Google Infrastructure and Security Management

Configuring access:

Managing Cloud Identity

- Configuring Google Cloud Directory Sync and third-party connectors
- Managing a super administrator account
- Automating the user lifecycle management process

Managing service accounts.

- 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 implementing authorization controls

- 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

Securing communications and establishing boundary protection

Designing and configuring perimeter security.

- 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)
- Configuring Cloud DNS security settings

Configuring boundary segmentation.

- 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

Establishing private connectivity

- Designing and configuring private connectivity between VPC networks and Google Cloud projects (Shared VPC, VPC peering, and Private Google Access for on-premises hosts.
- 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

Ensuring data protection

Protecting sensitive data and preventing data loss.

- Inspecting and redacting personally identifiable information (PII)
- Ensuring continuous discovery of sensitive data (structured and unstructured)
- Restricting access to BigQuery, Cloud Storage, and Cloud SQL datastores

Managing encryption at rest, in transit, and in use.

- 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
- Configuring object lifecycle policies for Cloud Storage

Managing operations

Automating infrastructure and application security.

- 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

Configuring logging, monitoring, and detection

- 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
- Exporting logs to external security systems
- Configuring and analyzing Google Cloud audit logs and data access logs

Supporting compliance requirements

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)