PCI 3DS Responsibility Summary

Google Cloud

6/17/2024

Definitions	
Term	**Description**
Google	The service provider
GCP	Google Cloud Platform
GCI	Google Cloud Infrastructure
PCI DSS	Payment Card Industry Data Security Standard
3DS	3-D Secure
ACS	Access Control Server
DS	Directory Server
3DSS	3DS Server
CDE	Cardholder Data Environment
3DE	3-D Secure Environment
HSM	Hardware Security Module
AOC	Attestation of Compliance
ROC	Report on Compliance
MFA	Multi-factor authentication
PED	PIN Entry Device

PCI 3DS RESPONSIBILITY

Google Cloud Platform (GCP) provides coverage for part of the PCI 3DS controls as a third-party service provider, and has demonstrated compliance for applicable requirements as evidenced in its published GCP 3DS AOC. PCI 3DS customers utilizing the GCP environment and services are responsible for implementing all applicable PCI 3DS controls in accordance with the PCI 3DS program requirements, and evidencing their own PCI 3DS compliance as required by the card brands where applicable. In conjunction with the GCP 3DS AOC, this responsibility summary provides additional clarification on the controls and responsibilties for applicable PCI 3DS controls. Some PCI 3DS requirements may be satisfied by the customer's use of GCP products, but most requirements are either shared responsibilities between the GCP customer and GCP, or entirely the customer's responsibility. The following two sections describe the responsibilities that GCP assumes for the products offered and the customer's responsibilities when utilizing the in-scope GCP products.

PCI 3DS Part 1: 3DS Baseline Security Requirements

• GCP has been assessed to PCI DSS as a third-party service provider (TPSP), and the GCP PCI DSS AOC and GCI PCI DSS AOC documents may be leveraged to satisfies portions of the customer's own PCI DSS ROC or 3DS Part 1 requirements, as allowed by the PCI 3DS program guidance.

• The customer is responsible for validation of PCI DSS for their CDE and/or PCI 3DS Part 1 for their own PCI 3DE in accordance with PCI 3DS program. For portions of the customer's 3DE that are fully hosted within GCP, please refer to the latest GCP PCI DSS Attestation of Compliance (AOC) and GCP PCI DSS responsibility matrix for guidance on customer responsibilities for meeting PCI DSS and/or PCI 3DS Part 1 controls for in-scope products. The applicable products may require specific configurations, connectivity and architecture considerations to implement in a PCI DSS / 3DS compliant manner. For any portion of the customer's CDE / 3DE that is hosted outside of GCP, the customer is fully responsible for all applicable controls under PCI DSS and/or PCI 3DS Part 1.

PCI 3DS Part 2: Security requirements to protect 3DS data and processes

• GCP has been assessed to PCI 3DS as a third-party service provider (TPSP), and the GCP PCI 3DS AOC document may be leveraged to satisfies portions of the customer's own 3DS Part 2 requirements, as allowed by the PCI 3DS program guidance.

• The Requirements sections of this document identify whether responsibility for each control falls to GCP, the Customer, or is Shared. The Summary section for each requirement provides further details on how these responsibilities may be understood based on the customer's specific implementation and products in use. Customers that host any portion of their PCI 3DE in GCP may refer to the PCI 3DS products in scope tab and tables within this GCP 3DS responsibility matrix to understand responsibilities for ensuring products are included in this analysis for PCI 3DS Part 2 controls. The applicable products may require specific configurations, connectivity and architecture considerations to implement the products in a PCI 3DS compliant manner. For any portion of the customer's 3DE that is hosted outside of GCP, the customer is fully responsible for all applicable controls under PCI 3DS Part 2.

List of Products In Scope	Product Details
Access Approval	Access Approval allows customers to approve eligible manual, targeted accesses by Google administrators to their data or workloads before those accesses happen.
Access Context Manager	Access Context Manager allows Google Cloud organization administrators to define fine-grained, attribute based access control for projects, apps and resources.
Access Transparency	Access Transparency captures near real-time logs of manual, targeted accesses by Google administrators, and serves them to customers via their Cloud Logging account.
Advanced API Security	API Security acts as your API's vigilant guardian. It constantly analyzes incoming traffic, seeking out anomalous patterns that might indicate attacks or abuse. When suspicious activity is spotted, it can block harmful requests or alert you for further action. Additionally, it evaluates your API setups against security best practices, offering recommendations for improvement. This comprehensive approach helps you proactively safeguard your APIs, protect sensitive data, and ensure your API configurations are designed to withstand security challenges.
Agent Assist	Agent Assist is an LLM-powered AI solution that increases human agent productivity and enhances customer service by offering real-time assistance.
AI Platform Deep Learning Container	Deep Learning VM and Container provides virtual machine and Docker images with AI frameworks that can be customized and used with Google Kubernetes Engine (GKE), Vertex AI, Cloud Run, Compute Engine, Kubernetes, and Docker Swarm.
AI Platform Training and Prediction	AI Platform Training and Prediction is a managed service that enables you to easily build and use machine learning models. It provides scalable training and prediction services that work on large scale datasets.
AlloyDB	AlloyDB is a fully managed PostgreSQL-compatible database service for most demanding enterprise workloads. AlloyDB combines with PostgreSQL, for superior performance, scale, and availability
Anti-Money Laundering AI	AML AI enhances financial institutions' legacy transaction monitoring systems with an AI-powered risk score to improve financial crime risk detection.
API Gateway	API Gateway is a fully-managed service that helps you develop, deploy, and secure your APIs running on Google Cloud Platform.
Apigee	Apigee is a full-lifecycle API management platform that lets customers design, secure, analyze, and scale APIs, giving them visibility and control. Apigee is available as Apigee, a fully-managed service, Apigee hybrid, a hybrid model that's partially hosted and managed by the customer, or Apigee Private Cloud, an entirely customer hosted Premium Software solution.
App Engine	App Engine enables you to build and host applications on the same systems that power Google applications. App Engine offers fast development and deployment; simple administration, with no need to worry about hardware, patches or backups; and effortless scalability.
Application Integration	Application Integration is an Integration-Platform-as-a-Service (iPaaS) that offers a comprehensive set of integration tools to connect and manage the multitude of applications and data required to support various business operations. Application Integration provides a unified drag and drop integration designer interface, triggers that help invoke an integration, configurable tasks and numerous connectors that allow connectivity to business applications, technologies, and other data sources using the native protocols of each target application.
Artifact Analysis	Artifact Analysis is a family of services that provide software composition analysis, metadata storage and retrieval. Its detection points are built into a number of Google Cloud products such as Artifact Registry and Google Kubernetes Engine (GKE) for quick enablement. The service works with both Google Cloud's first-party products and also lets customers store information from third-party sources. The scanning services leverage a common vulnerability store for matching files against known vulnerabilities.
Artifact Registry	Artifact Registry is a service for managing container images and packages. It is integrated with Google Cloud tooling and runtimes and comes with support for native artifact protocols. This makes it simple to integrate it with your CI/CD tooling to set up automated pipelines.
Assured Workloads	Assured Workloads provides functionality to create security controls that are enforced on your cloud environment. These security controls can assist with your compliance requirements (for example, FedRAMP Moderate).
AutoML Natural Language	AutoML Natural Language enables customers to categorize input text into their own custom defined labels (supervised classification). Users can customize models to their own domain or use case.
AutoML Tables	AutoML Tables enables your entire team of data scientists, analysts, and developers to automatically build and deploy state-of-the-art machine learning models on structured data at increased speed and scale.
AutoML Translation	AutoML Translation is a simple and scalable translation solution that allows businesses and developers with limited machine learning expertise to customize the Google Neural Machine Translation (GNMT) model for their own domain or use-case.
AutoML Video	AutoML Video is a simple and flexible machine learning service that lets businesses and developers easily train custom and scalable video models for their own domain or use cases.

List of Products In Scope	Product Details
AutoML Vision	AutoML Vision is a simple and flexible machine learning service that lets businesses and developers with limited machine learning expertise train custom and scalable vision models for their own use cases.
Backup for GKE	Backup for GKE enables data protection for workloads running in Google Kubernetes Engine clusters.
Bare Metal HSM	Bare Metal HSM is an infrastructure-as-a-service offering that lets you deploy customer-owned hardware security modules (HSMs) next to your Google Cloud workloads. Google hosts customer HSMs, providing physical and network security, rack space, power, and network integration for a monthly fee.
Bare Metal Rack HSM	Bare Metal Rack HSM is an infrastructure-as-a-service offering that lets you deploy dedicated racks of customer-owned hardware security modules (HSMs) next to your Google Cloud workloads. Google hosts customer HSMs, providing physical and network security, rack space, power, and network integration for a monthly fee.
Batch	Batch is a fully-managed service that allows you to create batch jobs at scale. The service dynamically provisions certain Google Cloud resources, schedules your batch job on the resources, manages the queue for the job, and executes the job. Batch is natively integrated with Google Cloud services for storage, logging, monitoring, and more.
BeyondCorp Enterprise	BeyondCorp Enterprise is a solution designed to enable zero-trust application access to enterprise users and protect enterprises from data leakage, malware and phishing attacks. BeyondCorp Enterprise is an integrated platform incorporating cloud-based services and software components, including:
BigQuery	BigQuery is a fully-managed data analysis service that enables businesses to analyze Big Data. It features highly scalable data storage that accommodates up to hundreds of terabytes, the ability to perform ad hoc queries on multi-terabyte datasets, and the ability to share data insights via the web.
BigQuery Data Transfer Service	BigQuery Data Transfer Service automates data movement from SaaS applications to BigQuery on a scheduled, managed basis. With the BigQuery Data Transfer Service, you can transfer data to BigQuery from SaaS applications including Google Ads, Campaign Manager, Google Ad Manager, and YouTube.
Binary Authorization	Binary Authorization helps customers ensure that only signed and explicitly-authorized workload artifacts are deployed to their production environments. It offers tools for customers to formalize and codify secure supply chain policies for their organizations.
CCAI Platform	CCAI Platform is an AI-driven Contact Center as a Service (CCaaS) platform that is built natively on Google Cloud and uses the other Google Cloud Contact Center AI (CCAI) products at its core. CCAI Platform is purpose-built to work alongside CRMs. It provides organizations with a single source of truth for their customer journeys. CCAI Platform is a unified contact center platform that accelerates the organization's ability to leverage and deploy CCAI without relying on multiple technology providers.
Certificate Authority Service	Certificate Authority Service is a cloud-hosted certificate issuance service that lets customers issue and manage certificates for their cloud or on-premises workloads. Certificate Authority Service can be used to create certificate authorities using Cloud KMS keys to issue, revoke, and renew subordinate and end-entity certificates.
Certificate Manager	Certificate Manager provides a central place for customers to control where certificates are used and how to obtain certificates, and to see the state of the certificates.
Chronicle SIEM	Chronicle SIEM is a cloud service, built as a specialized layer on top of core Google infrastructure, designed for enterprises to privately retain, analyze, and search the massive amounts of security and network telemetry they generate. Chronicle normalizes, indexes, correlates, and analyzes the data to provide instant analysis and context on risky activity.
Cloud Asset Inventory	Cloud Asset Inventory is an inventory of cloud assets with history. It enables users to export cloud resource metadata at a given timestamp or cloud resource metadata history within a time window.
Cloud Bigtable	Cloud Bigtable is a fast, fully-managed, highly-scalable NoSQL database service. It is designed for the collection and retention of data from 1TB to hundreds of PB.
Cloud Billing	Cloud Billing provides methods to programmatically manage billing for projects on the Google Cloud Platform.
Cloud Build	Cloud Build is a service that executes your builds on Google Cloud Platform infrastructure. Cloud Build can import source code from Cloud Storage, Cloud Source Repositories, GitHub, or Bitbucket; execute a build to your specifications; and produce artifacts such as Docker containers or Java archives.
Cloud CDN	Cloud CDN uses Google's globally distributed edge points of presence to cache HTTP(S) load balanced content close to your users.
Cloud Composer	Cloud Composer is a managed workflow orchestration service that can be used to author, schedule, and monitor pipelines that span across clouds and on-premises data centers. Cloud Composer allows you to use Apache Airflow without the hassle of creating and managing complex Airflow infrastructure.
Cloud Console	Cloud Console is a web-based interface used to build, modify, and manage services and resources on the Google Cloud Platform. Cloud services can be procured, configured, and run from Cloud Console.
Cloud Console App	Cloud Console App is a native mobile app that enables customers to manage key Google Cloud services. It provides monitoring, alerting, and the ability to take actions on resources.

