for all internal vulnerability scanning for their GCE, GCS, and GKE instances and applications.	GCP customers are responsible for all internal vulnerability scanning for their GCE, GCS, and GKE instances and applications.	GCP customers are responsible for all internal vulnerability scanning for their GCE, GCS, and GKE instances and applications.	GCP customers are responsible for all internal vulnerability scanning for their GCE, GCS, and GKE instances and applications.	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.
11.2.2 Perform quarterly external vulnerability scans, via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC). Perform rescans as needed, until passing scans are achieved. ***Note:*** *Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC).* *Refer to the ASV Program Guide published on the PCI SSC website for scan customer responsibilities, scan preparation, etc.*	x	x	GCP customers are responsible for all external vulnerability scanning for their GCE, GCS, and GKE instances and applications. (Note: External vulnerability scans should only include the customer endpoints, and not GCP endpoints as they are tested as part of the GCP compliance external vulnerability scans).	GCP customers are responsible for all external vulnerability scanning for their GCE, GCS, and GKE instances and applications. (Note: External vulnerability scans should only include the customer endpoints, and not GCP endpoints as they are tested as part of the GCP compliance external vulnerability scans).	GCP customers are responsible for all external vulnerability scanning for their GCE, GCS, and GKE instances and applications. (Note: External vulnerability scans should only include the customer endpoints, and not GCP endpoints as they are tested as part of the GCP compliance external vulnerability scans).	GCP customers are responsible for all external vulnerability scanning for their GCE, GCS, and GKE instances and applications. (Note: External vulnerability scans should only include the customer endpoints, and not GCP endpoints as they are tested as part of the GCP compliance external vulnerability scans).	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.
11.2.3 Perform internal and external scans, and rescans as needed, after any significant change. Scans must be performed by qualified personnel.	x	x	GCP customers are responsible for all internal vulnerability scanning, and rescanning as needed for their GCE, GCS, and GKE instances and applications. GCP customers are responsible for all external vulnerability scanning for their GCE, GCS, and GKE	GCP customers are responsible for all internal vulnerability scanning, and rescanning as needed for their GCE, GCS, and GKE instances and applications. GCP customers are responsible for all external vulnerability scanning for their GCE, GCS, and GKE instances and applications. (Note: External vulnerability	GCP customers are responsible for all internal vulnerability scanning, and rescanning as needed for their GCE, GCS, and GKE instances and applications. GCP customers are responsible for all external vulnerability scanning for their GCE, GCS, and GKE instances and applications. (Note: External vulnerability scans	GCP customers are responsible for all internal vulnerability scanning, and rescanning as needed for their GCE, GCS, and GKE instances and applications. GCP customers are responsible for all external vulnerability scanning for their GCE, GCS, and GKE instances and applications. (Note: External vulnerability scans should only include the customer endpoints, and not GCP endpoints as they are tested as part of the GCP	Google is responsible for conducting quarterly internal and 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.

