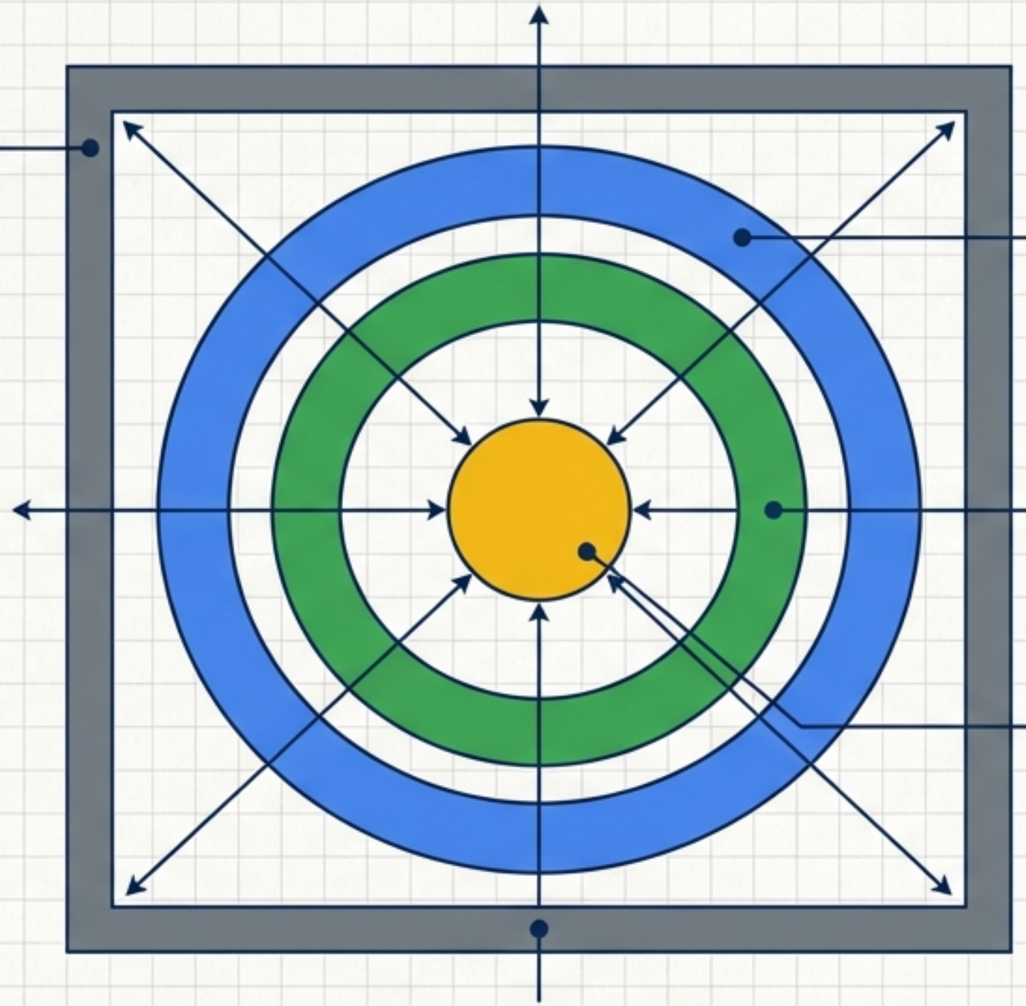
Designing for Security and Compliance

// Professional Cloud Architect Study Guide: Section 3 Framework

Architecture Domain:
Tech Equity RAD Application
Cloud Run & GKE
Shared Infrastructure

Defense in Depth: Architectural Blueprint

Oversight & Compliance
(Security Command Center, Audit Logs, Organization Policies)



Identity & Access
(IAM, Separation of Duties, IAP, Context-Aware Access)

Network Perimeter
(VPC Service Controls, Hierarchical Firewalls)