List of Products In Scope	Product Details
Cloud Data Fusion	Cloud Data Fusion is a fully-managed, cloud native, enterprise data integration service for quickly building and managing data pipelines. Cloud Data Fusion provides a graphical interface to help increase time efficiency and reduce complexity and allows business users, developers, and data scientists to easily and reliably build scalable data integration solutions to cleanse, prepare, blend, transfer, and transform data without having to wrestle with infrastructure.
Cloud Deployment Manager	Cloud Deployment Manager is a hosted configuration tool which allows developers and administrators to provision and manage their infrastructure on Google Cloud Platform. It uses a declarative model which allows users to define or change the resources necessary to run their applications and will then provision and manage those resources.
Cloud DNS	Cloud DNS is a high performance, resilient, global, fully-managed DNS service that provides a RESTful API to publish and manage DNS records for your applications and services.
Cloud Endpoints	Cloud Endpoints is a tool that helps you to develop, deploy, secure and monitor your APIs running on Google Cloud Platform.
Cloud External Key Manager (Cloud EKM)	Cloud EKM lets you encrypt data in Google Cloud Platform with encryption keys that are stored and managed in a third-party key management system deployed outside Google's infrastructure.
Cloud Filestore	Cloud Filestore is a scalable and highly available shared file service fully-managed by Google. Cloud Filestore provides persistent storage ideal for shared workloads. It is best suited for enterprise applications requiring persistent, durable, shared storage which is accessed by NFS or requires a POSIX compliant file system.
Cloud Firewall	Cloud NGFW is a fully distributed, cloud-native firewall service that evaluates incoming and outgoing traffic on a network, according to user-defined firewall policies.
Cloud Functions	Cloud Functions is a lightweight, event-based, asynchronous compute solution that allows you to create small, single-purpose functions that respond to cloud events without the need to manage a server or a runtime environment.
Cloud Functions for Firebase	Cloud Functions for Firebase lets you write code that responds to events and invokes functionality exposed by other Firebase features, once you deploy JavaScript code in a hosted, private, and scalable Node.js environment that requires no maintenance.
Cloud Healthcare	Cloud Healthcare is a fully-managed service to send, receive, store, query, transform, and analyze healthcare and life sciences data and enable advanced insights and operational workflows using highly scalable and compliance-focused infrastructure.
Cloud HSM	Cloud HSM (Hardware Security Module) is a cloud-hosted key management service that lets you protect encryption keys and perform cryptographic operations within a managed HSM service. You can generate, use, rotate, and destroy various symmetric and asymmetric keys.
Cloud Identity	Cloud Identity Services are the services and editions as described at: https://cloud.google.com/terms/identity/user-features.html or such other URL as Google may provide.
Cloud IDS (Cloud Intrusion Detection System)	Cloud IDS is a managed service that aids in detecting certain malware, spyware, command-and-control attacks, and other network-based threats.
Cloud Interconnect	Cloud Interconnect offers enterprise-grade connections to Google Cloud Platform using Google Services for Dedicated Interconnect, Partner Interconnect and Cloud VPN. This solution allows you to directly connect your on-premises network to your Virtual Private Cloud.
Cloud Key Management Service	Cloud Key Management Service is a cloud-hosted key management service that lets you manage cryptographic keys for your cloud services the same way you do on premises. You can generate, use, rotate, and destroy AES256, RSA 2048, RSA 3072, RSA 4096, EC P256, and EC P384 cryptographic keys. *Note: Where referenced within this responsibility summary, Cloud KMS refers to Cloud KMS with protection level SOFTWARE, to distinguish from Cloud HSM protection level HSM.*
Cloud Life Sciences (formerly Google Genomics)	Cloud Life Sciences provides services and tools for managing, processing, and transforming life sciences data.
Cloud Load Balancing	Cloud Load Balancing provides scaling, high availability, and traffic management for your internet-facing and private applications.
Cloud Logging	Cloud Logging is a fully-managed service that performs at scale and can ingest application and system log data, as well as custom log data from thousands of VMs and containers. Cloud Logging allows you to analyze and export selected logs to long-term storage in real time. Cloud Logging includes the Error Reporting feature, which analyzes and aggregates the errors in your cloud applications and notifies you when new errors are detected.
Cloud Monitoring	Cloud Monitoring provides visibility into the performance, uptime, and overall health of cloud-powered applications. Cloud Monitoring collects metrics, events, and metadata from certain Services, hosted uptime probes, application instrumentation, alert management, notifications and a variety of common application components.
Cloud NAT (network address translation)	Cloud NAT enables instances in a private network to communicate with the internet.

List of Products In Scope	Product Details
Cloud Natural Language API	Cloud Natural Language API provides powerful natural language understanding as an easy to use API. This API enables application developers to answer the following questions: 1) What are the entities referred to in the block of text?; 2) What is the sentiment (positive or negative) for this block of text?; 3) What is the language of this block of text?; and 4) What is the syntax for this block of text (including parts of speech and dependency trees)? Users can call this API by passing in a block of text or by referring to a document in Cloud Storage.
Cloud Profiler	Cloud Profiler provides continuous profiling of resource consumption in your production applications, helping you identify and eliminate potential performance issues.
Cloud Router	Cloud Router enables dynamic Border Gateway Protocol (BGP) route updates between your VPC network and your non-Google network.
Cloud Run	Cloud Run (fully-managed) lets you run stateless containers on a fully-managed environment.
Cloud Scheduler	Cloud Scheduler is a fully-managed enterprise-grade cron job scheduler. It allows you to schedule virtually any job, including batch, big data jobs, cloud infrastructure operations, and more. You can automate everything, including retries in case of failure to reduce manual toil and intervention. Cloud Scheduler even acts as a single pane of glass, allowing you to manage all your automation tasks from one place.
Cloud Shell	Cloud Shell is a tool that provides command-line access to cloud resources directly from your browser. You can use Cloud Shell to run experiments, execute Cloud SDK commands, manage projects and resources, and do lightweight software development via the built-in web editor.
Cloud Source Repositories	Cloud Source Repositories provides Git version control to support collaborative development of any application or service, including those that run on App Engine and Compute Engine.
Cloud Spanner	Cloud Spanner is a fully-managed, mission-critical relational database service. It is designed to provide a scalable online transaction processing (OLTP) database with high availability and strong consistency at global scale.
Cloud Speaker ID	Cloud Speaker ID quickly enrolls user's voice print with as little as 10 seconds of audio. Enrollment audio and voice print are stored securely on Google's servers and can even be encrypted with customers own key.
Cloud SQL	Cloud SQL is a web service that allows you to create, configure, and use relational databases that live in Google's cloud. It is a fully-managed service that maintains, manages, and administers your databases, allowing you to focus on your applications and services.
Cloud Storage	Cloud Storage is a RESTful service for storing and accessing your data on Google's infrastructure. The service combines the performance and scalability of Google's cloud with advanced security and sharing capabilities.
Cloud Storage for Firebase	Cloud Storage for Firebase adds customizable Google security (via Firebase Security Rules for Cloud Storage) to file uploads and downloads for your Firebase apps, as well as robust uploads and downloads regardless of network quality through the Firebase SDK. Cloud Storage for Firebase is backed by Cloud Storage, a service for storing and accessing your data on Google's infrastructure.
Cloud Tasks	Cloud Tasks is a fully-managed service that allows you to manage the execution, dispatch, and delivery of a large number of distributed tasks. Using Cloud Tasks, you can perform work asynchronously outside of a user or service-to-service request. Cloud Tasks provides all the benefits of a distributed task queue such as task offloading wherein heavyweight, background and long running processes can be dispatched to a task queue, loose coupling between microservices allowing them to scale independently, and enhanced system reliability as tasks are persisted in storage and retried automatically, making your infrastructure resilient to intermittent failures.
Cloud Trace	Cloud Trace provides latency sampling and reporting for App Engine, including per-URL statistics and latency distributions.
Cloud Translation	Cloud Translation API automatically translates text from one language to another language.
Cloud Vision	Cloud Vision enables developers to understand the content of an image by encapsulating powerful machine learning models in an easy to use API. It quickly classifies images into thousands of categories (e.g., "sailboat", "lion", "Eiffel Tower"), detects individual objects and faces within images, and finds and reads printed words contained within images. You can build metadata on your image catalog, moderate offensive content, or enable new marketing scenarios through image sentiment analysis. You can also analyze images uploaded in the request and integrate with your image storage on Cloud Storage.
Cloud VPN	Cloud VPN allows you to connect to your Virtual Private Cloud (VPC) network from your existing network, such as your on-premises network, another VPC network, or another cloud provider's network, through an IPsec connection using (i) Classic VPN, which supports dynamic (BGP) routing or static routing (route-based or policy-based), or (ii) HA (high-availability) VPN, which supports dynamic routing with a simplified redundancy setup, separate failure domains for the gateway interfaces, and a higher service level objective.
Cloud Workstations	Cloud Workstations provides managed development environments on Google Cloud with built-in security and preconfigured yet customizable development environments. Instead of requiring developers to install software and run setup scripts, customers can create a workstation configuration that specifies your environment in a reproducible way.

List of Products In Scope	Product Details
Compute Engine	Compute Engine offers scalable and flexible virtual machine computing capabilities in the cloud, with options to utilize certain CPUs, GPUs, or Cloud TPUs. You can use Compute Engine to solve large-scale processing and analytic problems on Google's computing, storage, and networking infrastructure.
Connect	Connect is a service that enables both users and Google-hosted components to interact with clusters through a connection to the in-cluster Connect software agent.
Contact Center AI (CCAI)	CCAI is a solution for improving the customer experience in your contact centers using AI. CCAI encompasses Dialogflow Essentials, Dialogflow Customer Experience Edition (CX), Speech-to-Text, and Text-to-Speech, and Speaker ID.
Contact Center AI Insights	Contact Center AI Insights helps customers extract value from their contact center data. It provides a console to explore the data, find relevant information and take action on the data. Customers can run advanced analysis within the platform to extract sentiment, topics and highlight key areas from their data.
Container Registry	Container Registry is a private Docker image storage system on Google Cloud Platform. The registry can be accessed through an HTTPS endpoint, so you can pull images from your machine, whether it's a Compute Engine instance or your own hardware.
Data Catalog	Data Catalog is a fully-managed and scalable metadata management service that empowers organizations to quickly discover, manage, and understand their data in Google Cloud. It offers a central data catalog across certain Google Cloud Services that allows organizations to have a unified view of their data assets.
Database Migration Service	Database Migration Service is a fully-managed migration service that makes it simple to perform high fidelity, minimal-downtime migrations at scale. You can use Database Migration Service to migrate from your on-premises environments, Compute Engine, and other clouds to certain Google Cloud-managed databases with minimal downtime.
Dataflow	Dataflow is a fully-managed service for strongly consistent, parallel data-processing pipelines. It provides an SDK for Java with composable primitives for building data-processing pipelines for batch or continuous processing. This service manages the life cycle of Compute Engine resources of the processing pipeline(s). It also provides a monitoring user interface for understanding pipeline health.
Dataform	Dataform is a service for data analysts to develop, test, version control, and schedule complex SQL workflows for data transformation in BigQuery.
Dataplex	Dataplex is a data fabric that unifies distributed data and automates data management and governance for that data.
Dataproc	Dataproc is a fast, easy to use, managed Spark and Hadoop service for distributed data processing. It provides management, integration, and development tools for unlocking the power of rich open source data processing tools. With Dataproc, you can create Spark/Hadoop clusters sized for your workloads precisely when you need them.
Dataproc Metastore	Dataproc Metastore provides a fully-managed metastore service that simplifies technical metadata management and is based on a fully-featured Apache Hive metastore. Dataproc Metastore can be used as a metadata storage service component for data lakes built on open source processing frameworks like Apache Hadoop, Apache Spark, Apache Hive, Presto, and others.
Datastore	Datastore is a fully-managed, schemaless, non-relational datastore. It provides a rich set of query capabilities, supports atomic transactions, and automatically scales up and down in response to load. It can scale to support an application with 1,000 users or 10 million users with no code changes.
Datastream	Datastream is a serverless change data capture (CDC) and replication service that enables data synchronization across heterogeneous databases, storage systems, and applications with minimal latency.
Dialogflow	Dialogflow is a development suite for voice and text conversational apps including chatbots. Dialogflow is cross-platform and can connect to apps (on the web, Android, iOS, and IoT) or existing platforms (e.g., Actions on Google, Facebook Messenger, Slack).
Document AI	Document AI classifies and extracts structured data from documents to help discover insights and automate business processes.
Document AI Warehouse	Document AI Warehouse is an integrated, cloud-based platform to store, search, organize, govern and analyze documents and their structured metadata (called Properties). Documents include structured (e.g. forms, invoices) and unstructured (e.g. contracts, research papers) and their Properties (metadata) includes AI-extracted data from documents and manually or AI-assigned tags (for example, account number, loan ID, document type).
Eventarc	Eventarc is a fully-managed service for eventing on Google Cloud Platform. Eventarc connects various Google Cloud services together, allowing source services (e.g., Cloud Storage) to emit events that are delivered to target services (e.g., Cloud Run or Cloud Functions).
Firebase Authentication	Firebase Authentication provides a service as part of the Firebase platform to authenticate and manage users in your applications. It supports authentication using email & password, phone number and popular federated identity providers like Google and Facebook.
Firestore	Firestore is a NoSQL document database for storing, syncing, and querying data for mobile and web apps. Its client libraries provide live synchronization and offline support, while its security features and integrations with Firebase and Google Cloud Platform accelerate building serverless apps.
Gemini for Google Cloud	Gemini for Google Cloud provides AI-powered end user assistance with a wide range of Google Cloud products. Gemini for Google Cloud is a generative AI-powered collaboration Service that provides assistance to Google Cloud end users. Gemini for Google Cloud is embedded in many Google Cloud products to provide developers, data scientists, and operators an integrated assistance experience. More details about the AI-assistance available through Gemini for Google Cloud can be found at https://cloud.google.com/gemini/docs/overview.

List of Products In Scope	Product Details
GKE Enterprise Config Management	Generative AI on Vertex AI is any Service with generative AI functionality in Vertex AI, including: ***Vertex AI API:*** enables customers to access generative AI foundation models via an API. ***Vertex AI Conversation (formerly Gen App Builder):*** allows customers to leverage foundational models and conversational AI to create multimodal chat or voice agents. ***Vertex AI Model Garden:*** enables customers to access generative AI foundation models, including large language, text-to-image, image-to-text, and multimodal models. ***Vertex AI Search:*** allows customers to leverage foundational models and search and recommendation technologies to create multimodal semantic search and question-answering experiences. ***Vertex AI Studio:*** is a user interface in the Google Cloud console for rapidly prototyping and testing generative AI models. *Generative AI Services also includes any generative AI features of a Service.*
GKE Identity Service	Identity Service is an authentication service that lets customers bring existing identity solutions for authentication to multiple environments. Users can log in to and access their clusters from the command line or from the Google Cloud console, all using their existing identity providers.
Google Cloud Armor	Google Cloud Armor offers a policy framework and rules language for customizing access to internet-facing applications and deploying defenses against denial of service attacks as well as targeted application attacks. Components of Google Cloud Armor include: L3/L4 volumetric DDos Protection, preconfigured web-application firewall (WAF) rules, and custom rules language.
Google Cloud Deploy	Cloud Deploy is fully managed continuous delivery service for easy scaling, with support for enterprise security and audit. Cloud Deploy makes continuous delivery to GKE, Cloud Run services and jobs, and Anthos easy and powerful. Define releases and progress them through environments, such as test, stage, and production. Cloud Deploy provides easy one-step promotion and rollback of releases via the web console, CLI, or API. Built-in metrics enable insight into deployment frequency and success.
Google Cloud Identity-Aware Proxy	Google Cloud Identity-Aware Proxy is a tool that helps control access, based on a user's identity and group membership, to applications running on Google Cloud Platform.
Google Cloud Marketplace	Google Cloud Platform (GCP) Marketplace offers ready-to-go development stacks, solutions, and services from third-party partners and Google to accelerate development. It enables the deployment of production-grade solutions, obtains direct access to partner support, and receives a single bill for both GCP and third-party services.
Google Cloud SDK	Google Cloud SDK is a set of tools to manage resources and applications hosted on Google Cloud Platform. It includes the Google Cloud Command Line Interface (CLI), Cloud Client Libraries for programmatic access to Google Cloud Platform services, the gsutil, kubectl, and bq command line tools, and various service and data emulators for local platform development. The Google Cloud SDK provides the primary programmatic interfaces to Google Cloud Platform.
Google Cloud Threat Intelligence for Chronicle	Google Cloud Threat Intelligence (GCTI) enables Cloud Security Products to deliver threat intelligence and detection use cases in-product to enable customers to better protect their Cloud/GCP environments through IoC feeds, curated content, and active research.
Google Kubernetes Engine (GKE)	Google Kubernetes Engine, powered by the open source container scheduler Kubernetes, enables you to run containers on Google Cloud Platform. Kubernetes Engine takes care of provisioning and maintaining the underlying virtual machine cluster, scaling your application, and operational logistics such as logging, monitoring, and cluster health management. Services include:
Healthcare Data Engine	HDE is a solution that enables (1) harmonization of healthcare data to the Fast Healthcare Interoperability Resources (“FHIR”) standard and (2) streaming of healthcare data to an analytic environment.
Hub	Hub is centralized control-plane that enables a user to register clusters running in a variety of environments, including Google’s cloud, on premises in customer datacenters, or other third party clouds. Hub provides a way for customers to centrally manage features and services on customer-registered clusters.
Identity & Access Management (IAM)	IAM provides administrators the ability to manage cloud resources centrally by controlling who can take what action on specific resources.
Identity Platform	Identity Platform provides you with functionality and tools to manage your users' identities and access to your applications. Identity Platform supports authentication and management of users with a variety of methods, including email & password, phone number, and popular federated identity providers like Google and Facebook.
Infrastructure Manager	Infrastructure Manager API is a GCP hosted Terraform Service that is used to create, update and delete GCP resources using customer provided Terraform configuration files.
Integration Connectors	Integration Connectors is a platform that allows customers to connect to business applications, technologies and other data sources using native protocols of each target application. The connectivity established through these connectors helps manage access to various data sources which can be used with other services like Application Integration through a consistent, standard interface.

