Google Cloud PCSE Cheat Sheet

One-page cram sheet for Professional Cloud Security Engineer access, network security, data protection, operations, and compliance.

Best for	Focus	Use with
Last review before drills or exam day	High-yield security controls and decision patterns	Use with the quick summary for rapid refresh

1. Configure access

IAM roles	Know predefined vs custom roles, least privilege, and why broad primitive access is usually wrong.
Service accounts	Use separate identities for workloads, restrict key creation, and prefer managed identity patterns.
Resource hierarchy	Organization, folders, projects, and inherited policy flow are core to security design.
Organization Policy	Use constraints to prevent unsafe configurations before they happen.

2. Secure communications and boundaries

VPC design	Subnets, firewall rules, routing, and private connectivity shape the attack surface.
Cloud Armor / WAF	Use for edge protection, especially for internet-facing HTTP(S) workloads.
Private Google Access / PSC	Know when services should stay private instead of traversing the public internet.
Zero Trust access	Identity-aware access patterns usually beat flat network trust.

3. Ensure data protection

Encryption by default	Google Cloud encrypts at rest by default, but key choice and access still matter.
CMEK vs Google-managed keys	Use CMEK when you need stronger control, separation, or compliance posture.
Secret handling	Use Secret Manager instead of embedding secrets in code or config.
Data residency and sensitivity	Map protection choices to regulation and business data classification.

4. Manage operations

Logging and monitoring	Cloud Logging, Monitoring, Audit Logs, and alerting support both detection and compliance evidence.
Security Command Center	Centralize findings, misconfigurations, and posture review.

Incident readiness	Good security operations need playbooks, logs, escalation paths, and tested response steps.
Automation	Policy guardrails and repeatable deployments reduce drift and human error.

5. Support compliance requirements

Policy enforcement	Use org policies, IAM, KMS, logging, and network controls together.
Evidence collection	Logs, asset inventory, and change history support audits.
Shared responsibility	Google secures the cloud; you still secure identities, data, configs, and monitoring choices.
Practical mindset	The best exam answer usually balances strong security with operational realism.