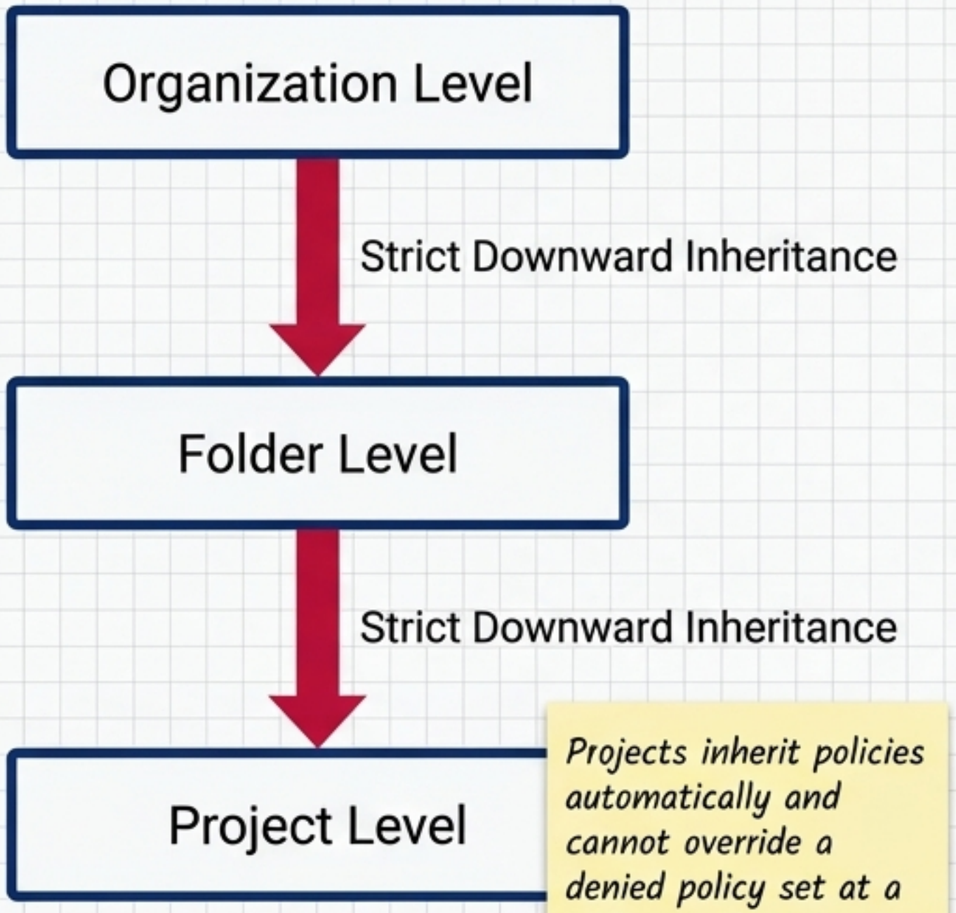
Workloads & Data
(Secret Manager, CMEK, Binary Authorization)

Oversight & Compliance
(Security Command Center, Audit Logs, Organization Policies)

Exam Weighting: ~17.5%

Goal: Bridge theoretical security domains with actionable Tech Equity RAD variables and GCP Console verifications.