List of Products In Scope	Product Details
Key Access Justifications (KAJ)	KAJ provides a justification for every request sent through Cloud EKM for an encryption key that permits data to change state from at-rest to in-use.
Knative serving	Knative, created originally by Google with contributions from over 50 different companies, delivers an essential set of components to build and run serverless applications on Kubernetes.
Looker Studio	Looker Studio is self-service business intelligence with flexibility for smarter business decisions. Users can deploy an example data warehouse or analytics lakehouse solution to store, analyze, and visualize data using BigQuery and Looker Studio. Looker Studio helps customers tell impactful stories by creating and sharing engaging reports and data visualizations.
Managed Service for Microsoft Active Directory (AD)	Managed Service for Microsoft Active Directory is a Google Cloud service running Microsoft AD that enables you to deploy, configure and manage cloud-based AD-dependent workloads and applications. It is a fully-managed service that is highly available, applies network firewall rules, and keeps AD servers updated with Operating System patches.
Media CDN	Media CDN is Google Cloud's media delivery solution. Media CDN complements Cloud CDN, which is Google Cloud's web acceleration solution. Media CDN is optimized for high-throughput egress workloads, such as streaming video and large file downloads.
Memorystore	Memorystore, which includes Memorystore for Redis and Memorystore for Memcached, provides a fully-managed in-memory data store service that allows customers to deploy distributed caches that provide sub-millisecond data access.
Migrate to Virtual Machines	Migrate to Virtual Machines is a fully-managed migration service that enables you to migrate workloads at scale into Google Cloud Compute Engine with minimal down time by utilizing replication-based migration technology.
Network Connectivity Center	Network Connectivity Center is a hub-and-spoke model for network connectivity management in Google Cloud that facilitates connecting a customer's resources to its cloud network.
Network Intelligence Center	Network Intelligence Center is Google Cloud's comprehensive network monitoring, verification, and optimization platform across the Google Cloud, multi-cloud, and on-prem environments.
Network Service Tiers	Network Service Tiers enable you to select different quality networks (tiers) for outbound traffic to the internet: the Standard Tier primarily utilizes third party transit providers while the Premium Tier leverages Google's private backbone and peering surface for egress.
Persistent Disk	Persistent Disk is a durable and high performance block storage service for Google Cloud Platform. Persistent Disk provides SSD and HDD storage that can be attached to instances running in either Compute Engine or Google Kubernetes Engine.
Pub/Sub	Pub/Sub is designed to provide reliable, many-to-many, asynchronous messaging between applications. Publisher applications can send messages to a "topic" and other applications can subscribe to that topic to receive the messages. By decoupling senders and receivers, Pub/Sub allows developers to communicate between independently written applications.
reCAPTCHA Enterprise	reCAPTCHA Enterprise helps detect fraudulent activity on websites.
Recommender	Recommenders automatically analyze your usage patterns to provide recommendations and insights across services to help you use Google Cloud Platform in a more secure, cost-effective, and efficient manner.
Resource Manager API	Resource Manager API allows you to programmatically manage Google Cloud Platform container resources (such as Organizations and Projects), that allow you to group and hierarchically organize other Google Cloud Platform resources. This hierarchical organization lets you easily manage common aspects of your resources such as access control and configuration settings.
Risk Manager	Risk Manager allows customers to scan their cloud environments and generate reports around their compliance with industry-standard security best practices, including CIS benchmarks. Customers then have the ability to share these reports with insurance providers and brokers.
Secret Manager	Secret Manager provides a secure and convenient method for storing API keys, passwords, certificates, and other sensitive data.
Secure Source Manager	Secure Source Manager is a fully-managed service that provides a Git-based source code management system.
Secure Web Proxy (Cloud SWP)	SWP provides a simple and scalable cloud-first web proxy for cloud workload protection, enabling monitoring, content inspection and granular policy control of web traffic, between Google Cloud hosted workloads and external destinations.
Security Command Center	Security Command Center is Google Cloud's centralized vulnerability and threat reporting service. Security Command Center provides asset inventory and discovery and allows you to identify misconfigurations, vulnerabilities and threats, helping you to mitigate and remediate risks.
Sensitive Data Protection (including Cloud Data Loss Prevention)	Sensitive Data Protection is a fully-managed service enabling customers to discover, classify, de-identify, and protect sensitive data, such as personally identifiable information.
Service Directory	Service Directory is a managed service that offers customers a single place to publish, discover and connect their services in a consistent way, regardless of their environment. Service Directory supports services in Google Cloud, multi-cloud, and on-prem environments and can scale up to thousands of services and endpoints for a single project.
Service Infrastructure	Service Infrastructure is a foundational platform for creating, managing, securing, and consuming APIs and services. It includes:

List of Products In Scope	Product Details
Service Mesh	Service Mesh is a managed service mesh service that includes (i) a managed certificate authority that issues cryptographic certificates that identify customer workloads within the Service Mesh for mutual authentication, and (ii) telemetry for customers to manage and monitor their services. Customers receive details showing an inventory of services, can understand their service dependencies, and receive metrics for monitoring their services. For clarity this service does not include Service Mesh -- Software (see below regarding Premium Software).
Speech-to-Text	Speech-to-Text allows developers to convert audio to text by applying powerful neural network models in an easy to use API.
Storage Transfer Service	Storage Transfer Service enables you to import large amounts of online data into Cloud Storage, quickly and cost-effectively. With Storage Transfer Service, you can transfer data from locations reachable by the general internet (e.g., HTTP/HTTPS), including Amazon Simple Storage Service (Amazon S3), as well as transfer data between Google Cloud products (e.g., between two Cloud Storage buckets). You can also use Storage Transfer Service to move data between private data center storage (e.g., NFS) and Google Cloud products (e.g., transfer from NFS to Cloud Storage).
Talent Solution	Talent Solution offers access to Google's machine learning, enabling company career sites, job boards, ATS, staffing agencies, and other recruitment technology platforms to improve the talent acquisition experience.
Text-to-Speech	Text-to-Speech synthesizes human-like speech based on input text in a variety of voices and languages.
Traffic Director	Traffic Director is Google Cloud Platform's traffic management service for open service meshes.
Transfer Appliance	Transfer Appliance is a solution that uses hardware appliances and software to transfer large amounts of data quickly and cost-effectively into Google Cloud Platform.
Vertex AI Codey	Vertex AI Codey helps you build and deploy machine learning models with an easy-to-use visual interface, without needing to write any code.
Vertex AI Data Labeling	AI Platform Data Labeling helps developers label data and centrally manage labels for training and evaluating machine learning models.
Vertex AI Platform	Vertex AI Platform is a service for managing the AI and machine learning development lifecycle. Customers can (i) store and manage datasets, labels, features, and models; (ii) build pipelines to train and evaluate models and run experiments using Google Cloud algorithms or custom training code; (iii) deploy models for online or batch use cases; (iv) manage data science workflows using Colab Enterprise and Vertex AI Workbench (also known as Notebooks); and (v) create business optimization plans with Vertex Decision Optimization.
Video Intelligence API	Video Intelligence API makes videos searchable, and discoverable, by extracting metadata with an easy to use REST API. It quickly annotates videos stored in Cloud Storage, and helps you identify key noun entities of your video and when they occur within the video.
Virtual Private Cloud	Virtual Private Cloud provides a private network topology with IP allocation, routing, and network firewall policies to create a secure environment for your deployments.
VPC Service Controls	VPC Service Controls provide administrators the ability to configure security perimeters around resources of API based cloud services (such as Cloud Storage, BigQuery, Bigtable) and limit access to authorized VPC networks, thereby mitigating data exfiltration risks.
Web Risk API	Web Risk API is a Google Cloud service that lets client applications check URLs against Google's constantly updated lists of unsafe web resources.
Workflows	Workflows is a fully-managed service for reliably executing sequences of operations across microservices, Google Cloud services, and HTTP-based APIs.
Workload Manager	Workload Manager is a rule-based validation service for evaluating workloads running on Google Cloud. If enabled, Workload Manager scans application workloads to detect deviations from standards, rules, and best practices that improve system quality, reliability, and performance.

P2-1 Validate Scope:
Scoping involves the identification of the facilities, people, processes, and technologies that interact with or could impact the security of 3DS data or systems. Once scope is properly identified, the appropriate security controls can be applied.

3DS PART 2 CORE SECURITY STANDARD REQUIREMENTS	VALIDATION REQUIREMENTS	GUIDANCE	CONTROL			SUMMARY
			GCP	CLIENT	SHARED	
P2–1.1 Scoping						
1.1.1 All networks and system components in-scope for these PCI 3DS security requirements are identified.	Examine documented results of scope reviews. Interview personnel.	A scope verification exercise includes identifying all locations and flows of 3DS data, as well as the systems performing 3DS functions (ACS, DS, and/or 3DSS) and any systems that are connected to or could impact the 3DE. Network mapping tools, data flow diagrams, and process documentation can often assist with this process. The scoping process should also include consideration of backup/recovery sites and fail-over systems. The scoping exercise should also include identifying personnel with access to 3DS data, as well as the physical locations where 3DS systems are housed. Validation of scope should be performed as frequently as needed to ensure the scope is known and scope documentation remains accurate and up to date. The results of scoping exercises should help to confirm that security controls are applied to all applicable systems, and that all connections to third-parties—for example, service providers and business partners—are identified and properly secured.			X	**Google Cloud:** Google provides platform for 3DS implementation by the client and does not directly store, process, or transmit 3DS data. Google has identified in scope products that are hosted within the GCP environment. The GCP environment includes infrastructure, development, operations, management, support for the in-scope products. (https://cloud.google.com/security/infrastructure/design) **Customers**: Customers are responsible for defining and documenting the scope for their PCI 3DS environment, including identification of any customer-owned systems in Google facilities.
1.1.2 All out-of-scope networks are identified with justification for being out of scope and descriptions of segmentation controls implemented.	Examine documented results of scope reviews. Examine data flow and network diagrams. Observe segmentation controls.				X	**Goo**gle Cloud: Google has outlined specific products for use within a 3DS environment, maintains internal network and dataflow diagrams applicable to its environment, and has made appropriate segmentation controls available to its customers based on customer need. **Customers**: Customers are responsible for identifying out-of-scope networks for their 3DE, maintaining data flow and network diagrams, and implementing segmentation as appropriate for their 3DS environment.
1.1.3 All connected entities with access to the 3DS environments are identified.	Examine documentation. Interview personnel.				X	**Google Cloud:** Google identifies and maintains connected entity access for the GCP environment. **Customers**: Customers are responsible for identifying the connected entities with access to their 3DS environment.

P2-2. Security governance
A security governance program provides oversight and assurance that an entity's information security strategies are aligned with its business objectives and adequately address risks to the entity's data and systems.

3DS PART 2 CORE SECURITY STANDARD REQUIREMENTS	VALIDATION REQUIREMENTS	GUIDANCE	CONTROL			SUMMARY
			GCP	CLIENT	SHARED	
P2–2.1 Security governance						
2.1.1 Security objectives are aligned with business objectives.	Examine documentation. Interview personnel.	The security objectives should be defined as part of an overarching security strategy that supports and facilitates business objectives. The security strategy should provide the foundation for the entity's security policies and procedures and provide a benchmark against which the health of security controls is monitored and measured.			X	**Google Cloud**: Google has documented the security objectives within their Security Baseline Governance documentation for their GCP environment. **Customers**: Customers are responsible for defining security objectives as part of their governance process.
2.1.2 Responsibilities and accountability for meeting security objectives are formally assigned, including responsibilities for the security of 3DS processes.	Examine documentation. Interview personnel.	The assignment of specific roles and responsibilities should include monitoring and measurement of performance to ensure security objectives are met. Roles and responsibilities may be assigned to a single owner or multiple owners for different aspects. Ownership should be assigned to individuals with the authority to make risk-based decisions and upon whom accountability rests for the specific function. Duties should be formally defined, and owners should be able to demonstrate an understanding of their responsibilities and accountability			X	**Google Cloud**: Google has responsibilities documented for the GCP environment as part of their security governance process. **Customers**: Customers are responsible for defining security objectives and assigning responsibilities and accountability to meet the objectives defined.
2.1.3 Responsibility for identifying and addressing evolving risks is assigned.	Examine documentation. Interview personnel.				X	**Google Cloud:** Google has responsibilities for identifying and addressing risks documented as part of their security governance process for their GCP environment. **Customers**: Customers are responsible for identifying and addressing evolving risks for their 3DE.
P2–2.2 Manage Risk						
2.2.1 A formal risk-management strategy is defined.	Examine documentation. Interview personnel.	The risk-management strategy defines a structured approach for identifying, evaluating, managing, and monitoring risk. The strategy should include requirements for regularly reviewing and updating the entity's risk- assessment processes as well as methods to monitor the effectiveness of risk-mitigation controls.			X	**Google Cloud:** Google has formal risk management program in place for the GCP environment where GCP products are hosted. **Customers**: Customers are responsible for documenting and implementing the formal risk management strategy for their 3DS environment.
2.2.2 The risk-management strategy is approved by authorized personnel and updated as needed to address changing risk environment.	Examine documentation. Interview personnel.	The risk-management strategy should be approved by personnel with appropriate responsibly and accountability. (See Requirements P2-2.1.2 and P2-2.1.3.)			X	**Google Cloud**: Google has formal risk management program in place for the GCP environment where GCP products are hosted. **Customers**: Customers are responsible for approval and updates of its risk management strategy.
P2–2.3 Business as usual (BAU)						
2.3.1 Review and/or monitoring is performed periodically to confirm personnel are following security policies and procedures.	Examine evidence of reviews and/or ongoing monitoring. Interview personnel.	Periodic reviews and/or ongoing monitoring of personnel and activities should ensure security is included as part of normal business operations on an ongoing basis. Reviews should be performed by responsible personnel as defined by the entity. The frequency of reviews should be defined in accordance with the entity's risk assessments and be appropriate for the particular job function.			X	**Google Cloud**: Google has the review and monitoring processes implemented for the GCP environment where GCP products are hosted. **Customers**: Customers are responsible for monitoring to confirm personnel are following security policies and procedures.