			instances and applications. (Note: External vulnerability scans should only include the customer endpoints, and not GCP endpoints as they are tested as part of the GCP compliance external vulnerability scans).	scans should only include the customer endpoints, and not GCP endpoints as they are tested as part of the GCP compliance external vulnerability scans).	should only include the customer endpoints, and not GCP endpoints as they are tested as part of the GCP compliance external vulnerability scans).	compliance external vulnerability scans).	
11.3 Implement a methodology for penetration testing that includes at least the following: • Is based on industry-accepted penetration testing approaches (for example, NIST SP800-115). • Includes coverage for the entire CDE perimeter and critical systems. • Includes testing from both inside and outside of the network. • Includes testing to validate any segmentation and scope reduction controls. • Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5. • Defines network-layer penetration tests to include components that support network functions as well as operating systems. • Includes review and consideration of threats and vulnerabilities experienced in the last 12 months. • Specifies retention of penetration testing results and remediation activities results.	x	x	GCP customers are responsible for all internal and external penetration testing for their GCE, GCS, and GKE instances and applications comprising their CDE. (Note: External penetration tests should include customer endpoints only as GCP endpoints are included as part of its annual compliance, and external penetration tests).	GCP customers are responsible for all internal and external penetration testing for their GCE, GCS, and GKE instances and applications comprising their CDE. (Note: External penetration tests should include customer endpoints only as GCP endpoints are included as part of its annual compliance, and external penetration tests).	GCP customers are responsible for all internal and external penetration testing for their GCE, GCS, and GKE instances and applications comprising their CDE. (Note: External penetration tests should include customer endpoints only as GCP endpoints are included as part of its annual compliance, and external penetration tests).	GCP customers are responsible for all internal and external penetration testing for their GCE, GCS, and GKE instances and applications comprising their CDE. (Note: External penetration tests should include customer endpoints only as GCP endpoints are included as part of its annual compliance, and external penetration tests).	Google is responsible for conducting internal and 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.
11.3.1 Perform **external** penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).	x	x	GCP customers are responsible for all external penetration testing for their GCE, GCS, and GKE instances and applications comprising their CDE. (Note: External penetration tests should include customer endpoints only as GCP endpoints are included as part of its annual compliance, and external penetration tests).	GCP customers are responsible for all external penetration testing for their GCE, GCS, and GKE instances and applications comprising their CDE. (Note: External penetration tests should include customer endpoints only as GCP endpoints are included as part of its annual compliance, and external penetration tests).	GCP customers are responsible for all external penetration testing for their GCE, GCS, and GKE instances and applications comprising their CDE. (Note: External penetration tests should include customer endpoints only as GCP endpoints are included as part of its annual compliance, and external penetration tests).	GCP customers are responsible for all external penetration testing for their GCE, GCS, and GKE instances and applications comprising their CDE. (Note: External penetration tests should include customer endpoints only as GCP endpoints are included as part of its annual compliance, and external penetration tests).	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.
11.3.2 Perform **internal** penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).	x	x	GCP customers are responsible for all internal penetration testing for their GCE, GCS, and GKE instances and applications comprising their CDE.	GCP customers are responsible for all internal penetration testing for their GCE, GCS, and GKE instances and applications comprising their CDE.	GCP customers are responsible for all internal penetration testing for their GCE, GCS, and GKE instances and applications comprising their CDE.	GCP customers are responsible for all internal penetration testing for their GCE, GCS, and GKE instances and applications comprising their CDE.	Google is responsible for conducting internal penetration testing on systems and infrastructure underlying GCP.