The Outer Perimeter: Resource Hierarchy & Organization Policies



Essential PCA Org Policy Constraints

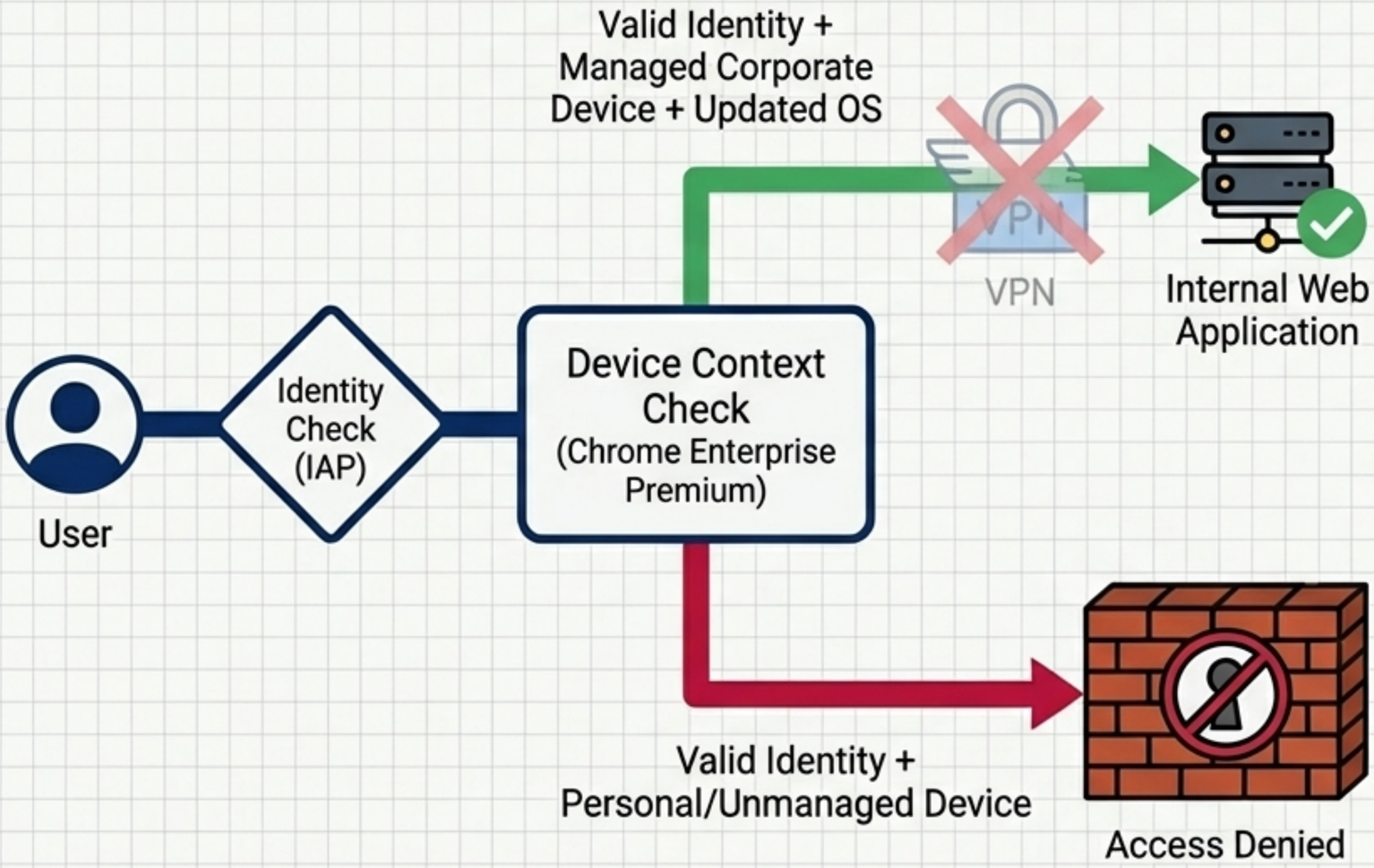
- `compute.requireShieldedVm`
- `iam.disableServiceAccountKeyCreation`
- `compute.restrictCloudRunRegions`
- `gcp.resourceLocations (Data Residency)`

Perimeter Defense Matrix: Firewall Strategies

	Hierarchical Firewall Policies	VPC Firewall Rules
Attachment Level	Organization or Folder	Per-Network
Evaluation Order	Evaluated First 	Evaluated Second
Primary Use Case	Central security team enforcing baseline deny rules across all projects.	Project teams configuring application-specific access.

Central Security Use Case: Block all inbound RDP/SSH from the internet centrally at the Folder level, preventing any individual project team from accidentally exposing a VM via local VPC rules.

