Google Cloud

Crown Commercial Service

Submission of Proposal

Google's Response to Crown Commercial Service Request for Proposal **RM1557.15 G-Cloud 15**

Date: *January, 30, 2026*

Service Description

Lot 1a - Infrastructure as a Service (IaaS) and Platform as a Service (PaaS)

GCP Service Name	GCP Service Description
App Engine	Enables you to build and host applications on the same systems that power Google applications. Offers fast development and deployment, simple administration, and effortless scalability.
Batch	A fully-managed service that allows you to create, schedule, and execute batch jobs at scale, natively integrated with Google Cloud storage, logging, and monitoring.
Blockchain Node Engine	A fully-managed node-hosting service for Web3 development.
Compute Engine	Offers scalable and flexible virtual machine computing capabilities in the cloud, with options to utilize certain CPUs, GPUs, or Cloud TPUs.
Google Cloud VMware Engine (GCVE)	A managed VMware-as-a-Service designed for running VMware workloads natively in a dedicated, private, software-defined data center on Google Cloud Platform.
VM Manager	A suite of tools that enables you to manage operating systems for virtual machine fleets running Windows and Linux on Compute Engine.
Workload Manager	A rule-based validation service that scans application workloads to detect deviations from standards, rules, and best practices to improve system quality, reliability, and performance.
Backup for GKE	Enables data protection for workloads running in Google Kubernetes Engine clusters.
Cloud Storage	A RESTful service for storing and accessing data on Google's infrastructure, combining performance and scalability with advanced security and sharing capabilities.
Persistent Disk	A durable and high-performance block storage service (SSD and HDD) that can be attached to instances in Compute Engine or GKE.
Cloud Filestore	A scalable, highly available, fully-managed shared file service (NFS/POSIX) ideal for shared workloads.
*Cloud Storage for Firebase	Adds customizable Google security via Firebase Security Rules to file uploads and downloads for Firebase apps.
NetApp Volumes	A fully-managed file service powered by NetApp (ONTAP) enabling high-performance storage with SMB, NFS, and Multi-protocol file support.
AlloyDB	A fully-managed, PostgreSQL-compatible database designed for demanding transactional and analytical workloads with enterprise-grade performance.

Cloud Bigtable	A fast, fully-managed, highly-scalable NoSQL database service designed for data from 1TB to hundreds of PB.
Datastore	A fully-managed, schemaless, non-relational datastore with rich query capabilities and atomic transactions.
Firestore	A NoSQL document database for storing, syncing, and querying data for mobile and web apps, featuring live synchronization and offline support.
Memorystore	Provides a fully-managed in-memory data store service (Redis and Memcached) for sub-millisecond data access.
Cloud Spanner	A fully-managed, mission-critical relational database service offering strong consistency and high availability at a global scale.
Cloud SQL	A fully-managed web service for creating, configuring, and using relational databases (MySQL, PostgreSQL, SQL Server) in Google's cloud.
Cloud CDN	Caches HTTP(S) load balanced content close to users using Google's globally distributed edge points of presence.
Cloud DNS	A high performance, resilient, global, fully-managed DNS service providing a RESTful API to manage DNS records.
Cloud IDS	A managed Intrusion Detection System that detects malware, spyware, and command-and-control attacks.
Cloud Interconnect	Offers enterprise-grade connections to Google Cloud Platform (Dedicated, Partner, Cross-Cloud, and Cross-Site options).
Cloud Load Balancing	Provides scaling, high availability, and traffic management for internet-facing and private applications.
Cloud NAT	Enables instances in a private network to communicate with the internet.
Cloud NGFW / Enterprise	A distributed, cloud-native firewall service. Enterprise edition includes an Intrusion Prevention System (IPS).
Cloud Router	Enables dynamic Border Gateway Protocol (BGP) route updates between VPC networks and non-Google networks.
Cloud VPN	Connects your VPC network to existing networks (on-prem, other clouds) through IPsec connections (Classic or HA).
*Firebase App Hosting	Serverless web hosting for modern, full-stack web apps, integrating with GitHub and managing builds, CDN, and rendering.

