

Professional Cloud Security Engineer

Section 1: Configuring access (~27% of the exam)

1.1 Managing Cloud Identity. Considerations include:

- Configuring Google Cloud Directory Sync and third-party connectors
- Managing a super administrator account
- Automating the user lifecycle management process
- Administering user accounts and groups programmatically
- Configuring Workforce Identity Federation

1.2 Managing service accounts. Considerations include:

- Securing and protecting service accounts (including default service accounts)
- Identifying scenarios requiring service accounts
- Creating, disabling, and authorizing service accounts
- Securing, auditing and mitigating the usage of service account keys
- Managing and creating short-lived credentials
- Configuring Workload Identity Federation
- Managing service account impersonation

1.3 Managing authentication. Considerations include:

- Creating a password and session management policy for user accounts
- Setting up Security Assertion Markup Language (SAML) and OAuth
- Configuring and enforcing two-step verification

1.4 Managing and implementing authorization controls. Considerations include:

- Managing privileged roles and separation of duties with Identity and Access Management (IAM) roles and permissions
- Managing IAM and access control list (ACL) permissions
- Granting permissions to different types of identities, including using IAM conditions and IAM deny policies
- Designing identity roles at the organization, folder, project, and resource level
- Configuring Access Context Manager
- Applying Policy Intelligence for better permission management
- Managing permissions through groups

1.5 Denning resource hierarchy. Considerations include:

- Creating and managing organizations at scale
- Managing organization policies for organization folders, projects, and resources
- Using resource hierarchy for access control and permissions inheritance

Section 2: Securing communications and establishing boundary protection (~21% of the exam)

2.1 Designing and configuring perimeter security. Considerations include:

- Configuring network perimeter controls (firewall rules, hierarchical firewall policies, Identity-Aware Proxy [IAP], load balancers, and Certificate Authority Service)
- Differentiating between private and public IP addressing
- Configuring web application firewall (Google Cloud Armor)
- Deploying Secure Web Proxy
- Configuring Cloud DNS security settings
- Continually monitoring and restricting configured APIs

2.2 Configuring boundary 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 applications
- Configuring VPC Service Controls

2.3 Establishing private connectivity. Considerations include:

- Designing and configuring private connectivity between VPC networks and Google Cloud projects (Shared VPC, VPC peering, and Private Google Access for on-premises hosts)
- Designing and configuring private connectivity between data centers and VPC network (HA-VPN, IPsec, MACsec, and Cloud Interconnect)
- Establishing private connectivity between VPC and Google APIs (Private Google Access, Private Google Access for on-premises hosts, restricted Google access, Private Service Connect)
- Using Cloud NAT to enable outbound traffic

Section 3: Ensuring data protection (~20% of the exam)

3.1 Protecting sensitive data and preventing data loss. Considerations include:

- Inspecting and redacting personally identifiable information (PII)
- Ensuring continuous discovery of sensitive data (structured and unstructured)
- Configuring pseudonymization

- Configuring format-preserving encryption
- Restricting access to BigQuery, Cloud Storage, and Cloud SQL datastores
- Securing secrets with Secret Manager
- Protecting and managing compute instance metadata

3.2 Managing encryption at rest, in transit, and in use. Considerations include:

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

3.3 Planning for security and privacy in AI. Considerations include:

- Implementing security controls for AI/ML systems (e.g., protecting against unintentional exploitation of data or models)
- Determining security requirements for IaaS-hosted and PaaS-hosted training models

Section 4: Managing operations (~22% of the exam)

4.1 Automating infrastructure and application security. Considerations include:

- Automating security scanning for Common Vulnerabilities and Exposures (CVEs) through a continuous integration and delivery (CI/CD) pipeline
- Configuring Binary Authorization to secure GKE clusters or Cloud Run
- Automating virtual machine image creation, hardening, maintenance, and patch management
- Automating container image creation, variation, hardening, maintenance, and patch management
- Managing policy and drift detection at scale (custom organization policies and custom modules for Security Health Analytics)

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

- Configuring and analyzing network logs (Firewall Rules Logging, VPC flow logs, Packet Mirroring, Cloud Intrusion Detection System [Cloud IDS], Log Analytics)
- Designing an effective logging strategy
- Logging, monitoring, responding to, and remediating security incidents
- Designing secure access to logs

- Exporting logs to external security systems
- Configuring and analyzing Google Cloud audit logs and data access logs
- Configuring log exports (log sinks and aggregated sinks)
- Configuring and monitoring Security Command Center

Section 5: Supporting compliance requirements (~10% of the exam)

5.1 Determining regulatory requirements for the cloud. Considerations include:

- Determining concerns relative to compute, data, network, and storage
- Evaluating the shared responsibility model
- Configuring security controls within cloud environments to support compliance requirements (regionalization of data and services)
- Restricting compute and data for regulatory compliance (Assured Workloads, organizational policies, Access Transparency, Access Approval)
- Determining the Google Cloud environment in scope for regulatory compliance