P2-2. Security governance
A security governance program provides oversight and assurance that an entity's information security strategies are aligned with its business objectives and adequately address risks to the entity's data and systems.

3DS PART 2 CORE SECURITY STANDARD REQUIREMENTS	VALIDATION REQUIREMENTS	GUIDANCE	CONTROL			SUMMARY
			GCP	CLIENT	SHARED	
2.3.2 Processes to detect and respond to security control failures are defined and implemented	Examine documented processes. Observe implemented processes. Interview personnel.	The entity should be able to detect any failures in security controls and respond to them in a timely manner. Processes for responding to security control failures should include: • Restoring the security control • Identifying the cause of failure • Identifying and addressing any security issues that arose during the failure of the security control • Implementing mitigation (such as process or technical controls) to prevent the cause of the failure recurring • Resuming monitoring of the security control			X	**Google Cloud:** Google has the security control failures detection and response process in place for the GCP environment where GCP products are hosted. **Customers**: Customers are responsible for documenting security policies and procedures and implementing the detection and response process for security control failures for their 3DS environment.
P2–2.4 Manage third-party relationships						
2.4.1 Policies and procedures for managing third-party relationships are maintained and implemented.	Examine documented policies/procedures. Interview personnel.	Policies and procedures for managing third-party relationships should consider the risk that each relationship represents, as well as how third- party performance and behavior will be monitored. The policy should be kept up to date, approved by management, and communicated to applicable personnel.			X	**Google Cloud:** Google maintains documented policies and procedures for managing third-party relationships within the GCP environment. **Customers**: Customers are responsible for maintaining and implementing policies and procedures for managing third-party relationships.
2.4.2 Due diligence is performed prior to any engagement with a third party.	Examine documented procedures. Examine results of due diligence efforts. Interview personnel.	Due-diligence processes should include thorough vetting and a risk analysis prior to establishing a formal relationship with the third party. Specific due-diligence processes and goals will vary for each entity and should provide sufficient assurance that the third party can meet the entity's security and operational needs.			X	**Google Cloud:** Google maintains documented policies and procedures that includes the due diligence steps for managing its third-party relationships within the GCP environment. **Customers**: Customers are responsible for maintaining and implementing policies and procedures that includes the due diligence steps for managing their third-party relationships.
2.4.3 Security responsibilities are clearly defined for each third-party engagement.	Examine documentation. Interview personnel.	The specific approach for defining security responsibilities will depend on the type of service as well as the particular agreement between the entity and third party. The entity should have a clear understanding of the security responsibilities to be met by the third party and those to be met by the entity.			X	**Google Cloud:** Google manages responsibilities with third parties as documented in the agreements for the GCP environment where GCP products are hosted. **Customers**: Customers are responsible for defining the security responsibilities for each third-party engagement.
2.4.4 The 3DS entity periodically verifies that the agreed-upon responsibilities are being met.	Examine results of periodic verification. Interview personnel.	The specific type of evidence provided by the third party will depend on the agreement in place between the two parties. The evidence should provide assurance that the agreed-upon responsibilities are being met on a continual basis. The frequency of verification should be aligned with the entity's risk analysis of the service being provided.			X	**Google Cloud:** Google manages responsibilities for its third parties as part of the agreement for the GCP environment where GCP products are hosted. **Customers**: Customers are responsible for verifying that the agreed-upon responsibilities are met for any third party they engage with.
2.4.5 Written agreements are maintained.	Examine documentation.	Agreements should promote a consistent level of understanding between parties about their applicable responsibilities, and be acknowledged by each party. The acknowledgement evidences each party's			X	**Google Cloud:** Google maintains documented written agreements with its third parties for the GCP environment where GCP products are hosted.

P2-2. Security governance
A security governance program provides oversight and assurance that an entity's information security strategies are aligned with its business objectives and adequately address risks to the entity's data and systems.

3DS PART 2 CORE SECURITY STANDARD REQUIREMENTS	VALIDATION REQUIREMENTS	GUIDANCE	CONTROL			SUMMARY
			GCP	CLIENT	SHARED	
	Interview personnel.	The acknowledgement evidences each party's commitment to maintaining proper security in regard to the 3DS services.			X	**Customers**: Customers are responsible for maintaining written agreements with their third-party service providers.

P2-3 Protect 3DS systems and applications
To maintain the security of 3DS environments, controls need to be designed and implemented to protect the confidentiality, integrity, and availability of 3DS technologies, processes, and data.

3DS PART 2 CORE SECURITY STANDARD REQUIREMENTS	VALIDATION REQUIREMENTS	GUIDANCE	CONTROL			SUMMARY
			GCP	CLIENT	SHARED	
P2–3.1 Protect boundaries						
3.1.1 Traffic to and from ACS and DS is restricted to only that which is relevant to the 3DS functions.	Examine log files. Observe implemented controls.	The only permitted traffic should be for the purposes of 3DS transactions, or to support a 3DS function, or support the 3DS system component—for example, for security or management purposes. Systems within the 3DE should be limited to those necessary for performing or supporting 3DS functions. All types of interfaces should be identified, including physical, logical, and virtual.		X		**Customers**: Customers are fully responsible for restricting traffic to its ACS and DS systems. If GCP products are utilized by the customer to meet this control, GCP-provided documentation should be used for restricting such traffic.
3.1.2 Traffic to and from ACS and DS is permitted only via approved interfaces.	Examine log files. Observe implemented controls.			X		**Customers**: Customers are fully responsible for identifying and restricting inbound and outbound access to approved ACS and DS connections. If GCP products are utilized by the customer to meet this control, GCP-provided documentation should be used for restricting such traffic.
P2–3.2 Protect baseline configurations						
3.2.1 Controls are implemented to protect the confidentiality and integrity of system configurations and documentation that support security settings.	Examine log files. Observe implemented controls.	Examples of the types of files requiring protection include baseline configuration files, system build data, system images, and build procedures. The controls should protect both integrity and confidentiality of such data, to prevent an attacker from changing the secure configuration of a 3DS system component, installing their own configuration, or using the information to identify security gaps they can then exploit.			X	**Google Cloud:** Google protects the confidentiality and integrity of the GCP infrastructure configurations supporting its products. (https://cloud.google.com/security/infrastructure/design) **Customers:** Customers are responsible for implementing the controls to protect the confidentiality and integrity of its system configurations within the GCP environment. If GCP products are utilized by the customer to meet this control, GCP-provided documentation should be used for protecting these configurations.
P2–3.3 Protect applications and application interfaces						
3.3.1 Applications and programs are protected from unauthorized changes once in a production state.	Examine log files. Observe implemented controls.	Ensuring the integrity of applications and programs in production requires more than an effective change-control process. A combination of strict access controls, monitoring, and programmatic controls should be considered. Examples of additional mechanisms include software authentication codes, digitally signed modules, or execution within an SCD. The use of a protection technique is only effective if the system confirms the results (for example, is the digital signature valid?) and acts on the results.			X	**Google Cloud**: Google has effective change control and access control process in place for managing any changes to the applications supporting GCP infrastructure and services. **Customers**: Customers are responsible for ensuring customer applications and programs are protected from unauthorized changes once in production state. If GCP products are utilized by the customer to meet this control, GCP-provided documentation should be used for configuring these protections.
3.3.2 The mechanisms to protect applications and programs from unauthorized changes are monitored and maintained to confirm effectiveness.	Observe implemented controls for monitoring and maintaining protection mechanisms.	Protection mechanisms should be kept up to date and monitored to ensure they are working as intended and continue to be effective. Cryptographic techniques used for API code protection may require updating as computation capabilities and cryptanalysis improvements evolve.			X	**Google Cloud:** Google has effective monitoring processes in place for managing any changes to the applications supporting GCP infracstruture and services. **Customers**: Customers are responsible for identifying. monitoring, and maintaining mechanisms to protect applications and programs from unauthorized changes. If GCP products are utilized by customer to meet this control, GCP-provided documentation should be used for configuring these protections.

P2-3 Protect 3DS systems and applications
To maintain the security of 3DS environments, controls need to be designed and implemented to protect the confidentiality, integrity, and availability of 3DS technologies, processes, and data.

3DS PART 2 CORE SECURITY STANDARD REQUIREMENTS	VALIDATION REQUIREMENTS	GUIDANCE	CONTROL			SUMMARY
			GCP	CLIENT	SHARED	
3.3.3 All APIs that interface with the 3DS environment are identified, defined, and tested to verify they perform as expected.	Examine network and data-flow diagrams. Observe implemented controls. Examine results of testing.	All exposed APIs need to be periodically reviewed and tested to ensure that they are functioning as intended. Use of industry best practices and guidance is recommended—for example, the OWASP REST (REpresentational State Transfer) Security Cheat Sheet provides best practices for REST-based services.			X	**Google Cloud:** Google has testing and scanning processes implemented for all APIs supporting GCP infrastruture and services. **Customers**: Customers are responsible for identifying, defining, and functional testing of APIs. If GCP products are utilized by customer to meet this control, GCP-provided documentation should be used for performing appropriate testing.
3.3.4 Controls are implemented to protect APIs exposed to untrusted networks.	Examine network and data-flow diagrams Observe implemented controls. Examine results of testing Interview personnel.				X	**Google Cloud:** Google has testing and scanning processes implemented for all APIs supporting GCP infrastructure and services. **Customers**: Customers are responsible for implementing the controls to protect APIs exposed to untrusted networks. If GCP products are utilized by customer to meet this control, GCP-provided documentation should be used for configuring these protections.
P2–3.4 Secure web configurations						
3.4.1 Only those HTTP request methods required for system operation are accepted. All unused methods are explicitly blocked.	Examine log files. Observe implemented controls. Interview personnel	All functionality not explicitly required for system operation should be disabled or blocked; and configurations should be designed to prevent common application attack scenarios such as XSS, Clickjacking, and injection attacks. Applications should be configured to restrict content and functionality from external sources to only that which is necessary for business purposes. If functionality or content from trusted external sources—for example, third-party websites—is necessary for business purposes, then those sources and the methods in which they are permitted to provide such content (e.g., as iframes, direct posts, etc.) should be explicitly authorized, and all other sources and methods blocked.			X	**Google Cloud:** Google ensures only required HTTP request methods are enabled for the applications supporting GCP infrastructure and services. **Customers**: Customers are responsible for implementing secure configuration of HTTP request methods. If GCP products are utilized by customer to meet this control, GCP-provided documentation should be used for configuring these protections. GCP customers are responsible for securing web configurations for in-house developed applications and third-party applications utilized within their 3DE.
3.4.2 The use of HTTPS is enforced across all application pages/resources and all communications are prevented from being sent over insecure channels (e.g., HTTP).	Examine log files. Observe implemented controls. Interview personnel.				X	**Google Cloud:** Google ensures all communications occur over secure channels for applications supporting GCP infrastructure and services. **Customers:** Customers are responsible for implementing the secure protocols and enforcing HTTPS usage. If GCP products are utilized by customer to meet this control, GCP provided guidance documentation should be used for configuration of products. GCP customers are responsible for securing web configurations for in-house developed applications or external third-party applications utilized within their PCI 3DE.
3.4.3 Applications (or the underlying systems) are configured to reject content provided by external sources by default. Exceptions are explicitly authorized.	Examine documented controls.					**Google Cloud:** Google leverages secure software development processes and testing to ensure no unauthorized functionality is enabled for applications supporting GCP infrastructure and services.

P2-3 Protect 3DS systems and applications
To maintain the security of 3DS environments, controls need to be designed and implemented to protect the confidentiality, integrity, and availability of 3DS technologies, processes, and data.

3DS PART 2 CORE SECURITY STANDARD REQUIREMENTS	VALIDATION REQUIREMENTS	GUIDANCE	CONTROL			SUMMARY
			GCP	CLIENT	SHARED	
	Observe implemented controls. Interview personnel.				X	**Customers:** Customers are responsible for configuring applications to meet this control. If GCP products are utilized by customer to meet this control, GCP-provided documentation should be used for configuring these protections.
3.4.4 Applications are configured to prevent content from being embedded into untrusted third-party sites/applications. Exceptions are explicitly authorized.	Examine documented controls. Observe implemented controls. Interview personnel.	Similarly, content provided by the 3DS provider should be prevented (to the extent possible) from being embedded in the sites of untrusted third parties. Otherwise, those parties might use the content of the 3DS entity to impersonate the 3DS entity in an attempt to hijack 3DS transactions and/or commit fraud.			X	**Google Cloud:** Google secure software development processes and testing mitigate exploits associated with unauthorized external content for applications supporting GCP infrastructure and services. **Customers:** Google does not manage content provided by the 3DS provider. Customers are fully responsible for meeting this control to prevent use of 3DS application content to impersonate, hijack, or otherwise conduct fraud. If GCP products are utilized by customer to meet this control, GCP-provided documentation should be used for configuring these protections.
3.4.5 Security features native to the development framework and/or application platform are enabled (where feasible) to protect against common client-side attacks (such as XSS, Injection, etc.)	Examine documented controls. Observe implemented controls. Interview personnel.	Native security functions are available in most modern development platforms and frameworks, and are effective at protecting against common client-side attacks without requiring additional security functionality to be written into the application code. Methods to restrict such content and functionality include the use of Content Security Policy (CSP) directives and HTTP Strict Transport Security (HSTS). Other security features native to the development framework that should be considered include automated compile-time security checks that are performed as part of the application build process. Where native security controls such as those described above are not used, 3DS entities should document the controls that have been implemented to protect applications and systems from common client-side attacks (such as XSS, XSRF, Injection attacks, etc.) and provide justification for why native features were not used.			X	**Google Cloud:** Google secure software development processes ensure systems and applications supporting GCP infrastructure and services are protected from common client-side attacks. **Customers**: Customers are responsible to maintain software development standards, change control, and vulnerability management programs aligned with other compliance framework to protect against common client-side attacks for applications they develop and host within the 3DE.
P2–3.5 Maintain availability of 3DS operations						
3.5.1 Availability mechanisms are implemented to protect against loss of processing capability within the 3DS infrastructure.	Examine documented controls. Observe implemented controls.	3DS components should be architected with high availability as a key factor in the software, system, and infrastructure design to maintain the integrity of the 3DS ecosystem. Security policies should reflect availability				**Goo**gle Cloud: GCP plans and actively manages resources to ensure availability of its infrastructure services, including customer-managed services for load balancing and failover between regions, availability zones, and services.