Google Cloud Armor / Enterprise	Policy framework and WAF rules for protecting internet-facing applications from DDoS and targeted attacks. Enterprise bundles additional protections and support.
Media CDN	Content delivery network leveraging Google's global edge cache nodes for exceptional caching efficiency.
Network Connectivity Center	A hub-and-spoke model for managing network connectivity and connecting customer resources to the cloud network.
Network Intelligence Center	Comprehensive network monitoring, verification, and optimization platform across Google Cloud, multi-cloud, and on-prem environments.
Network Security Integration	Helps integrate third-party network appliances or services with Google Cloud Platform workloads (inline or out-of-band).
Network Service Tiers	Enables selection of network quality for outbound traffic: Standard Tier (third-party transit) or Premium Tier (Google private backbone).
Private Service Connect	Allows consumers to access managed services privately from inside their VPC network.
Secure Web Proxy (SWP)	A simple and scalable cloud-first web proxy for monitoring, inspecting, and controlling web traffic.
Service Directory	A managed service offering a single place to publish, discover, and connect services across various environments.
Virtual Private Cloud (VPC)	Provides a private network topology with IP allocation, routing, and network firewall policies.
Cloud Logging	Fully-managed service that ingests and allows analysis of application and system log data at scale.
Cloud Error Reporting	Analyzes and aggregates errors in cloud applications and notifies when new errors are detected.
Cloud Monitoring	Provides visibility into performance, uptime, and overall health of applications via metrics, events, and metadata.
Cloud Profiler	Continuous profiling of resource consumption in production applications to identify performance issues.
Cloud Trace	Provides latency sampling and reporting for App Engine, including per-URL statistics.
Google Cloud Backup and DR	Managed backup and disaster recovery service for centralized protection of Google Cloud workloads.
Cloud Shell	Browser-based command-line access to cloud resources with a built-in web editor.

Recommenders	Automatically analyzes usage patterns to provide security, cost, and efficiency insights.
Cloud Workstations	Fully-managed, customizable, and secure development environments accessible via browser or local IDE.
Secret Manager	Secure method for storing API keys, passwords, certificates, and other sensitive data.
Android Device Streaming	Powered by Firebase, securely connects to remote physical Android devices for testing within Android Studio.
Artifact Registry	Service for managing container images and packages, integrated with Google Cloud tooling and CI/CD pipelines.
Assured OSS (AOSS)	Enables users to incorporate the same scanned, analyzed, and fuzz-tested open source software packages that Google uses.
Cloud Build	Executes builds on Google Cloud infrastructure, importing source code from various repositories to produce artifacts.
Cloud Deploy	Manages application continuous delivery to Google Kubernetes Engine.
Developer Connect	Creates and maintains connections to source code management platforms outside of Google Cloud.
*Firebase Test Lab / Test Lab	Tests mobile apps on physical and virtual devices in Google data centers, providing detailed results.
Secure Source Manager	A fully-managed, Git-based source code management system.
BigQuery	Fully-managed, highly scalable data analysis service for Big Data with ad hoc query capabilities.
Cloud Composer	Managed workflow orchestration service based on Apache Airflow for pipelines across clouds and on-premises.
Cloud Data Fusion	Fully-managed, cloud-native enterprise data integration service with a graphical interface for building pipelines.
Dataform	End-to-end experience for data analysts to develop, test, version control, and schedule SQL workflows.
Dataplex	Intelligent data fabric enabling unified data management, governance, and analytics at scale.
Dataflow	Fully-managed service for strongly consistent, parallel stream and batch data-processing pipelines (Java SDK).