11.3.3 Exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the corrections.	x	x	GCP customers are responsible for all internal and external penetration testing for their GCE, GCS, and GKE instances and applications comprising their CDE. (Note: External penetration tests should include customer endpoints only as GCP endpoints are included as part of its annual compliance, and external penetration tests).	GCP customers are responsible for all internal and external penetration testing for their GCE, GCS, and GKE instances and applications comprising their CDE. (Note: External penetration tests should include customer endpoints only as GCP endpoints are included as part of its annual compliance, and external penetration tests).	GCP customers are responsible for all internal and external penetration testing for their GCE, GCS, and GKE instances and applications comprising their CDE. (Note: External penetration tests should include customer endpoints only as GCP endpoints are included as part of its annual compliance, and external penetration tests).	GCP customers are responsible for all internal and external penetration testing for their GCE, GCS, and GKE instances and applications comprising their CDE. (Note: External penetration tests should include customer endpoints only as GCP endpoints are included as part of its annual compliance, and external penetration tests).	Google is responsible for conducting internal and external penetration testing on systems and infrastructure underlying GCP.
11.3.4 If segmentation is used to isolate the CDE from other networks, perform penetration tests at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE.	x	x	GCP customers are responsible for confirming PCI DSS scope by performing penetration testing on segmentation controls at least every six months and after any changes to segmentation controls/methods for their GCE, GCS, and GKE instances and applications.	GCP customers are responsible for confirming PCI DSS scope by performing penetration testing on segmentation controls at least every six months and after any changes to segmentation controls/methods for their GCE, GCS, and GKE instances and applications.	GCP customers are responsible for confirming PCI DSS scope by performing penetration testing on segmentation controls at least every six months and after any changes to segmentation controls/methods for their GCE, GCS, and GKE instances and applications.	GCP customers are responsible for confirming PCI DSS scope by performing penetration testing on segmentation controls at least every six months and after any changes to segmentation controls/methods for their GCE, GCS, and GKE instances and applications.	Google is responsible for conducting segmentation penetration testing on systems and infrastructure underlying GCP.
11.3.4.1 Additional requirement for service providers only: If segmentation is used, confirm PCI DSS scope by performing penetration testing on segmentation controls at least every six months and after any changes to segmentation controls/methods.	x	x	GCP customers are responsible for confirming PCI DSS scope by performing penetration testing on segmentation controls at least every six months and after any changes to segmentation controls/methods for their GCE, GCS, and GKE instances and applications.	GCP customers are responsible for confirming PCI DSS scope by performing penetration testing on segmentation controls at least every six months and after any changes to segmentation controls/methods for their GCE, GCS, and GKE instances and applications.	GCP customers are responsible for confirming PCI DSS scope by performing penetration testing on segmentation controls at least every six months and after any changes to segmentation controls/methods for their GCE, GCS, and GKE instances and applications.	GCP customers are responsible for confirming PCI DSS scope by performing penetration testing on segmentation controls at least every six months and after any changes to segmentation controls/methods for their GCE, GCS, and GKE instances and applications.	Google is responsible for conducting segmentation penetration testing on systems and infrastructure underlying GCP.
11.4 Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up to date.	x	x	GCP customers are responsible for implementing IDS functionality, typically using Host-based IDS (HIDS), for network segments they implement and manage.	GCP customers are responsible for implementing IDS functionality, typically using Host-based IDS (HIDS), for network segments they implement and manage.	GCP customers are responsible for implementing IDS functionality, typically using Host-based IDS (HIDS), for network segments they implement and manage.	GCP customers are responsible for implementing IDS functionality, 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 Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly. ***Note:*** *For change-detection purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. Change-detection mechanisms such as file-integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is, the merchant or service provider).*	x	x	GCP customers are responsible for file integrity monitoring for their GCE, GCS, and GKE instances and applications.	GCP customers are responsible for file integrity monitoring for their GCE, GCS, and GKE instances and applications.	GCP customers are responsible for file integrity monitoring for their GCE, GCS, and GKE instances and applications.	GCP customers are responsible for file integrity monitoring for their GCE, GCS, and GKE instances and applications.	Google is responsible for change-detection mechanisms on the systems and infrastructure underlying GCP in compliance with this requirement.
11.5.1 Implement a process to respond to any alerts generated by the change-detection solution.	x	x	GCP customers are responsible for file integrity monitoring for their GCE, GCS, and GKE instances and applications.	GCP customers are responsible for file integrity monitoring for their GCE, GCS, and GKE instances and applications.	GCP customers are responsible for file integrity monitoring for their GCE, GCS, and GKE instances and applications.	GCP customers are responsible for file integrity monitoring for their GCE, GCS, and GKE instances and applications.	Google is responsible for change-detection mechanisms on the systems and infrastructure underlying GCP in compliance with this requirement.
11.6 Ensure that security policies and operational procedures for security monitoring and testing are documented, in use, and known to all affected parties.		x	GCP customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	GCP customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	GCP customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	GCP customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	Not Applicable