P2-3 Protect 3DS systems and applications
To maintain the security of 3DS environments, controls need to be designed and implemented to protect the confidentiality, integrity, and availability of 3DS technologies, processes, and data.

3DS PART 2 CORE SECURITY STANDARD REQUIREMENTS	VALIDATION REQUIREMENTS	GUIDANCE	CONTROL			SUMMARY
			GCP	CLIENT	SHARED	
		requirements of 3DS components and security resources in support of 3DS platform and clusters—for example, review of catastrophic testing results, failover results, and change-control processes. The controls should ensure security resources are working correctly and according to policy within the respective testing processes. The plan for availability should allow the entity to withstand denial-of-service (DoS) attacks that could force fallback to less secure verification methods or provide cover for other attacks against a system or the infrastructure. The implemented controls should demonstrably reduce this risk through, for example, a combination of fault-tolerance and rapid response/recovery capabilities as well as the use of application isolation, data and system restraints, and load balancing. Documentation and domain architectures should be reviewed for denial-of-service utilities and network load-balancing capabilities. Testing of back-up process and data should be performed.			X	**Customers**: Customers are responsible for implementing mechanism that protect against loss of processing capability for their 3DS environment. If GCP products are utilized by customer to meet this control, GCP-provided documentation should be used for configuring these availability mechanisms.
3.5.2 The availability mechanisms implemented are monitored and maintained to confirm effectiveness.	Observe implemented controls for monitoring and maintaining the Interview personnel.	The mechanisms intended to maintain availability of the 3DS infrastructure should be maintained and monitored to ensure they are working as intended and continue to be effective. Continuous monitoring of processing availability and rapid reporting of outages aid in timely response to potential failures. Availability mechanisms and technologies evolve and may require periodic refresh. Additionally, the sophistication of attacks that may adversely impact availability or that may exploit a degraded system continues to evolve.			X	**Goo**gle Cloud: Google monitors resource availability and utilization and implements multiple mechanisms to ensure availability throughout its environment. Google provides the capability for customers to implement availability mechanisms for their GCP environment. **Customers**: Customers are responsible to monitor effectiveness of availability mechanisms for their 3DE to prevent and respond to service degradation or data loss. If GCP products are utilized by customer to meet this control, GCP-provided documentation should be used for configuring these monitoring mechanisms.

P2-4. Secure logical access to 3DS systems
In addition to ensuring strong access controls and account management for the 3DS environment, certain types of access present a higher risk and require more stringent controls to prevent them from being misused or compromised.

3DS PART 2 CORE SECURITY STANDARD REQUIREMENTS	VALIDATION REQUIREMENTS	GUIDANCE	CONTROL			SUMMARY
			GCP	CLIENT	SHARED	
P2–4.1 Secure connections for issuer and merchant customers						
4.1.1 Access by issuer and merchant users to their assigned issuer and merchant interfaces—for example, via API or web portal—for purposes of managing only their own account, is restricted to authorized personnel and requires a unique user ID with strong password and another form of strong authentication.	Examine documented procedures. Observe implemented controls.	This requirement is intended for scenarios where the 3DS entity provides issuer and merchant users with access to 3DS services and data through defined issuer and merchant interfaces, such as an API or web portal. In this scenario, the issuer and merchant personnel require a unique user ID with a strong password and another form of strong authentication. Strong authentication techniques should align with industry-accepted practices and may include: • One-time passcodes/passwords (OTP) • Certificate-based authentication (CBA/SAML) where a public and private key is unique to the authentication device and the person who possesses it • Context-based authentication where additional information is required to verify whether a user's identity is authentic • Restriction of connections to only predefined and authorized system components–e.g., via IP filtering or site-to-site VPN These merchant/issuer users have access only to their own merchant/issuer account and are not able to access any other account or impact the configuration of any application, system component, or network. While multi-factor authentication is not required for this type of access, it is recommended.		X		**Customers**: Customers are responsible for managing and implementing strong authentication requirements for issuer and merchant users. If GCP products are utilized by customer to meet this control, GCP-provided documentation should be used for configuring these services.
P2-4.2 Secure internal network connections						
4.2.1 Multi-factor authentication is required for all personnel with non-console access to ACS, DS and 3DSS.	Examine documented procedures.	Multi-factor authentication (MFA) requires the completion of at least two different authentication				**Google Cloud:** Google requires multi-factor authentication to be used by administrators who have access to the GCP production

P2-4. Secure logical access to 3DS systems
In addition to ensuring strong access controls and account management for the 3DS environment, certain types of access present a higher risk and require more stringent controls to prevent them from being misused or compromised.

3DS PART 2 CORE SECURITY STANDARD REQUIREMENTS	VALIDATION REQUIREMENTS	GUIDANCE	CONTROL			SUMMARY
			GCP	CLIENT	SHARED	
	Observe implemented controls.	methods—that is, something you know, something you have, and something you are—prior to access being granted. The authentication mechanisms used should be implemented to ensure their independence such that access to one factor does not grant access to any other factor, and the compromise of any one factor does not affect the integrity or confidentiality of any other factor. Additionally, no prior knowledge of the success or failure of any factor should be provided to the individual until all factors have been presented. Refer to industry standards and best practices for further guidance on MFA principles. MFA can be applied at the network level, system level, or application level. For example, MFA could be applied when connecting to the 3DE secure network or network segment, or when connecting to an individual 3DS system component. MFA is required for all personnel connections to the ACS, DS, and 3DSS that occur over a network interface. Examples of access include for purposes of maintenance, configuration, updating, administration, or general management of the 3DS component. MFA is not required for application or system accounts performing automated functions.			X	environment. **Customers**: Customers are responsible for managing and implementing strong authentication requirements including multi-factor authentication for all personnel with non-console access to 3DS systems. If GCP products are utilized by customer to meet this control, GCP-provided documentation should be used for configuring these services.
P2–4.3 Secure remote access						
4.3.1 Multi-factor authentication is required for all remote access originating from outside the entity's network that provides access into the 3DE.	Examine documented procedures. Observe implemented controls.	Multi-factor authentication (MFA) is required for all personnel—both user and administrator, and including third-party access for support or maintenance—accessing the 3DE from outside the entity's network. Where MFA is implemented to grant access to the 3DE, additional MFA is not required for access to individual systems or applications within the 3DE.			X	**Goo**gle Cloud: GCP requires multi-factor authentication to be used by administrators who have access to GCP production environment. Authentication controls including hardware/software as their second factor is required. **Customers**: Customers are responsible for managing and implementing the strong authentication requirements including multi-factor authentication for all remote access into the 3DE. If GCP products are utilized by customer to meet this control, GCP-provided documentation should be used for configuring these services.
4.3.2 Remote access to the 3DE is controlled and documented, including: · System components for which remote access is permitted · The location(s) from which remote access is permitted · The conditions under which remote access is acceptable · Individuals with remote access permission · The access privileges applicable to each authorized use	Examine policies and procedures. Observe remote access controls. Interview personnel.	Remote access processes should be fully documented to ensure access is only granted to users or systems that have been previously approved for such access. Disconnection of remote access sessions after a period of inactivity should be considered. Policies and operational procedures should be kept up to date so personnel understand the proper processes and to prevent unauthorized access to the network.			X	**Google Cloud:** Google has access control and monitoring procedures in place for managing remote access to the GCP environment where GCP products are hosted. **Customers:** Customers are responsible for managing and implementing the strong authentication requirements including remote access into the 3DE. If GCP products are utilized by customer to meet this control, GCP-provided documentation should be used for configuring these services.

P2-4. Secure logical access to 3DS systems
In addition to ensuring strong access controls and account management for the 3DS environment, certain types of access present a higher risk and require more stringent controls to prevent them from being misused or compromised.

3DS PART 2 CORE SECURITY STANDARD REQUIREMENTS	VALIDATION REQUIREMENTS	GUIDANCE	CONTROL			SUMMARY
			GCP	CLIENT	SHARED	
4.3.3 Where remote access using personally owned devices is permitted, strict requirements for their use are defined and implemented to include: · Device security controls are implemented and maintained as equivalent to corporate-owned devices. · Each device is explicitly approved by management.	Examine policies and procedures. Observe remote access controls. Interview personnel.	Remote access using a personally owned device should only be permitted under a strictly defined process that includes management approval and verification that the device could not impact the security of 3DS systems. Devices should be verified as meeting at least the same rigor of security as defined in the entity's security policies. Devices should be maintained and monitored via a centralized, secure device-management solution. Approval for the use of a personal device should be explicitly provided on a case-by- case basis, by an appropriate person who has assigned responsibilities for security. (See Requirement P2-2.1.2.)		X		**Customers**: Customers are fully responsible for managing policies around personally owned devices for users with remote access into 3DE. If GCP products are utilized by customer to meet this control, GCP-provided documentation should be used for configuring these services.
4.3.4 Remote access privileges are monitored and/or reviewed at least quarterly by an authorized individual to confirm access is still required.	Examine documented processes. Examine evidence of monitoring and/or reviews. Interview personnel.	Remote access privileges should be regularly reviewed, at least quarterly, by an authorized individual. Documentation of reviews should be retained. Results of these reviews should include identification and removal of any unneeded or incorrect access, and should ensure that only individuals with a current business need are granted remote access. Automated processes may be used to assist in reviewing access privileges—for example, to generate notifications when an account has not been used for a period of time. Organizational processes to actively review and change access when an individual changes job function can also assist.			X	**Google Cloud:** Google has processes in place for continuous monitoring and review of users and access to GCP environment where GCP products are hosted. **Customers:** Customers are responsible for monitoring and/or reviewing the remote access privileges on a minimum of quarterly basis. If GCP products are utilized by customer to meet this control, Google provided guidance documentation should be used for configuration of GCP products.
P2-4.4 Restrict Wireless Exposure						
4.4.1 3DS components (ACS, DS, 3DSS) do not use or connect to any wireless network.	Examine network diagrams. Observe implemented controls. Interview personnel.	To prevent 3DS components from being exposed to wireless networks, wireless-enabled devices should not be present within the 3DE. Additionally, ACS, DS, and 3DSS system components should not use or be connected to any wireless-enabled components. Any wireless networks and devices used or supported by the 3DS entity— for example, for remote users—should be properly secured and configured in accordance with industry standards.	X			**Goo**gle Cloud: Google disallows wireless networking access, and acitvely scans and prevents unauthorized use of wireless networking in its production environment.
P2–4.5 Secure VPNs						

P2-4. Secure logical access to 3DS systems
In addition to ensuring strong access controls and account management for the 3DS environment, certain types of access present a higher risk and require more stringent controls to prevent them from being misused or compromised.

3DS PART 2 CORE SECURITY STANDARD REQUIREMENTS	VALIDATION REQUIREMENTS	GUIDANCE	CONTROL			SUMMARY
			GCP	CLIENT	SHARED	
4.5.1 All VPNs that provide access to 3DE are properly configured to provide strong security communications and protect against eavesdropping, replay attacks, and man-in-the-middle attacks.	Examine configuration standards. Observe VPN controls. Interview personnel.	VPN configurations should be reviewed against industry-recommended implementations to verify security features are enabled. Use of a trusted CA, a third party that utilizes a chain-of-trust model to provide assurance for a particular certificate, is recommended. If an internal CA is used the internal CA also needs to be verified as meeting industry requirements such as TS101456.		X		**Google Cloud:** Google does not utilize VPNs for access to the production environment. Google provides strong security communication and protection against attacks using zero-trust microsegmentation using BeyondCorp (https://cloud.google.com/beyondcorp). **Customers:** Customers are responsible for ensuring if VPN technologies are used they are configured as per the requirements. If GCP products are utilized by customer to meet this control, GCP-provided documentation should be used for configuring these services.

P2-5. Protect 3DS data

Minimizing the distribution and amount of data to only that which is necessary helps to reduce the risk of data exposure. The use of data- specific controls provides a critical layer of protection when data is exposed to public or untrusted environments, and can also protect data in trusted environments in the event other security controls are circumvented.