Dataproc	Managed Spark and Hadoop service for distributed data processing, available in standard and serverless configurations.
Dataproc Metastore	Fully-managed metastore service based on Apache Hive for data lakes.
Datastream	Serverless change data capture (CDC) and replication service for minimal latency data synchronization.
Google Earth Engine	Platform for global-scale analysis and visualization of geospatial datasets and satellite imagery.
Pub/Sub	Reliable, many-to-many, asynchronous messaging service decoupling senders and receivers.
Managed Service for Apache Kafka	Runs reliable, secure Kafka clusters and supporting services.
Agent Assist	LLM-powered AI solution increasing human agent productivity with real-time assistance.
Document AI / Workbench / Warehouse	Console for document processing using pre-trained models (OCR, Form Parser) or custom models; includes storage and governance.
*Talent Solution	Offers access to machine learning for improving talent acquisition experiences on career sites and ATS.
Translation Hub	Fully-managed document translation solution for self-service document translation.
Vertex AI Search for Industry/Commerce	Enables retail and media verticals to deliver Google-quality search results and recommendations.
*Recommendations AI / Retail Search	Builds personalized recommendation systems and leverages Google's search capabilities for retail.
Cloud Natural Language API	Analyzes text to identify entities, sentiment, languages, and syntax.
Cloud Translation / Media Translation API	Automatically translates text or audio from one language to another (supports real-time streaming for audio).
Cloud Vision API	Classifies images, detects objects/faces, and reads printed text.
Speech Services (Speech-to-Text, Text-to-Speech)	Converts audio to text or synthesizes human-like speech from text using neural network models.
Video Intelligence API	Analyzes videos to extract metadata, annotations, and identify entities.
Vertex AI Platform	Unified service for managing the entire ML development lifecycle (datasets, training, deployment, MLOps).
AutoML	Enables building custom models using transfer learning and Neural Architecture Search for various data types.

Vertex AI NAS	Leverages neural architecture search to generate, evaluate, and train model architectures.
Vertex AI Vision	Fully managed environment for building and deploying computer vision applications.
Gemini for Google Cloud	AI-powered assistance embedded in Google Cloud products for developers, data scientists, and operators.
Gemini Code Assist	AI-powered assistance for building, deploying, and operating applications.
Gemini in BigQuery	AI-powered assistance for understanding and querying data in BigQuery.
Generative AI on Vertex AI	Includes Vertex AI API, Conversation, Live API, Model Garden, Search, Studio, and NotebookLM for enterprise.
Gemini Enterprise	Combines AI Agents, Gemini models, and search technologies for enterprise automation and productivity.
Firebase AI Logic	Allows adding generative AI features to mobile and web applications via proxy service and SDKs.
Google Kubernetes Engine (GKE)	Managed environment for running containerized applications using Kubernetes, handling provisioning and scaling.
GKE Autopilot	Operation mode in GKE where Google manages cluster configuration, nodes, scaling, and security.
Cloud Service Mesh	Managed service including certificate authority for mutual authentication, telemetry, and traffic management.
BigQuery Data Transfer Service	Automates data movement from SaaS applications (Google Ads, YouTube, etc.) to BigQuery.
Database Migration Service	Fully-managed service for minimal-downtime migrations from on-prem or other clouds to Google managed databases.
Migration Center	Provides tools and guidance to accelerate end-to-end cloud migration journeys (discovery, planning, execution).
Migrate to Virtual Machines	Fully-managed service to migrate workloads into Compute Engine with minimal downtime using replication.
Storage Transfer Service	Imports large amounts of online data into Cloud Storage from other clouds or private data centers.
Transfer Appliance	Hardware appliance solution for transferring large amounts of data quickly to Google Cloud.

