

**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 2a- Infrastructure Software  
(I-SaaS)



| GCP Service Category | GCP Service Name                        | GCP Service Description                                                                             |
|----------------------|-----------------------------------------|-----------------------------------------------------------------------------------------------------|
| Security & Identity  | <a href="#">Security Command Center</a> | Centralised vulnerability and threat reporting service for identifying misconfigurations and risks. |

# 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

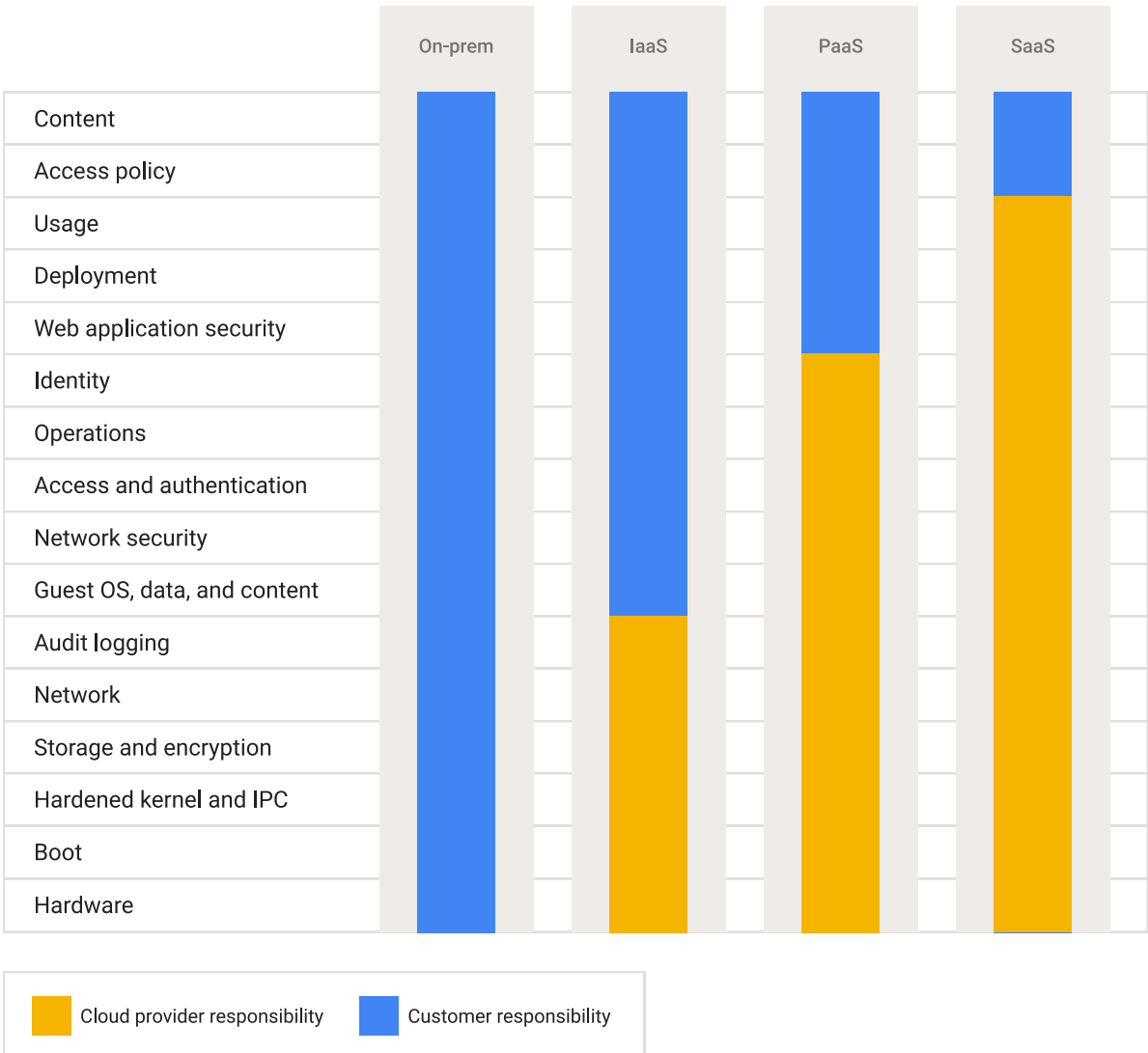
## Defined by workloads

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) | <p>IaaS services include <a href="/compute/docs/">Compute Engine (/compute/docs/)</a>, <a href="/storage/docs/introduction/">Cloud Storage (/storage/docs/introduction/)</a>, and networking services such as <a href="/network-connectivity/docs/vpn/concepts/overview/">Cloud VPN (/network-connectivity/docs/vpn/concepts/overview/)</a>, <a href="/load-balancing/docs/load-balancing-overview/">Cloud Load Balancing (/load-balancing/docs/load-balancing-overview/)</a>, and <a href="/dns/docs/overview/">Cloud DNS (/dns/docs/overview/)</a>.</p> <p>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.</p> <p>In IaaS, the bulk of the security responsibilities are yours, and our responsibilities are focused on the underlying infrastructure and physical security.</p> |
| Platform as a service (PaaS)       | <p>PaaS services include <a href="/appengine/">App Engine (/appengine/)</a>, <a href="/kubernetes-engine/docs/">Google Kubernetes Engine (GKE) (/kubernetes-engine/docs/)</a>, and <a href="/bigquery/docs/introduction/">BigQuery (/bigquery/docs/introduction/)</a>.</p> <p>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.</p> <p>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.</p>                                                                                                                                                                                                                                 |
| Software as a service (SaaS)       | <p>SaaS applications include <a href="https://workspace.google.com/">Google Workspace (https://workspace.google.com/)</a>, <a href="/chronicle/docs/overview/">Google Security Operations (/chronicle/docs/overview/)</a>, and third-party SaaS applications that are available in <a href="/marketplace/">Google Cloud Marketplace (/marketplace/)</a>.</p> <p>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.</p>                                                                                                                                                                                                                                                                                                                                                                                            |

| 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 | <p>FaaS provides the platform for developers to run small, single-purpose code (called <i>functions</i>) 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.</p> <p>FaaS has a similar shared responsibility list as SaaS. <a href="#">Cloud Run functions</a> (/functions/docs/2nd-gen/overview) is a FaaS application.</p> |