3DS PART 2 CORE SECURITY STANDARD REQUIREMENTS	VALIDATION REQUIREMENTS	GUIDANCE	CONTROL			SUMMARY
			GCP	CLIENT	SHARED	
P2–5.1 Data lifecycle						
5.1.1 Policies and procedures for usage, flow, retention, and disposal of 3DS data are maintained and implemented.	Examine documented policies. Examine evidence of data usage, flow, retention and disposal. Interview personnel.	Policies should address protection of 3DS data throughout its lifecycle and be based on data sensitivity and legal and business requirements. Protection for data in transit, persistent storage, temporary storage, and memory should be defined. Documentation should explain the purpose, scope, retention goals, disposal requirements, and applicable legal and business requirements. Local or applicable laws supersede any defined practices regarding data storage—for example, PII Laws and breach notification laws should be included in data-classification and retention policies. Data should be classified according to its security need.		X		**Customers**: Customers are responsible for development of policies and procedures for managing 3DS data.
5.1.2 3DS data is retained only as necessary and securely purged when no longer needed.	Examine data retention schedule and data disposal process. Interview personnel. Observe data storage.	Data-retention schedules should be defined to identify what data needs to be retained, for how long, where that data resides, and procedures for its secure destruction as soon as it is no longer needed.		X		**Customers:** Customers are responsible for schedule and processes for retention and disposal of 3DS data.
P2–5.2 Data transmission						
5.2.1 Strong cryptography and security protocols are used to safeguard 3DS sensitive data during transmission.	Examine documentation describing methods for encrypting data. Examine configuration standards. Observe implemented controls.	Controls should be applied at all interfaces and locations where 3DS sensitive data (as defined in the PCI 3DS Data Matrix) is transmitted or received. This includes all transmissions over open or public networks, internal networks, and transmissions within and between 3DS system domains. 3DS sensitive data should be protected to a level that is at least equivalent to that identified in Annex D of the current version of EMV® 3DS Protocol and Core Functions Specification.			X	**Google Cloud:** Google implements strong cryptography and security protocols for applications and systems supporting GCP infrastructure and services. **Customers**: Customers are responsible for implementing strong cryptography and security protocols for the applications or servers managed within their 3DE. If GCP products are utilized by customer to meet this control, GCP-provided documentation should be used for configuring these services.
5.2.2 Fallback to insecure cryptographic protocols and configurations is not permitted.	Examine documentation describing methods for encrypting data. Examine configuration standards. Observe implemented controls.	Secure transmission of 3DS data requires use of trusted keys/certificates, a secure protocol for transport, and strong cryptography to encrypt the 3DS data. Connection requests from systems that do not support the required encryption strength, and that would result in an insecure connection, should not be accepted.			X	**Google Cloud:** Google implements strong cryptography and security protocols for applications and systems supporting GCP infrastructure and services. **Customers**: Customers are responsible for implementing strong cryptography and security protocols and ensuring fallback is not possible to insecure protocols or configurations. If GCP products are utilized by customer to meet this control, GCP-provided documentation should be used for configuring these services.
P2–5.3 TLS configuration						
5.3.1 All TLS communications between ACS, DS and 3DSS for purposes of 3DS transmissions use only allowed cipher suites, as defined in the *EMV® 3DS Protocol and Core*	Examine configuration standards and TLS configurations.	Refer to Annex D, "Approved Transport Layer Security Versions," in the current version of the EMV® 3DS Protocol and Core Functions Specification, to identify				**Customers**: Google does not manage communications between ACS, DS, or 3DSS systems. Customers are responsible for implementing strong cryptography and allowed cipher suites for TLS

P2-5. Protect 3DS data
Minimizing the distribution and amount of data to only that which is necessary helps to reduce the risk of data exposure. The use of data- specific controls provides a critical layer of protection when data is exposed to public or untrusted environments, and can also protect data in trusted environments in the event other security controls are circumvented.

3DS PART 2 CORE SECURITY STANDARD REQUIREMENTS	VALIDATION REQUIREMENTS	GUIDANCE	CONTROL			SUMMARY
			GCP	CLIENT	SHARED	
Functions Specification.	Observe TLS communications.	those cipher suites that shall be supported and those that must not be offered or supported. The Implementation Notes in Annex D may also contain additional considerations for TLS implementations. The use of 3DES and SHA-1 should be phased out, as they may be deprecated in future versions of the EMV® 3DS Protocol and Core Functions Specification.		X		communications as defined in the standard. If GCP products are utilized by customer to meet this control, GCP-provided documentation should be used for configuring these services.
5.3.2 3DS components (ACS, DS, and 3DSS) do not offer or support any cipher suite that identified as "not supported" in the *EMV® 3DS Protocol and Core Functions Specification*.	Examine configuration standards and TLS configurations. Observe TLS communications.			X		**Customers:** Google does not manage cipher suites utilized for ACS, DS, or 3DSS systems. Customers are responsible for restricting use of disallowed cipher suites for TLS communications as defined in the standard. If GCP products are utilized by customer to meet this control, GCP-provided documentation should be used for configuring these services.
5.3.3 TLS configurations do not support rollback to unapproved algorithms, key sizes, or implementations.	Examine configuration standards and TLS configurations. Observe TLS communications.	TLS configurations may not support rollback to unapproved algorithms, key sizes, or implementations.			X	**Google Cloud:** Google implements strong cryptography and security protocols for applications and systems supporting GCP infrastructure and services. **Customers**: Customers are responsible for implementing strong cryptography and restricting rollback to unapproved algorithms, key sizes, or implementations, as defined in the standard. If GCP products are utilized by customer to meet this control, GCP-provided documentation should be used for configuring these services.
5.3.4 Controls are in place to monitor TLS configurations to identify configuration changes and to ensure secure TLS configuration is maintained.	Observe implemented controls for monitoring and maintaining TLS configurations. Interview personnel.	A combination of tools and processes should be considered to ensure an appropriate level of monitoring is implemented. Examples of controls include real-time monitoring, change-detection software, and analysis of audit logs. Continuous monitoring is recommended to prevent, detect, and allow timely response to unauthorized modifications or use of non- permitted configurations. The implemented controls should provide continued assurance that TLS is properly configured and using only approved cipher suites.			X	**Google Cloud:** Google monitors configurations to ensure secure TLS configurations are maintained for transmission of data between its services and networks. **Customers**: Customers are responsible for monitoring its TLS configuration, as defined in the standard. If GCP products are utilized by customer to meet this control, GCP-provided documentation should be used for configuring these services.
P2–5.4 Data Storage						
5.4.1 Storage of 3DS sensitive data is limited to only permitted data elements.	Examine data flows and 3DS transaction processes. Observe data storage.	The PCI 3DS Data Matrix identifies storage restrictions for 3DS sensitive data elements. Where storage of a particular data element is not permitted, the 3DS entity should be able to confirm that the data element is not stored to any persistent media—including to any hard drive, portable media or other data storage device—for any period of time or for any reason. The presence of these data elements in volatile memory is permitted as needed for 3DS transaction purposes; however, controls should be implemented to prevent data in memory being inadvertently copied to persistent media.		X		**Customers**: Customers are responsible for documenting the data flows and 3DS transaction processes. Customers are responsible for implementing the controls and configurations for storage of 3DS sensitive data. If GCP products are utilized by customer to meet this control, GCP-provided documentation should be used for configuring these services.

P2-5. Protect 3DS data
Minimizing the distribution and amount of data to only that which is necessary helps to reduce the risk of data exposure. The use of data- specific controls provides a critical layer of protection when data is exposed to public or untrusted environments, and can also protect data in trusted environments in the event other security controls are circumvented.

3DS PART 2 CORE SECURITY STANDARD REQUIREMENTS	VALIDATION REQUIREMENTS	GUIDANCE	CONTROL			SUMMARY
			GCP	CLIENT	SHARED	
5.4.2 Strong cryptography is used to protect any permitted storage of 3DS sensitive data.	Examine documentation describing methods for protecting stored data. Observe implemented controls and configurations.	3DS sensitive data—as identified in the PCI 3DS Data Matrix—should be protected wherever it is stored, using industry-recognized methods for strong cryptography. The cryptographic control may be applied either to the individual data elements or to the entire data packet or file that contains the data element. For example, where an element of 3DS sensitive data is contained in a transaction log with other data, encryption may be applied to the entire log or to only the sensitive data elements within the log. Strong cryptographic controls include one-way hash functions that use an appropriate algorithm and a strong input variable, such as a "salt." Hash functions are appropriate when there is no need to retrieve the original data, as one-way hashes are irreversible. Alternatively the data can be protected using cryptography based on an industry-tested and accepted algorithm (not a proprietary or "home-grown" algorithm) with strong cryptographic keys. Associated key-management processes and procedures are defined in Requirement P2-6. Refer to industry standards and best practices for information on strong cryptography and secure protocols (e.g., NIST SP 800-52 and SP 800-57, OWASP, etc.).		X		**Customers**: Customers are responsible for documenting methods for protecting stored data. Customers are responsible for implementing the controls and configurations for storage and protection of 3DS sensitive data. If GCP products are utilized by customer to meet this control, GCP-provided documentation should be used for configuring these services.
P2–5.5 Monitor 3DS transactions						
5.5.1 3DS transactions are monitored to identify, log, and alert upon anomalous activity.	Examine documented procedures and configuration standards. Examine log files. Observe implemented controls. Interview personnel.	Maintaining a baseline of normal 3DS traffic and transaction patterns will assist in identifying anomalous behaviors and developing use cases. All identified deviations should be ranked by risk level and responded to accordingly. In addition to real-time monitoring and analysis, frequent reviews of network traffic and correlation of audit logs may identify potentially suspicious activity. Response processes should include specific investigative activities, escalation, and notification, in accordance with the entity's incident response plan.		X		**Customers**: Customers are responsible for documenting procedures, and maintaining standards for identifying, logging, and alerting upon anomalous activities. If GCP products are utilized by customer to meet this control, GCP-provided documentation should be used for configuring these services.
5.5.2 Anomalous or suspicious transaction activity is investigated and addressed in a timely manner.	Examine documented procedures and configuration standards. Examine log files. Observe implemented controls. Interview personnel.			X		**Customers**: Customers are responsible for procedures, configuration standards, and logs related to investigation and resolution of suspicious transaction activities. If GCP products are utilized by customer to meet this control, GCP-provided documentation should be used for configuring these services.

P2-6 Cryptography and Key Management

Proper management and use of cryptographic keys is critical to the continued security of any encryption implementation. Strong key- management practices prevent unauthorized or unnecessary access to the keys, which in turn could result in exposure of keys and compromise of data the keys are intended to protect.

3DS PART 2 CORE SECURITY STANDARD REQUIREMENTS	VALIDATION REQUIREMENTS	GUIDANCE	CONTROL			SUMMARY
			GCP	CLIENT	SHARED	
P2–6.1 Key management						
6.1.1 Policies and procedures for managing cryptographic processes and keys are maintained and implemented.	Examine documented policies and procedures. Interview personnel.	Policies should cover all cryptographic keys and processes used to protect the confidentiality and integrity of 3DS data and messages during transmission and storage, as well as all respective key-encrypting keys. Cryptographic key-management processes should be monitored and maintained to ensure adherence to the defined policies.			X	**Google Cloud:** Google has policies and procedures for managing keys and processes for applications and systems supporting GCP infrastructure and services, including Cloud KMS and Cloud HSM. Google offers Bare Metal Rack HSM and Bare Metal HSM as single-tenancy options for customers to host their own HSMs within GCP facilities, but is not responsible for management of any cryptographic keys on customer-owned HSMs. **Customers**: GCP customers are responsible for maintaining appropriate policies, procedures, processes for the creation, usage, and management of all customer-managed keys, including all keys on customer-owned HSMs.
6.1.2 *For ACS and DS only:* All key management activity for specified cryptographic keys (as defined in the *PCI 3DS Data Matrix*) is performed using an HSM that is either: · FIPS 140-2 Level 3 (overall) or higher certified, or · PCI PTS HSM approved.	Examine documented key-management procedures. Interview personnel.	The requirement to use an HSM applies to ACS and DS entities. The PCI 3DS Data Matrix identifies 3DS cryptographic key types required to be managed in an HSM. Key-management activities include key-encryption and decryption operations, as well as key lifecycle functions such as key generation and storage. The HSM approval documentation verifies the HSM is either: • Listed on the NIST Cryptographic Module Validation Program (CMVP) list, with a valid listing number, and approved to FIPS 140-2 Level 3 (overall) or higher. Refer to http://csrc.nist.gov. • Listed on the PCI SSC website, with a valid PCI SSC listing number, as an Approved PCI PTS Device under the approval class "HSM." While an HSM is required only for the keys specified in the PCI 3DS Data Matrix, use of an HSM for other 3DS keys is strongly recommended. All 3DS keys should be evaluated in accordance with the 3DS entity's risk- management policy to determine whether they should be managed in an HSM. It is not required that 3DSS entities use an HSM to manage 3DS keys; however it is strongly recommended. 3DSS entities are subject to all other key management requirements in this standard.			X	**Google Cloud:** Google is not involved in management of ACS and DS components identified within the requirement. Google Cloud offers Cloud HSM, Bare Metal Rack HSM, and Bare Metal HSM offerings to customers for key management activities that are FIPS 140-2 Level 3 certified. **Customers:** ACS and DS customers are responsible to ensure all management of in-scope keys use HSMs that meet this control. ACS and DS customers providing customer-owned HSMs for use with Bare Metal Rack HSM or Bare Metal HSM are responsible to ensure selected devices meet this requirement and that all key management activities are performed on such devices.
6.1.3 *For ACS and DS only:* The HSM is deployed securely, in accordance with the security policy, as follows: · If FIPS-approved HSMs are used, the HSM uses the FIPS-approved cryptographic primitives, data-protection mechanisms, and key-management processes for account data decryption and related processes	Examine HSM approval documentation / security policy (as applicable).	An integral component of a PCI PTS or FIPS certification is the HSM security policy, which defines how to configure and operate the HSM in accordance with the certification. The security policy enforced by the HSM should not allow unauthorized or unnecessary functions. HSM API functionality and commands that are not required to support specified functionality				**Google Cloud:** Google is not involved in management of ACS and DS components identified within the requirement. Google Cloud offers Cloud HSM, Bare Metal Rack HSM, and Bare Metal HSM offerings to customers for key management activities that are FIPS 140-2 Level 3 certified. **Customers:** ACS and DS customers using Bare Metal Rack HSM or Bare

P2-6 Cryptography and Key Management

Proper management and use of cryptographic keys is critical to the continued security of any encryption implementation. Strong key- management practices prevent unauthorized or unnecessary access to the keys, which in turn could result in exposure of keys and compromise of data the keys are intended to protect.