Access Transparency / Approval	Captures logs of manual Google admin access and allows customers to approve such accesses.
Identity Platform / IAM	Tools to manage user identities (authentication) and administrator access to cloud resources.
Cloud Identity	Identity and device management only
Assured Workloads	Creates security controls to assist with compliance requirements (e.g., FedRAMP).
Binary Authorization	Ensures only signed and explicitly-authorized workload artifacts are deployed to production.
Certificate Authority Service	Cloud-hosted service to issue and manage certificates for cloud or on-premises workloads.
Cloud HSM / Cloud KMS / External KMS	Managed services for protecting and managing cryptographic keys (hosted or third-party).
Sensitive Data Protection (DLP)	Fully-managed service to discover, classify, de-identify, and protect sensitive data.
VPC Service Controls	Configures security perimeters around API-based cloud services to mitigate data exfiltration.
Managed Service for Microsoft AD	Highly available, hardened Google Cloud service running actual Microsoft Active Directory.
Cloud Run	Runs stateless containers on a fully-managed environment.
Cloud Run functions	Lightweight, event-based, asynchronous compute solution for single-purpose functions.
Cloud Scheduler	Fully-managed enterprise-grade cron job scheduler.
Cloud Tasks	Fully-managed service for executing, dispatching, and delivering distributed tasks.
Eventarc	Fully-managed service for connecting various Google Cloud services via events.
Workflows	Fully-managed service for executing sequences of operations across microservices and APIs.
Media Services (Live Stream, Transcoder)	APIs for live encoding, batch media conversion, and dynamic ad insertion (Video Stitcher).
Google Distributed Cloud Connected	Allows running private GKE clusters on dedicated hardware on customer premises.
Premium Support	Premium Support includes Technical Account Manager (TAM) services.
Enhanced Support	A current support tier offering faster response times than Standard Support.
Standard Support	The baseline paid support tier for production workloads.
API Gateway	Fully-managed service to develop, deploy, and secure APIs running on Google Cloud Platform.
Application Integration	iPaaS offering tools, triggers, and connectors to manage applications and data for business operations.

Service Infrastructure	Foundational platform for creating, managing, securing, and consuming APIs and services.

Shared responsibilities and shared fate on Google Cloud

Last reviewed 2023-08-21 UTC

This document describes the differences between the shared responsibility model and shared fate in Google Cloud. It discusses the challenges and nuances of the shared responsibility model. This document describes what shared fate is and how we partner with our customers to address cloud security challenges.

Understanding the shared responsibility model is important when determining how to best protect your data and workloads on Google Cloud. The shared responsibility model describes the tasks that you have when it comes to security in the cloud and how these tasks are different for cloud providers.

Understanding shared responsibility, however, can be challenging. The model requires an in-depth understanding of each service you utilize, the configuration options that each service provides, and what Google Cloud does to secure the service. Every service has a different configuration profile, and it can be difficult to determine the best security configuration. Google believes that the shared responsibility model stops short of helping cloud customers achieve better security outcomes. Instead of shared responsibility, we believe in *shared fate*.

Shared fate includes us building and operating a trusted cloud platform for your workloads. We provide best practice guidance and secured, attested infrastructure code that you can use to deploy your workloads in a secure way. We release solutions that combine various Google Cloud services to solve complex security problems and we offer innovative insurance options to help you measure and mitigate the risks that you must accept. Shared fate involves us more closely interacting with you as you secure your resources on Google Cloud.

Shared responsibility

You're the expert in knowing the security and regulatory requirements for your business, and knowing the requirements for protecting your confidential data and resources. When you run your workloads on Google Cloud, you must identify the security controls that you need to configure in Google Cloud to help protect your confidential data and each workload. To decide which security controls to implement, you must consider the following factors:

- Your regulatory compliance obligations
- Your organization's security standards and risk management plan
- Security requirements of your customers and your vendors