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) (/docs/security/encryption/default-encryption) and [infrastructure controls](/docs/security/infrastructure/design) (/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) (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) (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) (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) (/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) (/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) (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) (/architecture/blueprints/security-foundations) and the [secured data warehouse blueprint](/architecture/blueprints/confidential-data-warehouse-blueprint) (/architecture/blueprints/confidential-data-warehouse-blueprint).
- [Google Cloud Well-Architected Framework](/architecture/framework/security) (/architecture/framework/security) recommendations for building security into your designs.
- [Landing zone navigation guides](/architecture/landing-zones) (/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) (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) (/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) (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) (/assured-workloads/docs/concept-overview), which helps you meet your compliance obligations.
- [Security Command Center](/security-command-center/docs/security-command-center-overview) (/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) (/resource-manager/docs/organization-policy/overview) and [resource settings](/resource-manager/docs/cloud-platform-resource-hierarchy) (/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) (/policy-intelligence/docs/overview) that provide you with insights on access to accounts and resources.
- [Confidential Computing](/confidential-computing/confidential-vm/docs/about-cvm) (/confidential-computing/confidential-vm/docs/about-cvm), which lets you encrypt data in use.
- [Sovereign Controls by Partners](/sovereign-controls-by-partners/docs/overview) (/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) (<https://cloud.google.com/security/compliance>) that relate to those requirements.
- Review the list of available blueprints and architectures in the [Architecture Center](/architecture) (/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) (/architecture/landing-zones) and the recommendations in the [enterprise foundations guide](/architecture/blueprints/security-foundations) (/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) (<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) (/architecture/framework/security#core\_principles).
- Keep up to date with [shared fate resources](https://cloud.google.com/security/shared-fate) (<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) (<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) (<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) (/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) ([https://services.google.com/fh/files/misc/gcp\\_nist\\_cybersecurity\\_framework.pdf](https://services.google.com/fh/files/misc/gcp_nist_cybersecurity_framework.pdf)).

Except as otherwise noted, the content of this page is licensed under the [Creative Commons Attribution 4.0 License](https://creativecommons.org/licenses/by/4.0/) (<https://creativecommons.org/licenses/by/4.0/>), and code samples are licensed under the [Apache 2.0 License](https://www.apache.org/licenses/LICENSE-2.0) (<https://www.apache.org/licenses/LICENSE-2.0>). For details, see the [Google Developers Site Policies](https://developers.google.com/site-policies) (<https://developers.google.com/site-policies>). Java is a registered trademark of Oracle and/or its affiliates.

Last updated 2023-08-21 UTC.