3DS PART 2 CORE SECURITY STANDARD REQUIREMENTS	VALIDATION REQUIREMENTS	GUIDANCE	CONTROL			SUMMARY
			GCP	CLIENT	SHARED	
decryption and related processes. · If PCI PTS-approved HSMs are used, the HSM is configured to operate in accordance with the security policy that was included in the PTS HSM approval, for all operations (including algorithms, data protection, key management, etc.).	Observe HSM configurations.	commands that are not required to support specified functionality should be disabled before the HSM is commissioned. When HSMs are connected to online systems, controls should be in place to prevent the HSM being used to perform privileged or sensitive functions that are not available during routine HSM operations. Examples of sensitive functions include but are not limited to: loading of key components, outputting clear-text key components, and altering HSM configuration.			X	**Customers:** ACS and DS customers using Bare Metal Rack HSM or Bare Metal HSM are responsible for ensuring customer-owned HSMs are deployed in accordance with the FIPS or PCI PTS security policy.
6.1.4 A documented description of the cryptographic architecture exists that includes: · Description of the usage for all keys · Details of all keys used by each HSM (if applicable)	Examine documented description of the cryptographic architecture. Interview personnel. Examine HSM approval documentation.	Cryptographic keys must be stored and functions handled securely to prevent unauthorized or unnecessary access that could result in the exposure of keys and compromise cardholder data			X	**Google Cloud:** Google offers several products to customers for management of cryptographic keys that may be used for protection of 3DS sensitive data. Google documents its own cryptographic architecture for management and usage of Google-managed keys in support of Cloud KMS and Cloud HSM. Google neither manages nor has access to any cryptographic keys managed in customer-owned HSMs (e.g., Bare Metal Rack HSM, Bare Metal HSM). **Customers**: Customers are responsible for documentation related to all customer-managed keys applicable to their 3DS environment.
6.1.5 Cryptographic keys are securely managed throughout the cryptographic lifecycle including: · Generation · Distribution/conveyance · Storage · Established crypto periods · Replacement/rotation when the crypto period is reached · Escrow/backup · Key compromise and recovery · Emergency procedures to destroy and replace keys · Accountability and audit	Examine documented key-management procedures. Observe key-management activities. Interview personnel.	A good key-management process, whether manual or automated, is based on industry standards and addresses all elements of the key lifecycle. Applicable standards include NIST Special Publication 800-57 (all parts), Special Publication 800-130, ISO 11568, and ISO/IEC 11770—including associated normative references cited within as applicable. For example, the generation and use of deterministic random numbers should conform to NIST Special Publication 800-90A, ISO/IEC 18031, or equivalent. Keys should only be distributed in a secure manner, never in the clear, and only to designated custodians or recipients. Procedures for distribution apply both within the entity and across 3DS domains. Secret and private keys should be encrypted with a strong key-encrypting key that is stored separately, or be stored within a secure cryptographic device (such as a HSM), or be stored as at least two full-length key components or key shares, in accordance with an industry-accepted method. The existence of clear-text keys during data-encryption/decryption operations should be limited to the minimum time needed for its purpose—for example, where clear-text keys may temporarily exist in memory, they should be securely purged from memory upon completion of the encryption/decryption operation. A crypto period should be identified for each key based on a risk			X	**Google Cloud:** Google offers several products to customers for management of cryptographic keys that may be used for protection of 3DS sensitive data. Google documents its own cryptographic architecture for management and usage of Google-managed keys in support of Cloud KMS and Cloud HSM. Google neither manages nor has access to any cryptographic keys managed in customer-owned HSMs (e.g., Bare Metal Rack HSM, Bare Metal HSM). **Customers**: Customers are responsible for secure lifecycle management of all customer-managed keys applicable to their 3DS environment

P2-6 Cryptography and Key Management
Proper management and use of cryptographic keys is critical to the continued security of any encryption implementation. Strong key- management practices prevent unauthorized or unnecessary access to the keys, which in turn could result in exposure of keys and compromise of data the keys are intended to protect.

3DS PART 2 CORE SECURITY STANDARD REQUIREMENTS	VALIDATION REQUIREMENTS	GUIDANCE	CONTROL			SUMMARY
			GCP	CLIENT	SHARED	
6.1.6 Cryptographic key-management processes conform to recognized national or international key-management standards.	Examine documented key-management procedures. Observe key-management activities. Interview personnel.	A crypto-period should be identified for each key based on a risk assessment, and keys changed when this period is reached. Additionally, keys should be destroyed and replaced immediately upon suspicion of a compromise. Secure key-management practices include minimizing access to keys to the fewest number of custodians necessary, enforcing split knowledge and dual control for activities involving clear-text keys or key components, and defining roles and responsibilities for key custodians and key managers.			X	**Google Cloud**: Google offers several products to customers for management of cryptographic keys that may be used for protection of 3DS sensitive data. Google documents its own cryptographic architecture for management and usage of Google-managed keys in support of Cloud KMS and Cloud HSM. Google neither manages nor has access to any cryptographic keys managed in customer-owned HSMs (e.g., Bare Metal Rack HSM, Bare Metal HSM). **Customers**: Customers are responsible for ensuring the key-management processes used for management of customer-managed keys conform to recognized standards.
6.1.7 Cryptographic keys are used only for their intended purpose, and keys used for 3DS functions are not used for non-3DS purposes.	Examine documented key-management procedures. Interview personnel.	Cryptographic keys should only be used for the purpose they were intended—for example, a key-encryption key should never be used to encrypt 3DS sensitive data. Similarly, public and private keys should only be used for a single defined purpose—private keys should be used either for decryption or for creating digital signatures, and public keys used only for encryption or for verifying digital signatures. Keys used to protect 3DS transactions or data should not be used for any business function other than their 3DS purpose.			X	**Google Cloud**: Google offers several products to customers for management of cryptographic keys that may be used for protection of 3DS sensitive data. Google documents its own cryptographic architecture for management and usage of Google-managed keys in support of Cloud KMS and Cloud HSM. Google neither manages nor has access to any cryptographic keys managed in customer-owned HSMs (e.g., Bare Metal Rack HSM, Bare Metal HSM). **Customers**: Customers are required to verify that customer-managed cryptographic keys are used only for their intended purpose, and keys used for 3DS functions are not used for other non-3DS purposes.
6.1.8 A trusted Certificate Authority is used to issue all digital certificates used for 3DS operations between 3DSS, ACS, and DS components.	Examine documented evidence of Certificate Authority validation (e.g., security assessments, certifications). Observe implemented digital certificates.	Entities need to ensure that the Certificate Authority (CA) that they use has robust security controls to ensure the security of 3DS protocols and to verify a chain of trust. Refer to Section 6.1, "Links," in the current version of the EMV® 3DS Protocol and Core Functions Specification to identify connections between 3DSS, ACS, and DS components that require digital certificates. The CA could be approved by a payment brand or could undergo a security assessment, conducted by the entity or other third party, against an industry-standard framework such as ISO 27001. The assessment should confirm the CA has robust controls around security, processing integrity, confidentiality, online privacy, and availability. Entities can also leverage WebTrust, an assurance service jointly developed by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA).		X		**Customers:** Google does not have knowledge of or manages certificates used for 3DSS, ACS, or DS components. Customers are fully responsible for ensuring a trusted Certificate Authority is used to issue digital certificates between 3DS components. If GCP products are utilized by customer to meet this control, GCP-provided documentation should be used for configuring these services.

P2-6 Cryptography and Key Management

Proper management and use of cryptographic keys is critical to the continued security of any encryption implementation. Strong key- management practices prevent unauthorized or unnecessary access to the keys, which in turn could result in exposure of keys and compromise of data the keys are intended to protect.

3DS PART 2 CORE SECURITY STANDARD REQUIREMENTS	VALIDATION REQUIREMENTS	GUIDANCE	CONTROL			SUMMARY
			GCP	CLIENT	SHARED	
6.1.9 Audit logs are maintained for all key-management activities and all activities involving clear-text key components. The audit log includes: · Unique identification of the individual that performed each function · Date and time · Function being performed · Purpose · Success or Failure of activity"	Examine documented key-management procedures. Examine audit logs. Interview personnel.	Recording the function or key-management activity being performed (for example, key loading), and the purpose of the affected key (for example, 3DS data encryption) provides the entity with a complete and concise record of key-management activities. Identifying whether the activity resulted in success or failure confirms the status upon conclusion of the activity. By recording these details for the auditable events, a potential compromise can be quickly identified with sufficient detail to know who, what, where, when, and how.			X	**Google Cloud:** Google offers several products to customers for management of cryptographic keys that may be used for protection of 3DS sensitive data. Google documents its own cryptographic architecture for management and usage of Google-managed keys in support of Cloud KMS and Cloud HSM. Google neither manages nor has access to any cryptographic keys managed in customer-owned HSMs (e.g., Bare Metal Rack HSM, Bare Metal HSM). **Customers**: Customers are responsible for maintaining audit logs for all activities related to customer-managed keys or clear-text key components.
6.1.10 Incident response procedures include activities for reporting and responding to suspicious or confirmed key-related issues.	Examine documented incident response procedures. Interview personnel.	The appropriate personnel should be notified immediately of any breach impacting the keys. Documented procedures should explain how this issue would be escalated for further investigation and resolution, including initiation of the entity's incident response procedures.			X	**Google Cloud**: Google offers several products to customers for management of cryptographic keys that may be used for protection of 3DS sensitive data. Google documents its own cryptographic architecture for management and usage of Google-managed keys in support of Cloud KMS and Cloud HSM. Google neither manages nor has access to any cryptographic keys managed in customer-owned HSMs (e.g., Bare Metal Rack HSM, Bare Metal HSM). **Customers**: Customers are responsible for documenting and implementing incident response procedures for customer-managed keys.
P2–6.2 Secure Logical Access to HSMs (*For ACS and DS only*)						
6.2.1 Personnel with logical access to HSMs must be either at the HSM console or using an HSM non-console access solution that has been evaluated by an independent laboratory to comply with the following sections of the current version of ISO 13491: · Annex A – Section A.2.2: Logical security characteristics. · Annex D – Section D.2: Logical security characteristics. (Note: The use of single DEA message authentication codes is not permitted.) · Annex E – Section E.2.1: Physical security characteristics, and Section E.2.2 Logical security characteristics. (Note: Only random number generators meeting the requirements of SP 800-90A are allowed.) · Annex F – Section F.2.1: Physical security characteristics, and Section F.2.2 Logical security characteristics. · If digital signature functionality is provided: Annex G – Section G.2.1 General considerations, and Section G.2.2 Device management for digital signature verification.	Examine systems configurations. If non-console access is used: - Examine documented evidence (e.g., lab certification letters, solution technical documentation, or vendor attestation) that the solution has been validated to applicable ISO requirements. - Observe implemented solution.	HSMs have high security needs, and additional controls are necessary to restrict and protect logical access to these systems. If personnel have network (non-console) access to HSMs, the security of the HSM non- console access solution is critical to the overall security of the HSM itself. Examples of personnel access include for purposes of maintenance, configuration, updating, administration, and general management of the HSM. Use of non-console access solution is not required for application or system accounts performing automated functions. An HSM non-console access solution is typically comprised of both hardware components (for example, network appliances and smart cards) and software components (for example, client-side applications) that define and manage how non-console access is handled. For additional assurance that only authorized persons can access the HSM, the use of multi-factor authentication for all personnel access should also be considered. An independent laboratory is one that is organizationally independent of the non-console management solution vendor and is not otherwise subject to any commercial, financial, or other commitment that might influence its evaluation of the vendor's product.			X	**Google Cloud:** Google is not involved in management of ACS and DS components identified within the requirement. All service processes used in Google-managed HSMs are performed using application-level accounts and are thus not subject to this control. Where emergency procedures for Cloud HSM require remote logical access to these HSMs, Google has been assessed to the Alternative Set of Requirements and confirmed to use MFA for all such connections. **Customers**: ACS and DS customers using Cloud HSM are fully responsible for managing CMEK, including ensuring any non-console logical access uses only HSM access solutions which have been independently tested to comply with the identified annexes of ISO 13491. ACS and DS customers using Bare Metal Rack HSM or Bare Metal HSM are fully responsible for managing CMEK and customer-owned HSMs, whether prior to deployment, at the physical console within Google facilities (Bare Metal Rack HSM only), or via a non-console access solution that has been independently tested to comply with the identified annexes of ISO 13491.
	P2-6.2 Alternative Set of Requirements, per "3DS Core v1.x Technical FAQs" published September 2023:					**Where validating P2-6 to the Alternative Set of Requirements:** **Customers:** ACS and DS customers using Cloud HSM, Bare Metal Rack HSM, or Bare Metal HSM are fully responsible for managing CMEK including ensuring any non-console logical access for management and configuration of

P2-6 Cryptography and Key Management
Proper management and use of cryptographic keys is critical to the continued security of any encryption implementation. Strong key- management practices prevent unauthorized or unnecessary access to the keys, which in turn could result in exposure of keys and compromise of data the keys are intended to protect.

3DS PART 2 CORE SECURITY STANDARD REQUIREMENTS	VALIDATION REQUIREMENTS	GUIDANCE	CONTROL			SUMMARY
			GCP	CLIENT	SHARED	
	(P2-6.2.1) Non-console HSM access for the purposes of management and configuration requires the use of MFA.				X	HSMs via non-console access enforces use of MFA. If GCP products are utilized by customer to meet this control, GCP-provided documentation should be used for configuring these services.
6.2.2 All non-console access to HSMs originates from a 3DE network(s).	Examine network and system configuration settings.	To ensure that non-console access to HSMs originates from a secure location, such access may only be provided to systems located within a 3DS environment (3DE) that is protected in accordance with the requirements in this standard.			X	**Google Cloud:** Google is not involved in management of ACS and DS components identified within the requirement. All service processes used in Google-managed HSMs are performed using application-level accounts and are thus not subject to this control. Where emergency procedures for Cloud HSM require remote logical access to these HSMs, Google has been assessed to the Alternative Set of Requirements and confirmed to use MFA for all such connections. **Custome**rs: ACS and DS customers are responsible for configuring and implementing non-console access to the HSM such that it is only accessible from secured 3DE network(s). Where such network is outside the GCP network, the customer is responsible for all physical and logical security controls for this environment.
	P2-6.2 Alternative Set of Requirements, per "3DS Core v1.x Technical FAQs" published September 2023: (P2-6.2.2) Non-console HSM access for the purposes of management and configuration is performed using a secure channel.				X	**Where validating P2-6 to the Alternative Set of Requirements:** **Customers:** ACS and DS customers are responsible for enforcing secure channel for management and configuration of HSMs via non-console access. If GCP products are utilized by customer to meet this control, GCP-provided documentation should be used for configuring these services.
6.2.3 Devices used to provide personnel with non-console access to HSMs are secured as follows: · Located in a designated secure area or room that is monitored at all times. · Locked in room/rack/cabinet/ drawer/safe when not in use. · Physical access is restricted to authorized personnel and managed under dual control. · Authentication mechanisms (e.g., smart cards, dongles etc.) for devices with non-console access are physically secured when not in use. · Operation of the device requires dual-control and multifactor authentication. · Devices have only applications and software installed that is necessary. · Devices are verified as having up-to-date security configurations. · Devices cannot be connected to other networks while connected to the HSM. · Devices are cryptographically authenticated prior to the connection being granted access to HSM functions.	Observe locations of devices used for non-console access to HSMs. Observe device configurations. Observe HSM authentication mechanisms	The term "devices" refers to the endpoint device (for example, a PC, laptop, terminal, or secure cryptographic device) that an individual is using to access the HSM via a non-console connection. The implemented physical and logical security controls should provide assurance that devices are being used only as intended, and only by authorized personnel. The specific security configurations for each device will depend on its particular technology and function. In order to prevent malicious individuals from "piggy-backing" on an authorized connection, devices should only be connected to the network used to access the HSM. For example, connectivity on multi-homed devices should be disabled for all but the interface accessing the HSM, and any VPN/SSH tunnels to other networks should be closed before opening a tunnel to the HSM. Methods to verify that only authorized devices are permitted to connect to the HSM can include digital signatures and other cryptographic techniques. All non-console access to HSMs should occur only over a secure communication channel, such as a VPN that meets Requirement 4.4.			X	**Google Cloud:** Google is not involved in management of ACS and DS components identified within the requirement. All service processes used in Google-managed HSMs are performed using application-level accounts and are thus not subject to this control. Where emergency procedures for Cloud HSM require remote logical access to these HSMs, Google has been assessed to the Alternative Set of Requirements and confirmed to use MFA for all such connections. **Customers**: ACS and DS customers are responsible for protecting access to the area or room as outlined in the requirement for any non-console access to the HSMs. Where such network is outside the GCP network, the customer is responsible for all physical and logical security controls for this environment.
	Alternate Validation Requirements, per "3DS Core v1.x Technical FAQs" published September 2023: (P2-6.2.3) Secret or private				X	**Where validating P2-6 to the Alternative Set of Requirements:** **Customers:** ACS and DS customers are responsible for enforcing dual control and split knowledge for management and configuration of HSMs via non-console access. If GCP products are utilized by customer to meet this control, GCP-provided documentation should be used for configuring these

P2-6 Cryptography and Key Management

Proper management and use of cryptographic keys is critical to the continued security of any encryption implementation. Strong key- management practices prevent unauthorized or unnecessary access to the keys, which in turn could result in exposure of keys and compromise of data the keys are intended to protect.