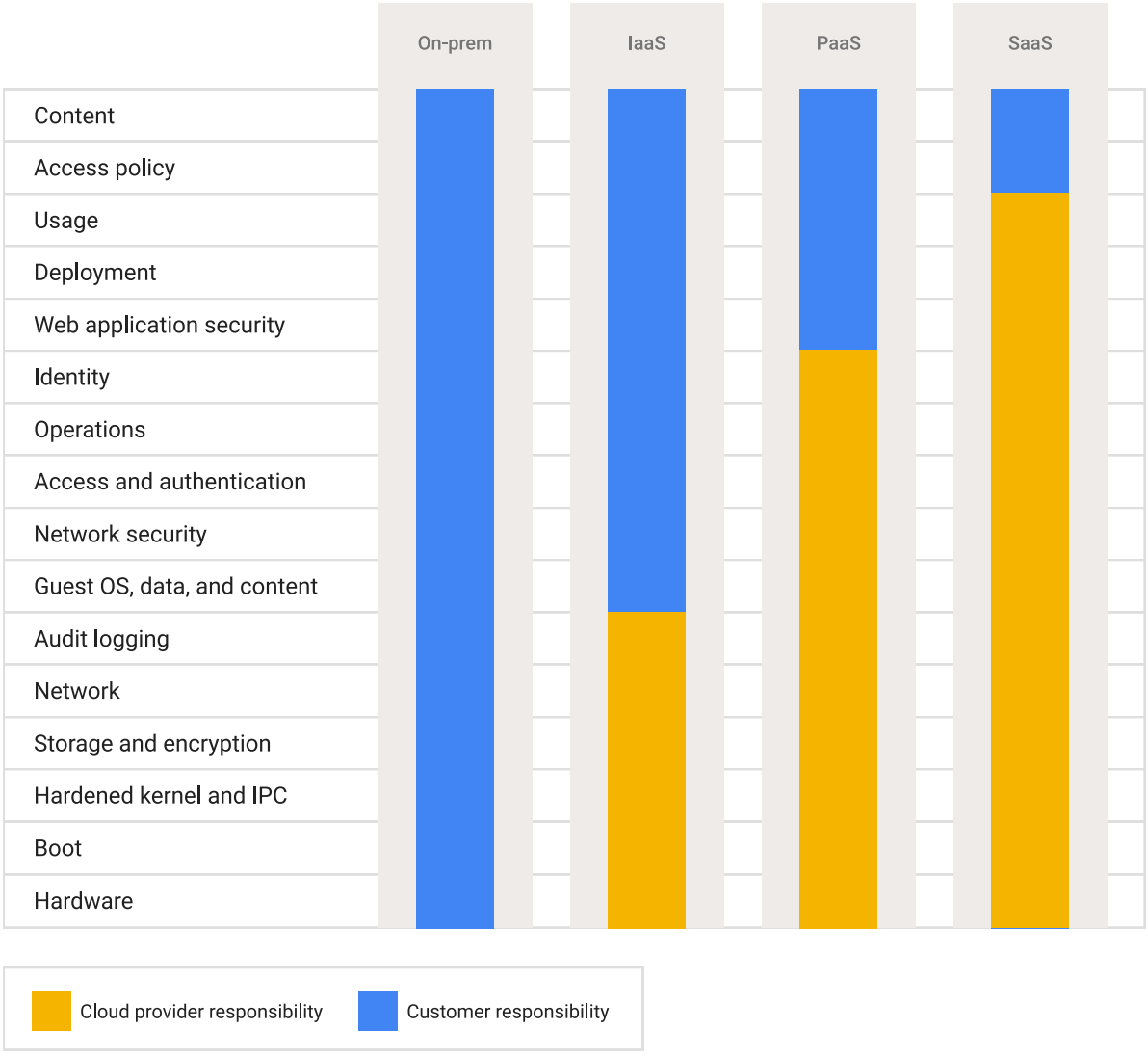
Defined by workloads

Traditionally, responsibilities are defined based on the type of workload that you're running and the cloud services that you require. Cloud services include the following categories:

Cloud service	Description
Infrastructure as a service (IaaS)	IaaS services include Compute Engine (/compute/docs), Cloud Storage (/storage/docs/introduction), and networking services such as Cloud VPN (/network-connectivity/docs/vpn/concepts/overview), Cloud Load Balancing (/load-balancing/docs/load-balancing-overview), and Cloud DNS (/dns/docs/overview). IaaS provides compute, storage, and network services on demand with pay-as-you-go pricing. You can use IaaS if you plan on migrating an existing on-premises workload to the cloud using lift-and-shift, or if you want to run your application on particular VMs, using specific databases or network configurations. In IaaS, the bulk of the security responsibilities are yours, and our responsibilities are focused on the underlying infrastructure and physical security.
Platform as a service (PaaS)	PaaS services include App Engine (/appengine), Google Kubernetes Engine (GKE) (/kubernetes-engine/docs), and BigQuery (/bigquery/docs/introduction). PaaS provides the runtime environment that you can develop and run your applications in. You can use PaaS if you're building an application (such as a website), and want to focus on development not on the underlying infrastructure. In PaaS, we're responsible for more controls than in IaaS. Typically, this will vary by the services and features that you use. You share responsibility with us for application-level controls and IAM management. You remain responsible for your data security and client protection.
Software as a service (SaaS)	SaaS applications include Google Workspace (https://workspace.google.com/), Google Security Operations (/chronicle/docs/overview), and third-party SaaS applications that are available in Google Cloud Marketplace (/marketplace). SaaS provides online applications that you can subscribe to or pay for in some way. You can use SaaS applications when your enterprise doesn't have the internal expertise or business requirement to build the application themselves, but does require the ability to process workloads.

