# Professional Cloud Security Engineer

GO TO PAGE (#)

## Certification exam guide

A Professional Cloud Security Engineer enables organizations to design and implement a secure infrastructure on Google Cloud. Through an understanding of security best practices and industry security requirements, this individual designs, develops, and manages a secure infrastructure leveraging Google security technologies. The Cloud Security Professional should be proficient in all aspects of Cloud Security including managing 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 regulatory concerns.

## 1. Configuring access within a cloud solution environment

1.1 Configuring Cloud Identity. Considerations include:

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

1.2 Managing user accounts. Considerations include:

- Designing identity roles at the project and organization level
- Automation of user lifecycle management process
- API usage

**GO TO PAGE** (#)

- Auditing service accounts and keys
- Automating the rotation of user-managed service account keys
- Identification of scenarios requiring service accounts
- Creating, authorizing, and securing service accounts
- Securely managed API access management

1.4 Managing authentication. Considerations include:

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

1.5 Managing and implementing authorization controls. Considerations include:

- Using resource hierarchy for access control
- 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 Google Cloud Storage IAM and ACLs

1.6 Defining resource hierarchy. Considerations include:

- Creating and managing organizations

- Resource structures (orgs, folders, and projects)
- Defining and managing organization constraints
- Using resource hierarchy for access control and permissions inheritance
- Trust and security boundaries within Google Cloud projects

**GO TO PAGE** (#) ⌄

## 2. Configuring network security

2.1 Designing network security. Considerations include:

- Security properties of a VPC network, VPC peering, shared VPC, and firewall rules
- Network isolation and data encapsulation for N tier application design
- Use of DNSSEC
- Private vs. public addressing
- App-to-app security policy

2.2 Configuring network segmentation. Considerations include:

- Network perimeter controls (firewall rules; IAP)
- Load balancing (global, network, HTTP(S), SSL proxy, and TCP proxy load balancers)

2.3 Establish private connectivity. Considerations include:

- Private RFC1918 connectivity between VPC networks and Google Cloud projects (Shared VPC, VPC peering)
- Private RFC1918 connectivity between data centers and VPC network (IPSEC and Cloud Interconnect).
- Enable private connectivity between VPC and Google APIs (private access)

## 3. Ensuring data protection

3.1 Preventing data loss with the DLP API. Considerations include:

- Identification and redaction of PII

GO TO PAGE (#)

- [illegible]
- Restricting access to DLP datasets

3.2 Managing encryption at rest. Considerations include:

- Understanding use cases for default encryption, customer-managed encryption keys (CMEK), and customer-supplied encryption keys (CSEK)
- Creating and managing encryption keys for CMEK and CSEK
- Managing application secrets
- Object lifecycle policies for Cloud Storage
- Enclave computing
- Envelope encryption

## 4. Managing operations within a cloud solution environment

4.1 Building and deploying infrastructure. Considerations include:

- Backup and data loss strategy
- Creating and automating an incident response plan
- Log sinks, audit logs, and data access logs for near-real-time monitoring
- Standby models

- Automate security scanning for Common Vulnerabilities and Exposures (CVEs) through a CI/CD pipeline
- Virtual machine image creation, hardening, and maintenance
- Container image creation, hardening, maintenance, and patch management

GO TO PAGE (#)

- Application logs near-real-time monitoring
- Static code analysis
- Automate security scanning through a CI/CD pipeline

4.3 Monitoring for security events. Considerations include:

- Logging, monitoring, testing, and alerting for security incidents
- Exporting logs to external security systems
- Automated and manual analysis of access logs
- Understanding capabilities of Forseti

## 5. Ensuring compliance

5.1 Comprehension of regulatory concerns. Considerations include:

- Evaluation of concerns relative to compute, data, and network.
- Security shared responsibility model
- Security guarantees within cloud execution environments
- Limiting compute and data for regulatory compliance

5.2 Comprehension of compute environment concerns. Considerations include:

- Security guarantees and constraints for each compute environment (Compute Engine, Google Kubernetes Engine, App Engine)
- Determining which compute environment is appropriate based on company compliance standards

**GO TO PAGE** (#)