High Level Security Model
Accounts, Access, and Identification

1. Use *Google Cloud Identity* to establish unified Identity with on-prem
2. Create roles with least privilege access through *Cloud IAM*
3. Establish *Org level policies* (no external IPs, Domain Restricted Sharing, Trusted Images)
4. Leverage *Shared VPC* for connectivity and segregated network control
5. Build *HA/DR topologies* - multi-AZ/multi-region with subnets

*FedRAMP Moderate Product
* FedRAMP High Product
6. Use *Cloud Interconnect* or *Cloud VPN*, along with *Cloud Router*, to establish a *hybrid connectivity* to on-prem.

7. Secure application infrastructure against DDoS and external threats with *Cloud Load Balancer*, *Cloud Armor* & *Firewalls*.
8. Leverage *Log Sink* to collect logs from *Cloud Audit Logs, *VPC Flow Logs*, and *Firewall logs*

10. Create a Shared VPC *Service Project to host workloads
11. Create security perimeter with *VPC Service Controls
12. Access GCP services and the Internet through *GCP private access, *Cloud DNS, and Cloud NAT

*FedRAMP Moderate Product
*FedRAMP High Product
Putting it all together