Cloud service	Description
	In SaaS, we own the bulk of the security responsibilities. You remain responsible for your access controls and the data that you choose to store in the application.
Function as a service (FaaS) or serverless	FaaS provides the platform for developers to run small, single-purpose code (called *functions*) that run in response to particular events. You would use FaaS when you want particular things to occur based on a particular event. For example, you might create a function that runs whenever data is uploaded to Cloud Storage so that it can be classified. FaaS has a similar shared responsibility list as SaaS. Cloud Run functions (/functions/docs/2nd-gen/overview) is a FaaS application.

The following diagram shows the cloud services and defines how responsibilities are shared between the cloud provider and customer.



As the diagram shows, the cloud provider always remains responsible for the underlying network and infrastructure, and customers always remain responsible for their access

policies and data.

Defined by industry and regulatory framework

Various industries have regulatory frameworks that define the security controls that must be in place. When you move your workloads to the cloud, you must understand the following:

- Which security controls are your responsibility
- Which security controls are available as part of the cloud offering
- Which default security controls are inherited

Inherited security controls (such as our default encryption (/docs/security/encryption/default-encryption) and infrastructure controls (/docs/security/infrastructure/design)) are controls that you can provide as part of your evidence of your security posture to auditors and regulators. For example, the Payment Card Industry Data Security Standard (PCI DSS) defines regulations for payment processors. When you move your business to the cloud, these regulations are shared between you and your CSP. To understand how PCI DSS responsibilities are shared between you and Google Cloud, see Google Cloud: PCI DSS Shared Responsibility Matrix (https://services.google.com/fh/files/misc/gcp_pci_dss_v4_responsibility_matrix.pdf).

As another example, in the United States, the Health Insurance Portability and Accountability Act (HIPAA) has set standards for handling electronic personal health information (PHI). These responsibilities are also shared between the CSP and you. For more information on how Google Cloud meets our responsibilities under HIPAA, see HIPAA - Compliance (https://cloud.google.com/security/compliance/hipaa-compliance).

Other industries (for example, finance or manufacturing) also have regulations that define how data can be gathered, processed, and stored. For more information about shared responsibility related to these, and how Google Cloud meets our responsibilities, see Compliance resource center (https://cloud.google.com/security/compliance).

Defined by location

Depending on your business scenario, you might need to consider your responsibilities based on the location of your business offices, your customers, and your data. Different countries and regions have created regulations that inform how you can process and store your customer's data. For example, if your business has customers who reside in the European Union, your business might need to abide by the requirements that are described

in the General Data Protection Regulation (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679) (GDPR), and you might be obligated to keep your customer data in the EU itself. In this circumstance, you are responsible for ensuring that the data that you collect remains in the Google Cloud regions in the EU (https://cloud.google.com/about/locations#europe). For more information about how we meet our GDPR obligations, see GDPR and Google Cloud (https://cloud.google.com/privacy/gdpr).

For information about the requirements related to your region, see Compliance offerings (https://cloud.google.com/security/compliance/offerings). If your scenario is particularly complicated, we recommend speaking with our sales team (https://cloud.google.com/contact) or one of our partners (https://cloud.google.com/find-a-partner) to help you evaluate your security responsibilities.