			Customers Responsibility Summary				
PCI DSS v3.2.1 Requirements	**GCP**	**Customer**	**Compute** App Engine Bare Metal Compute Engine Cloud Run Preemptible VMs Shielded VMs	**Networking** Cloud Armor Cloud NAT Hybrid Connectivity Network Intelligence Center Network Telemetry Service Directory Traffic Director Virtual Private Cloud (VPC)	**Storage** Archive Storage Cloud Storage Filestore Local SSD Persistent Disk	**Security** Access Transparency Assured Workloads Binary Authorization Chronicle Cloud Asset Inventory Cloud Data Loss Prevention Cloud Key Management Firewalls Secret Manager Security Command Center Shielded VMs VPC Service Controls **Identity and Access** Cloud Identity Identity and Access Management Identity-Aware Proxy Identity Platform Managed Service for Microsoft Active Directory Policy Intelligence Resource Manager Titan Security Key	**Google Responsibility Summary**
Requirement 12: Maintain a policy that addresses information security for all personnel.							
12.1 Establish, publish, maintain, and disseminate a security policy.		x	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	Not Applicable
12.1.1 Review the security policy at least annually and update the policy when the environment changes.		x	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	Not Applicable
12.2 Implement a risk-assessment process that: - Is performed at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.), - Identifies critical assets, threats, and vulnerabilities, and - Results in a formal, documented analysis of risk. Examples of risk-assessment methodologies include but are not limited to OCTAVE, ISO 27005 and NIST SP 800-30.		x	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	Not Applicable

12.3 Develop usage policies for critical technologies and define proper use of these technologies. *Note: Examples of critical technologies include, but are not limited to, remote access and wireless technologies, laptops, tablets, removable electronic media, e-mail usage and Internet usage.* Ensure these usage policies require the following:		x	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	Not Applicable
12.3.1 Explicit approval by authorized parties		x	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	Not Applicable
12.3.2 Authentication for use of the technology		x	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	Not Applicable
12.3.3 A list of all such devices and personnel with access		x	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	Not Applicable
12.3.4 A method to accurately and readily determine owner, contact information, and purpose (for example, labeling, coding, and/or inventorying of devices)		x	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	Not Applicable
12.3.5 Acceptable uses of the technology		x	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	Not Applicable
12.3.6 Acceptable network locations for the technologies		x	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	Not Applicable
12.3.7 List of company-approved products		x	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	Not Applicable
12.3.8 Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity		x	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	Not Applicable

12.3.9 Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use		x	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	Not Applicable
12.3.10 For personnel accessing cardholder data via remote-access technologies, prohibit the copying, moving, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need. Where there is an authorized business need, the usage policies must require the data be protected in accordance with all applicable PCI DSS Requirements.		x	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	Not Applicable
12.4 Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.		x	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	Not Applicable
12.4.1 Additional requirement for service providers only: Executive management shall establish responsibility 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		x	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	Not Applicable
12.5 Assign to an individual or team the following information security management responsibilities:		x	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	Not Applicable
12.5.1 Establish, document, and distribute security policies and procedures.		x	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	Not Applicable
12.5.2 Monitor and analyze security alerts and information, and distribute to appropriate personnel.		x	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	Not Applicable
12.5.3 Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.		x	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	Not Applicable
12.5.4 Administer user accounts, including additions, deletions, and modifications.		x	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	Not Applicable

12.5.5 Monitor and control all access to data.		x	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	Not Applicable
12.6 Implement a formal security awareness program to make all personnel aware of the importance of cardholder data security policy and procedures.		x	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	Not Applicable
12.6.1 Educate personnel upon hire and at least annually. *Note: Methods can vary depending on the role of the personnel and their level of access to the cardholder data.*		x	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	Not Applicable
12.6.2 Require personnel to acknowledge at least annually that they have read and understood the security policy and procedures.		x	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	Not Applicable
12.7 Screen potential personnel prior to hire to minimize the risk of attacks from internal sources. (Examples of background checks include previous employment history, criminal record, credit history, and reference checks.) *Note: For those potential personnel to be hired for certain positions such as store cashiers who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only.*		x	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	Not Applicable
12.8 Maintain and implement policies and procedures to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data, as follows:		x	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	Not Applicable
12.8.1 Maintain a list of service providers including a description of the service provided.		x	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	Not Applicable
12.8.2 Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment. *Note: The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to*		x	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	Not Applicable