3DS PART 2 CORE SECURITY STANDARD REQUIREMENTS	VALIDATION REQUIREMENTS	GUIDANCE	CONTROL			SUMMARY
			GCP	CLIENT	SHARED	
	(P2-6.2.3) Secret or private cryptographic keys, key components, and/or key shares input to or output from the HSM are secured through dual control and split knowledge.				X	control, GCP-provided documentation should be used for configuring these services.
6.2.4 The loading and exporting of clear-text cryptographic keys, key components and/or key shares to/from the HSM is not performed over a non-console connection.	Examine device configurations.	Non-console access to HSMs should only be used for the purpose of HSM maintenance/administration. Because the loading and export of clear-text keys, key components, and key shares requires a higher assurance of physical security, all such activities are required to be performed at the HSM.		X		**Google Cloud:** For Cloud HSM, Google prevents customer-managed keys from being imported or exported in clear-text, leveraging PKCS#11 key wrapping (using method CKM_RSA_AES_KEY_WRAP). For Bare Metal Rack HSM and Bare Metal HSM, Google is not responsible for ensuring clear-text key material is not loaded or exported over a non-console connection. **Customers**: For Bare Metal Rack HSM and Bare Metal HSM, ACS and DS customers are fully responsible for ensuring that loading and exporting of clear-text keys and key components for the cryptographic keys does not occur over a non-console connection.
	Alternate Validation Requirements, per "3DS Core v1.x Technical FAQs" published September 2023: (P2-6.2.4) Non-console access used for the loading of clear-text key components or key shares originates from a Secure Cryptographic Device (SCD), that is either: - Listed on the NIST Cryptographic Module Validation Program (CMVP) list and approved to FIPS 140-2 Level 3 or 140-3 Level 3 (overall) or higher. Refer to http://csrc.nist.gov. Or, - Listed on the PCI SSC website, with a valid PCI SSC listing number, as an Approved PCI PTS Device			X		**Where validating P2-6 to the Alternative Set of Requirements:** **Customers:** ACS and DS customers are responsible to ensure all management of in-scope keys use HSMs that meet this control. ACS and DS customers providing customer-owned HSMs for use with Bare Metal Rack HSM or Bare Metal HSM are responsible to ensure selected devices meet this requirement and that all key management activities are performed on such devices.
6.2.5 Activities performed via non-console access adhere to all other HSM and key-management requirements.	Examine policies and procedures. Interview personnel. Examine HSM configurations and observe connection processes.	If personnel are not physically at the HSM console, additional controls may be necessary to ensure that the 3DS entity's policies and procedures around key management and HSM usage are adhered to. For example, if the ability to access an HSM function or key-management activity requires dual control, and the activity or function can be accessed by personnel physically at the HSM console or over a non-console (network) connection, the requirements for dual control need to be enforced over both methods of access.			X	**Google Cloud:** Google is not involved in management of ACS and DS components identified within the requirement. All service processes used in Google-managed HSMs are performed using application-level accounts and are thus not subject to this control. Where emergency procedures for Cloud HSM require remote logical access to these HSMs, Google has been assessed to the Alternative Set of Requirements and confirmed to use MFA for all such connections. **Customers**: Customers are responsible for adhering to all other HSM and key management requirements performed via non-console access.

P2-6 Cryptography and Key Management
Proper management and use of cryptographic keys is critical to the continued security of any encryption implementation. Strong key- management practices prevent unauthorized or unnecessary access to the keys, which in turn could result in exposure of keys and compromise of data the keys are intended to protect.

3DS PART 2 CORE SECURITY STANDARD REQUIREMENTS	VALIDATION REQUIREMENTS	GUIDANCE	CONTROL			SUMMARY
			GCP	CLIENT	SHARED	
	Alternate Validation Requirements, per "3DS Core v1.x Technical FAQs" published September 2023: (P2-6.2.5) When loaded through a non-console interface, key components and key shares are encrypted using a key encryption key that is specific for the purposes of key transport. Use of encryption provided by a secure channel is not sufficient to meet this requirement.				X	**Where validating P2-6 to the Alternative Set of Requirements:** **Customers:** ACS and DS customers are responsible to ensure all management of in-scope keys use HSMs that meet this control. ACS and DS customers providing customer-owned HSMs for use with Bare Metal Rack HSM or Bare Metal HSM are responsible to ensure selected devices meet this requirement and that all key management activities are performed on such devices.
P2–6.3 Secure Physical Access to HSMs *(For ACS and DS only)*						
6.3.1 HSMs are stored in a dedicated area(s).	Examine 3DS device inventory. Observe physical locations of HSMs.	Physical access to HSMs requires passing an additional physical control— e.g., via locked cabinets or cages, or a separate secure room. HSMs could be in multiple racks within the same dedicated physical space, or in one or more dedicated rooms, and so on. Where HSMs are in a data center managed by the 3DS entity, the HSMs should be in a space dedicated to HSMs and HSM-management devices. Where a 3DS entity's HSMs are in a shared data center, such as a co- location facility, the 3DS entity's HSMs should be in a space that is dedicated to the entity's systems and is physically separate from all other customers of the co-location facility. Dual control requires two or more people to perform a function, and no single person can access or use the authentication materials of another.	X			**Goo**gle Cloud: Google stores all HSMs for Cloud HSM, Bare Metal Rack HSM, and Bare Metal HSM in dedicated HSM racks, and leverages physical, logical, and procedural controls to prevent access to another customer's HSMs.
6.3.2 Physical access to the HSMs is restricted to authorized personnel and managed under dual control.	Examine documented procedures. Observe access controls.				X	**Goo**gle Cloud: Google maintains Bare Metal HSM devices in racks specific to the Bare Metal HSM service, and maintains Bare Metal Rack HSM devices in customer-dedicated racks. **Customers**: Customers are responsible for managing physical access under dual control at the locations where HSMs are provisions or decommissioned outside of Google Cloud facilities. Bare Meta Rack HSM customers are responsible for maintaining procedures ensuring customer access to production HSMs is restricted to authorized personnel.

P2-7 Physically secure 3DS systems
As ACS and DS systems are critical components of the 3DS infrastructure, they require a secure facility with elevated physical security controls to restrict, manage, and monitor all physical access.

3DS PART 2 CORE SECURITY STANDARD REQUIREMENTS	VALIDATION REQUIREMENTS	GUIDANCE	CONTROL			SUMMARY
			GCP	CLIENT	SHARED	
P2-7.1 Data center security						
7.1.1 ACS and DS systems are hosted in data center environments.	Observe ACS/DS locations.	Data centers should apply controls across a number of levels—for example, door-entry controls may be applied at room level within the data center, at an outer level that must be passed through to access the data center, or a combination of both. Some controls may also be applied at rack level—for example, where the 3DS component is in a secured rack. However the controls are implemented, they must ensure that access to the 3DS component is controlled and monitored as defined in these requirements.	X			**Goo**gle Cloud: Google is responsible for all physical security controls for production Google Cloud facilities. (Customers are responsible for managing the physical security of systems not managed within the Google Cloud environment.)
7.1.2 Data centers supporting ACS and DS are equipped with a positively controlled single-entry portal (e.g., mantrap), that: · Requires positive authentication prior to granting entry; and · Grants entry to a single person for each positive authentication.	Observe data center entry points.	A positively controlled mantrap is typically a small room with an entry door on one wall and an exit door on the opposite wall. One door of a mantrap cannot be unlocked and opened until the opposite door has been closed and locked. Access controls can be a combination of automated (for example, electronic access cards and physical barriers) and manual (for example, a human security guard performing visual verification and confirmation of identity). These controls ensure that the second door is not opened until authentication is complete, and that only one individual is provided access per authentication.	X			**Goo**gle Cloud: Google is responsible for all physical security controls for production Google Cloud facilities. (Customers are responsible for managing the physical security of systems not managed within the Google Cloud environment.)
7.1.3 Doors to areas within the data center that contain 3DS systems are fitted with an electronic access control system (e.g., card reader, biometric scanner) that controls and records all entry and exit activities.	Observe all entrances to the 3DE. Examine audit logs and/or other access records.	Electronic access-control systems, such as a keypad with individually assigned PIN codes or individually assigned access cards, provide assurance that the individual gaining access is who they claim to be. To provide additional protection against the unauthorized use of an individual's credential, multi-factor authentication should be considered.	X			**Goo**gle Cloud: Google is responsible for all physical security controls for production Google Cloud facilities. (Customers are responsible for managing the physical security of systems not managed within the Google Cloud environment.)
7.1.4 Multi-factor authentication is required for entry to telecommunications rooms that are not located within a	Examine access controls.	A telecommunications room is a room or space where communications are consolidated and distributed.				**Google Cloud:** Google is responsible for all physical security controls for production Google Cloud facilities. (Customers are

P2-7 Physically secure 3DS systems
As ACS and DS systems are critical components of the 3DS infrastructure, they require a secure facility with elevated physical security controls to restrict, manage, and monitor all physical access.

3DS PART 2 CORE SECURITY STANDARD REQUIREMENTS	VALIDATION REQUIREMENTS	GUIDANCE	CONTROL			SUMMARY
			GCP	CLIENT	SHARED	
secure data center.	Observe access events.	Telecommunications rooms typically house communications equipment (such as switches and routers), cable termination points, and cross-connects serving a specific area and/or floor. Examples of multi-factor authentication for physical access include use of an access card with PIN/passcode and use of an access card with a biometric reader. Visual verification of government-issued photo ID by an authorized guard at the entry point may also be acceptable as one of the two factors. Multi-factor authentication is not required for physical access to telecommunications rooms housed within a	X			responsible for managing the physical security of systems not managed within the Google Cloud environment.) **Customers :** GCP customers are responsible for implementing the multi-factor authentication controls into the telecommunications rooms if applicable for their 3DE.
7.1.5 Entry controls prevent piggy-backing by granting access to a single person at a time, with each person being identified and authenticated before access is granted.	Observe personnel entering the data center.	Each individual is identified and authenticated before being granted access to the 3DS data centers. These controls provide assurance that the identity of every individual in the data center is known at any given time.	X			**Goo**gle Cloud: Google is responsible for all physical security controls for production Google Cloud facilities. (Customers are responsible for managing the physical security of systems not managed within the Google Cloud environment.)
7.1.6 A physical intrusion-detection system that is connected to the alarm system is in place.	Interview personnel. Observe intrusion-detection controls.	To be effective, an intrusion-detection system should be activated whenever the 3DS environment is intended to be unoccupied. The intrusion-detection system may be activated automatically or via manual process.	X			**Goo**gle Cloud: Google is responsible for all physical security controls for production Google Cloud facilities. (Customers are responsible for managing the physical security of systems not managed within the Google Cloud environment.)
7.1.7 Physical connection points leading into the 3DE are controlled at all times.	Observe physical connection points.	Securing networking and communications hardware prevents malicious users from intercepting network traffic or physically connecting their own devices to wired network resources.	X			**Google Cloud:** Google is responsible for all physical security controls for production Google Cloud facilities. (Customers are responsible for managing the physical security of systems not managed within the Google Cloud environment.)
P2–7.2 CCTV						
7.2.1 CCTV cameras are located at all entrances and emergency exit points and capture identifiable images, at all times of the day and night.	Observe all entrances and emergency exit points. Examine CCTV footage.	The cameras need to be able to identify individuals physically entering and exiting the area, even during dark periods, as this provides valuable information in the event of an investigation.	X			**Goo**gle Cloud: Google is responsible for all physical security controls for production Google Cloud facilities. (Customers are responsible for managing the physical security of systems not managed within the Google Cloud environment.)
7.2.2 CCTV recordings are time stamped.	Examine CCTV records.	Clocks need to be properly synchronized to ensure the captured images can be correlated to create an				**Goo**gle Cloud: Google is responsible for all physical security controls for production Google Cloud facilities. (Customers are

P2-7 Physically secure 3DS systems
As ACS and DS systems are critical components of the 3DS infrastructure, they require a secure facility with elevated physical security controls to restrict, manage, and monitor all physical access.

3DS PART 2 CORE SECURITY STANDARD REQUIREMENTS	VALIDATION REQUIREMENTS	GUIDANCE	CONTROL			SUMMARY
			GCP	CLIENT	SHARED	
		accurate record of the sequence of events. Synchronization may use automated or manual mechanisms.	X			responsible for managing the physical security of systems not managed within the Google Cloud environment.)