Challenges for shared responsibility

Though shared responsibility helps define the security roles that you or the cloud provider has, relying on shared responsibility can still create challenges. Consider the following scenarios:

- Most cloud security breaches are the direct result of misconfiguration (listed as number 3 in the Cloud Security Alliance's Pandemic 11 Report (https://cloudsecurityalliance.org/press-releases/2022/06/07/cloud-security-alliance-s-top-threats-to-cloud-computing-pandemic-11-report-finds-traditional-cloud-security-issues-becoming-less-concerning/)) and this trend is expected to increase. Cloud products are constantly changing, and new ones are constantly being launched. Keeping up with constant change can seem overwhelming. Customers need cloud providers to provide them with opinionated best practices to help keep up with the change, starting with best practices by default and having a baseline secure configuration.
- Though dividing items by cloud services is helpful, many enterprises have workloads that require multiple cloud services types. In this circumstance, you must consider how various security controls for these services interact, including whether they overlap between and across services. For example, you might have an on-premises application that you're migrating to Compute Engine, use Google Workspace for corporate email, and also run BigQuery to analyze data to improve your products.
- Your business and markets are constantly changing; as regulations change, as you enter new markets, or as you acquire other companies. Your new markets might have different requirements, and your new acquisition might host their workloads on

another cloud. To manage the constant changes, you must constantly re-assess your risk profile and be able to implement new controls quickly.

- How and where to manage your data encryption keys is an important decision that ties with your responsibilities to protect your data. The option that you choose depends on your regulatory requirements, whether you're running a hybrid cloud environment or still have an on-premises environment, and the sensitivity of the data that you're processing and storing.
- Incident management is an important, and often overlooked, area where your responsibilities and the cloud provider responsibilities aren't easily defined. Many incidents require close collaboration and support from the cloud provider to help investigate and mitigate them. Other incidents can result from poorly configured cloud resources or stolen credentials, and ensuring that you meet the best practices for securing your resources and accounts can be quite challenging.
- Advanced persistent threats (APTs) and new vulnerabilities can impact your workloads in ways that you might not consider when you start your cloud transformation. Ensuring that you remain up-to-date on the changing landscape, and who is responsible for threat mitigation is difficult, particularly if your business doesn't have a large security team.

Shared fate

We developed shared fate in Google Cloud to start addressing the challenges that the shared responsibility model doesn't address. Shared fate focuses on how all parties can better interact to continuously improve security. Shared fate builds on the shared responsibility model because it views the relationship between cloud provider and customer as an ongoing partnership to improve security.

Shared fate is about us taking responsibility for making Google Cloud more secure. Shared fate includes helping you get started with a secured landing zone (/architecture/landing-zones#what-is-a-google-cloud-landing-zone) and being clear, opinionated, and transparent about recommended security controls, settings, and associated best practices. It includes helping you better quantify and manage your risk with cyber-insurance, using our Risk Protection Program. Using shared fate, we want to evolve from the standard shared responsibility framework to a better model that helps you secure your business and build trust in Google Cloud.

The following sections describe various components of shared fate.

Help getting started

A key component of shared fate is the resources that we provide to help you get started, in a secure configuration in Google Cloud. Starting with a secure configuration helps reduce the issue of misconfigurations which is the root cause of most security breaches.

Our resources include the following:

- Enterprise foundations blueprint (/architecture/blueprints/security-foundations) that discuss top security concerns and our top recommendations.
- Secure blueprints (https://cloud.google.com/security/best-practices#deployable-security-blueprints-and-landing-zones) that let you deploy and maintain secure solutions using *infrastructure as code* (IaC). Blueprints have our security recommendations enabled by default. Many blueprints are created by Google security teams and managed as products. This support means that they're updated regularly, go through a rigorous testing process, and receive attestations from third-party testing groups. Blueprints include the enterprise foundations blueprint (/architecture/blueprints/security-foundations) and the secured data warehouse blueprint (/architecture/blueprints/confidential-data-warehouse-blueprint).
- Google Cloud Well-Architected Framework (/architecture/framework/security) recommendations for building security into your designs.
- Landing zone navigation guides (/architecture/landing-zones) that step you through the top decisions that you need to make to build a secure foundation for your workloads, including resource hierarchy, identity onboarding, security and key management, and network structure.