each party. The acknowledgement does not have to include the exact wording provided in this requirement.							
12.8.3 Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.		x	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	Not Applicable
12.8.4 Maintain a program to monitor service providers' PCI DSS compliance status at least annually.		x	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	Not Applicable
12.8.5 Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.		x	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	Not Applicable
12.9 Additional requirement for service providers only: Service providers acknowledge in writing to customers that they are responsible for the security of cardholder data the service provider possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment. *Note: The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgement does not have to include the exact wording provided in this requirement.*		x	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	Not Applicable
12.10 Implement an incident response plan. Be prepared to respond immediately to a system breach.		x	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	Not Applicable
12.10.1 Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum: - Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum - Specific incident response procedures - Business recovery and continuity procedures - Data backup processes - Analysis of legal requirements for reporting compromises - Coverage and responses of all critical system components - Reference or inclusion of incident response procedures from the payment brands.		x	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	Not Applicable

12.10.2 Review and test the plan, including all elements listed in Requirement 12.10.1, at least annually.		x	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	Not Applicable
12.10.3 Designate specific personnel to be available on a 24/7 basis to respond to alerts.		x	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	Not Applicable
12.10.4 Provide appropriate training to staff with security breach response responsibilities.		x	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	Not Applicable
12.10.5 Include alerts from security monitoring systems, including but not limited to intrusion-detection, intrusion-prevention, firewalls, and file-integrity monitoring systems.		x	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	Not Applicable
12.10.6 Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.		x	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	Not Applicable
12.11 Additional requirement for service providers only: Perform reviews at least quarterly to confirm personnel are following security policies and operational procedures. Reviews must cover the following processes: - Daily log reviews - Firewall rule-set reviews - Applying configuration standards to new systems - Responding to security alerts - Change management processes		x	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	Not Applicable
12.11.1 Additional requirement for service providers only: Maintain documentation of quarterly review process to include: - Documenting results of the reviews - Review and sign-off of results by personnel assigned responsibility for the PCI DSS compliance program		x	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	GCP customers are responsible to maintain policies and processes applicable to their cardholder data environment to maintain compliance with the PCI Data Security Standards.	Not Applicable

Appendix

Additional Requirements for Entities using SSL/early TLS

Requirement	PCI-DSS Requirement	Additional Customer Responsibility
A2.1	Where POS POI terminals (and the SSL/TLS termination points to which they connect) use SSL and/or early TLS, the entity must either: Confirm the devices are not susceptible to any known exploits for those protocols. ***Or:*** Have a formal Risk Mitigation and Migration Plan in place.	N/A no POS/POI devices in scope.
A2.2	Entities with existing implementations (other than as allowed in A.2.1) that use SSL and/or early TLS must have a formal Risk Mitigation and Migration Plan in place.	GCP customers are responsible for complying with this requirement for any virtual machines, applications, services or databases deployed by them on GCP.
A2.3	***Additional Requirement for Service Providers Only:*** All service providers must provide a secure service offering by June 30, 2016.	Google has implemented controls for secure administrative access for the Google production infrastructure underlying GCP
		GCP Customers are responsible for configuring their apps hosted on Google Cloud Platform such that it doesn't accept TLS1.0 requests from their app users. Example: Connections between Customer Instances and End-User
		GCP Customers wishing to disable 3DES or TLS 1.0 for web-based access to the covered services will need to file a support case referencing issue #73300651 and requesting 3DES or TLS 1.0 be disabled for their managed accounts. Google will then apply a policy to user accounts managed under the applicable GCP domain preventing sign in when the user is on a connection using 3DES or TLS 1.0. Example: Connections between Customer administrators and Google's Cloud Console
		GCP customers are responsible for configuring their clients to disallow connections via TLS 1.0 Example: Connections between Customer and their third-parties.

Product Specific Customer Considerations

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