Professional Cloud Security Engineer BETA

Certification Exam Guide

A Cloud Security Engineer enables organizations to design and implement secure workloads and infrastructure on Google Cloud. Through an understanding of security best practices and industry security requirements, this individual designs, develops, and manages a secure infrastructure by leveraging Google security technologies. The Cloud Security Engineer should be proficient in all aspects of cloud security, including identity and access management, defining organizational structure and policies, using Google technologies to provide data protection, configuring network security defenses, collecting and analyzing Google Cloud logs, managing incident responses, and demonstrating an understanding of the application of dynamic regulatory considerations.

Section 1: Configuring access within a cloud solution environment

1.1 Configuring Cloud Identity. Considerations include:

- Managing Cloud Identity
- Configuring Google Cloud Directory Sync
- Managing super administrator account

- Automating user lifecycle management process
- Administering user accounts and groups programmatically

1.2 Managing service accounts. Considerations include:

- Protecting and auditing service accounts and keys
- Automating the rotation of user-managed service account keys
- Identifying scenarios requiring service accounts
- Creating, authorizing, and securing service accounts
- Securely managing API access management
- Managing and creating short-lived credentials

1.3 Managing authentication. Considerations include:

- Creating a password policy for user accounts
- Establishing Security Assertion Markup Language (SAML)
- Configuring and enforcing two-factor authentication

1.4 Managing and implementing authorization controls. Considerations include:

- Managing privileged roles and separation of duties
- Managing IAM permissions with basic, predefined, and custom roles
- Granting permissions to different types of identities
- Understanding difference between Cloud Storage IAM and ACLs
- Designing identity roles at the organization, folder, project, and resource level

- Configuring Access Context Manager

1.5 Defining resource hierarchy. Considerations include:

- Creating and managing organizations
- Designing resource policies for organizations, folders, projects, and resources
- Managing organization constraints
- Using resource hierarchy for access control and permissions inheritance
- Designing and managing trust and security boundaries within Google Cloud projects

Section 2: Configuring network security

2.1 Designing network security. Considerations include:

- Configuring network perimeter controls (firewall rules; Identity-Aware Proxy (IAP))
- Configuring load balancing (global, network, HTTP(S), SSL proxy, and TCP proxy load balancers)
- Identifying Domain Name System Security Extensions (DNSSE)
- Identifying differences of private versus public addressing
- Configuring web application firewall (Google Cloud Armor)
- Configuring Cloud DNS

2.2 Configuring network segmentation. Considerations include:

- Configuring security properties of a VPC network, VPC peering, Shared VPC, and firewall rules
- Configuring network isolation and data encapsulation for N tier application design

- Configuring app-to-app security policy

2.3 Establishing private connectivity. Considerations include:

- Designing and configuring private RFC1918 connectivity between VPC networks and Google Cloud projects (Shared VPC, VPC peering)
- Designing and configuring private RFC1918 connectivity between data centers and VPC network (IPsec and Cloud Interconnect)
- Establishing private connectivity between VPC and Google APIs (Private Google Access, Private Google Access for on-premises hosts, Private Service Connect)
- Configuring Cloud NAT

Section 3: Ensuring data protection

3.1 Protecting sensitive data. Considerations include:

- Inspecting and redacting personally identifiable information (PII)
- Configuring pseudonymization
- Configuring format-preserving substitution
- Restricting access to BigQuery datasets
- Configuring VPC Service Controls
- Securing secrets with Secret Manager
- Protecting and managing compute instance metadata

3.2 Managing encryption at rest. Considerations include:

- Understanding use cases for Google default encryption, customer-managed encryption keys (CMEK), customer-supplied encryption keys (CSEK), Cloud External Key Manager (EKM), and Cloud HSM
- Creating and managing encryption keys for CMEK, CSEK, and EKM
- Applying Google's encryption approach to use cases
- Configuring object lifecycle policies for Cloud Storage
- Enabling confidential computing

Section 4: Managing operations in a cloud environment

4.1 Building and deploying secure infrastructure and applications.

Considerations include:

- Automating security scanning for Common Vulnerabilities and Exploits (CVEs) through a CI/CD pipeline
- Automating virtual machine image creation, hardening, and maintenance
- Automating container image creation, verification, hardening, maintenance, and patch management

4.2 Configuring logging, monitoring, and detection. Considerations include:

- Configuring and analyzing network logs (Firewall rule logs, VPC flow logs, packet mirroring)
- Designing an effective logging strategy
- Logging, monitoring, responding to, and remediating security incidents

- Exporting logs to external security systems
- Configuring and analyzing Google Cloud audit logs and data access logs
- Configuring log exports (log sinks, aggregated sinks, logs router)
- Configuring and monitoring Security Command Center (Security Health Analytics, Event Threat Detection, Container Threat Detection, Web Security Scanner)

Section 5: Ensuring compliance

5.1 Determining regulatory requirements for the cloud. Considerations include:

- Determining concerns relative to compute, data, and network
- Evaluating security shared responsibility model
- Configuring security controls within cloud environments
- Determining the Google Cloud environment in scope for regulatory compliance