Risk Protection Program

Shared fate also includes the Risk Protection Program (https://cloud.google.com/security/products/risk-protection-program) (currently in preview), which helps you use the power of Google Cloud as a platform to manage risk, rather than just seeing cloud workloads as another source of risk that you need to manage. The Risk Protection Program is a collaboration between Google Cloud and two leading cyber insurance companies, Munich Re and Allianz Global & Corporate Speciality.

The Risk Protection Program includes Cyber Insurance Hub (/risk-manager/docs/overview), which provides data-driven insights that you can use to better understand your cloud security posture. If you're looking for cyber insurance coverage, you can share these insights from Cyber Insurance Hub directly with our insurance partners to obtain a quote.

For more information, see Google Cloud Risk Protection Program now in Preview (https://cloud.google.com/blog/products/identity-security/google-cloud-risk-protection-program-now-in-preview)

.

Help with deployment and governance

Shared fate also helps with your continued governance of your environment. For example, we focus efforts on products such as the following:

- Assured Workloads (/assured-workloads/docs/concept-overview), which helps you meet your compliance obligations.
- Security Command Center (/security-command-center/docs/security-command-center-overview) Premium, which uses threat intelligence, threat detection, web scanning, and other advanced methods to monitor and detect threats. It also provides a way to resolve many of these threats quickly and automatically.
- Organization policies (/resource-manager/docs/organization-policy/overview) and resource settings (/resource-manager/docs/cloud-platform-resource-hierarchy) that let you configure policies throughout your hierarchy of folders and projects.
- Policy Intelligence tools (/policy-intelligence/docs/overview) that provide you with insights on access to accounts and resources.
- Confidential Computing (/confidential-computing/confidential-vm/docs/about-cvm), which lets you encrypt data in use.
- Sovereign Controls by Partners (/sovereign-controls-by-partners/docs/overview), which is available in certain countries and helps enforce data residency requirements.

Putting shared responsibility and shared fate into practice

As part of your planning process, consider the following actions to help you understand and implement appropriate security controls:

- Create a list of the type of workloads that you will host in Google Cloud, and whether they require IaaS, PaaS, and SaaS services. You can use the shared responsibility diagram (#shared-diagram) as a checklist to ensure that you know the security controls that you need to consider.

- Create a list of regulatory requirements that you must comply with, and access resources in the Compliance resource center (https://cloud.google.com/security/compliance) that relate to those requirements.
- Review the list of available blueprints and architectures in the Architecture Center (/architecture) for the security controls that you require for your particular workloads. The blueprints provide a list of recommended controls and the IaC code that you require to deploy that architecture.
- Use the landing zone documentation (/architecture/landing-zones) and the recommendations in the enterprise foundations guide (/architecture/blueprints/security-foundations) to design a resource hierarchy and network architecture that meets your requirements. You can use the opinionated workload blueprints, like the secured data warehouse, to accelerate your development process.
- After you deploy your workloads, verify that you're meeting your security responsibilities using services such as the Cyber Insurance Hub, Assured Workloads, Policy Intelligence tools, and Security Command Center Premium.

For more information, see the CISO's Guide to Cloud Transformation paper (https://services.google.com/fh/files/misc/ciso-guide-to-security-transformation.pdf).

What's next

- Review the core security principles (/architecture/framework/security#core_principles).
- Keep up to date with shared fate resources (https://cloud.google.com/security/shared-fate).
- Familiarize yourself with available blueprints (https://cloud.google.com/security/best-practices#deployable-security-blueprints-and-landing-zones), including the security foundations blueprint and workload examples like the secured data warehouse.
- Read more about shared fate (https://cloud.google.com/blog/products/identity-security/delivering-the-industrys-most-trusted-cloud).
- Read about our underlying secure infrastructure in the Google infrastructure security design overview (/docs/security/infrastructure/design).
- Read how to implement NIST Cybersecurity Framework best practices in Google Cloud (PDF) (https://services.google.com/fh/files/misc/gcp_nist_cybersecurity_framework.pdf).

Last updated 2023-08-21 UTC.