Google Cloud Security Engineer: Exam Prep & Practice Training

10 – 14 January 2027
Chicago

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

Google Cloud Security Engineer: Exam Prep & Practice Training

Ref: 94_87603 **Date:** 10 – 14 January 2027 **Location:** Chicago **Fees:** 12000 Euro

Overview

Enterprise workloads hosted on public cloud infrastructure require robust identity governance, network perimeter defence, and cryptographic controls. This 5-day Google Cloud Security Engineer training provides systematic preparation across the core domains evaluated in Google Cloud professional security certifications. Participants learn to configure least-privilege identity access management policies, establish boundary defence with VPC Service Controls, implement customer-managed encryption keys, and automate threat detection. The curriculum emphasizes operational security, infrastructure hardening, and compliance monitoring across enterprise cloud environments. This course is delivered by Agile Leaders Training Center.

Who Should Attend

- Cloud Security Engineers establishing and maintaining protective perimeters
- System Administrators responsible for cloud access governance and user provisioning
- Security Architects designing enterprise security blueprints on cloud infrastructure
- DevSecOps Engineers integrating automated policy checks into deployment pipelines
- GCP Solution Architects aligning security postures with organizational standards
- Network Security Specialists configuring virtual topologies, firewalls, and private interconnects
- IT Infrastructure Managers overseeing regulatory compliance and operational risk

Departments and Industries

This course supports technical teams responsible for cloud infrastructure defence across regulated and data-intensive sectors.

- Cloud Engineering and Security Operations in Technology and Cloud Services
- Information Security and Risk Assurance in Banking and Financial Services
- Digital Health Platforms and Data Governance in Healthcare and Pharmaceuticals
- Enterprise Infrastructure and Compliance in Public Sector and Government Bodies
- Platform Operations and Infrastructure Security in E-commerce and Retail
- Telecommunications and Media Infrastructure Management Units

Learning Objectives

By the end of this course, participants will be able to:

- Configure organizational hierarchies, IAM policies, and granular access boundaries.
- Establish secure network architectures using Cloud Armor, firewall policies, and private endpoints.
- Deploy VPC Service Controls to prevent unauthorized data exfiltration.
- Protect sensitive data assets using Cloud KMS, customer-managed encryption keys, and DLP inspection templates.
- Enforce container integrity through software supply chain controls and Binary Authorization.
- Monitor security posture and automate incident response using Security Command Center and audit logs.
- Align cloud configurations with corporate compliance frameworks and governance mandates.

Course Agenda

Day 1: Identity and Access Management

- Google Cloud Identity architecture and single sign-on integration
- Hierarchical IAM role assignment, custom roles, and policy inheritance
- Service account management, key handling, and security hardening
- Access Context Manager setup and IAM deny policy implementation
- Workforce Identity Federation and short-lived credentials management
- Principle of least privilege auditing across resource hierarchies

Day 2: Network Architecture and Perimeter Security

- Virtual Private Cloud topologies, subnets, and Shared VPC deployments
- Distributed firewall policies, Cloud Next Generation Firewall, and Cloud Armor
- Private Google Access, Cloud NAT, and secure private connectivity
- Perimeter segmentation using VPC Service Controls and access levels
- Cloud DNS security extensions, DNS peering, and Secure Web Proxy
- Internal and external load balancer security and Identity-Aware Proxy

Day 3: Data Protection and Cryptography

- Sensitive data identification and de-identification using Cloud DLP
- Encryption across storage services using customer-managed encryption keys
- Cloud Key Management Service lifecycles, key rotation, and Cloud EKM
- Centralized credential protection and access auditing with Secret Manager
- Confidential Computing architecture and storage lifecycle management rules
- Access control and fine-grained permissions for BigQuery and Cloud Storage

Day 4: Workload Protection and Operational Security

- Software supply chain integrity and deployment policies with Binary Authorization
- Cloud Audit Logs, VPC Flow Logs, and Packet Mirroring configuration
- Centralized threat detection and posture evaluation in Security Command Center
- Security configurations for machine learning workloads in Vertex AI
- Continuous delivery pipeline controls and container artifact vulnerability scanning
- Infrastructure drift detection and automated policy enforcement workflows

Day 5: Compliance, Governance, and Exam Readiness

- Mapping industry security frameworks to native cloud security controls
- Access Transparency, data residency boundaries, and Assured Workloads
- Operational boundaries under the cloud security shared responsibility model
- Audit log export pipelines and regulatory compliance reporting
- Exam syllabus breakdown, scenario analysis, and practice question reviews
- Implementation planning and individual study roadmaps

Practical Exercises

Participants apply configuration practices through structured technical scenarios reflecting enterprise security challenges.

- Suggested activity: Configure workforce identity federation to exchange external identity tokens for short-lived credentials.
- Suggested activity: Define a secure perimeter using VPC Service Controls to restrict data movement between services.
- Suggested activity: Create and rotate customer-managed encryption keys to protect Cloud Storage buckets and BigQuery datasets.
- Suggested activity: Set up Binary Authorization rules to restrict container deployments to signed artifacts.

FAQs

What specific qualifications or prerequisites are needed for participants before enrolling in the course?

Participants should possess foundational knowledge of cloud infrastructure, network security principles, and practical experience navigating Google Cloud services.

How long is each day's session, and is there a total number of hours required for the entire course?

Daily sessions run for four to five hours, including practical exercises and breaks. Over five days, the course provides 20 to 25 instructional hours.

AGILE LEADERS
Training Center

What is the difference between Google-managed encryption and customer-managed keys?

Google-managed encryption automates cryptographic key creation, rotation, and storage by default. Customer-managed encryption keys enable organizations to generate, rotate, and revoke their own keys in Cloud KMS to satisfy specific regulatory and internal governance standards.

Conclusion

Participants gain the technical competence to design, configure, and maintain secure enterprise environments on Google Cloud. Through thorough coverage of identity, networking, cryptography, and operational compliance, professionals build practical skills required to protect cloud infrastructure and validate their capabilities against industry exam benchmarks.