Zero-Trust Edge: IAP & Context-Aware Access



Theory-to-Practice

RAD UI Variable:
`enable_iap (Group 4)`

Concept: IAP replaces traditional VPNs by verifying Google identities at the edge. Context-Aware Access upgrades this to zero-trust based on device trust, location, and risk score.

Identity & Authentication Matrix

Long-lived JSON Keys

Avoid when possible.

High risk of credential leakage.

Service Account Impersonation

`iam.serviceAccounts.actAs`

Preferred for Developer Workflows.

Allows users to temporarily act at target SA (e.g., running Terraform locally) without downloading keys. Tokens expire automatically.

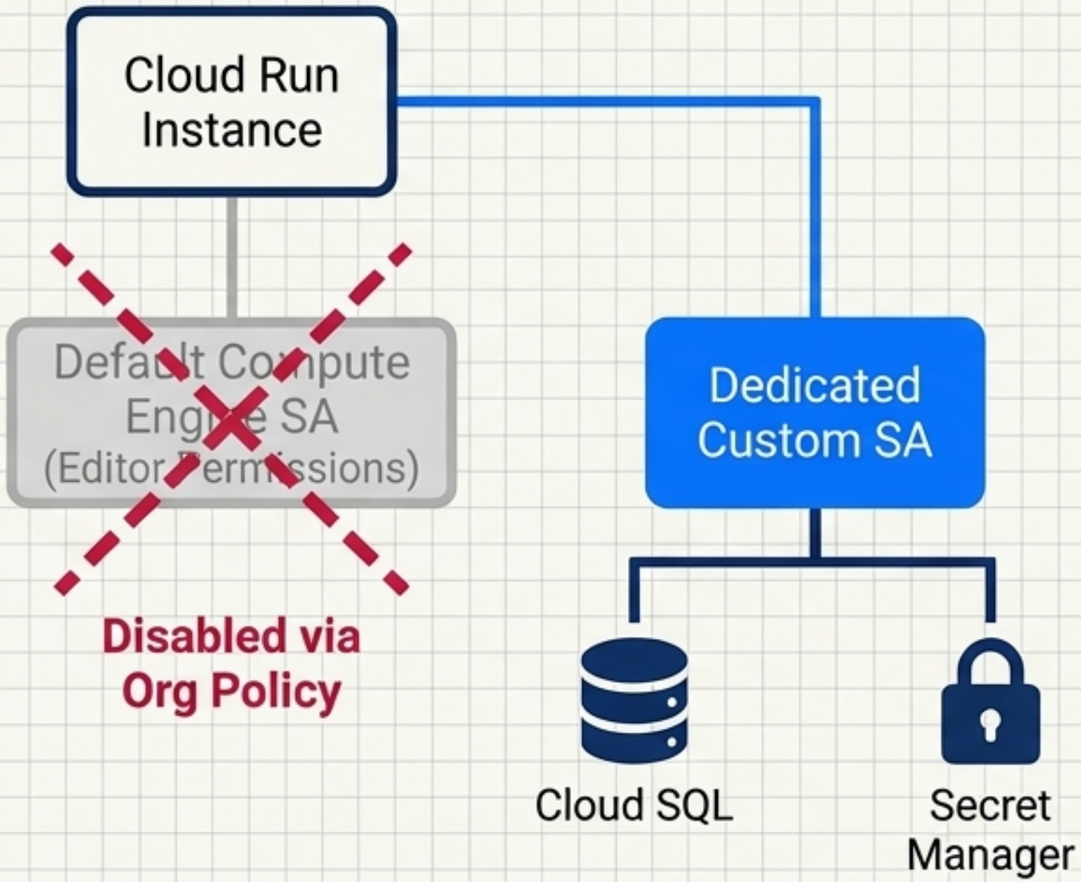
Workload Identity Federation

Preferred for External CI/CD.

Authenticate external workloads (GitHub Actions, AWS EC2) directly to GCP using short-lived federated tokens instead of static keys.

Least Privilege & Separation of Duties

Mini-Case: Professional Services Firm



RAD Console Implementation

Concept: Principle of Least Privilege via Predefined Roles

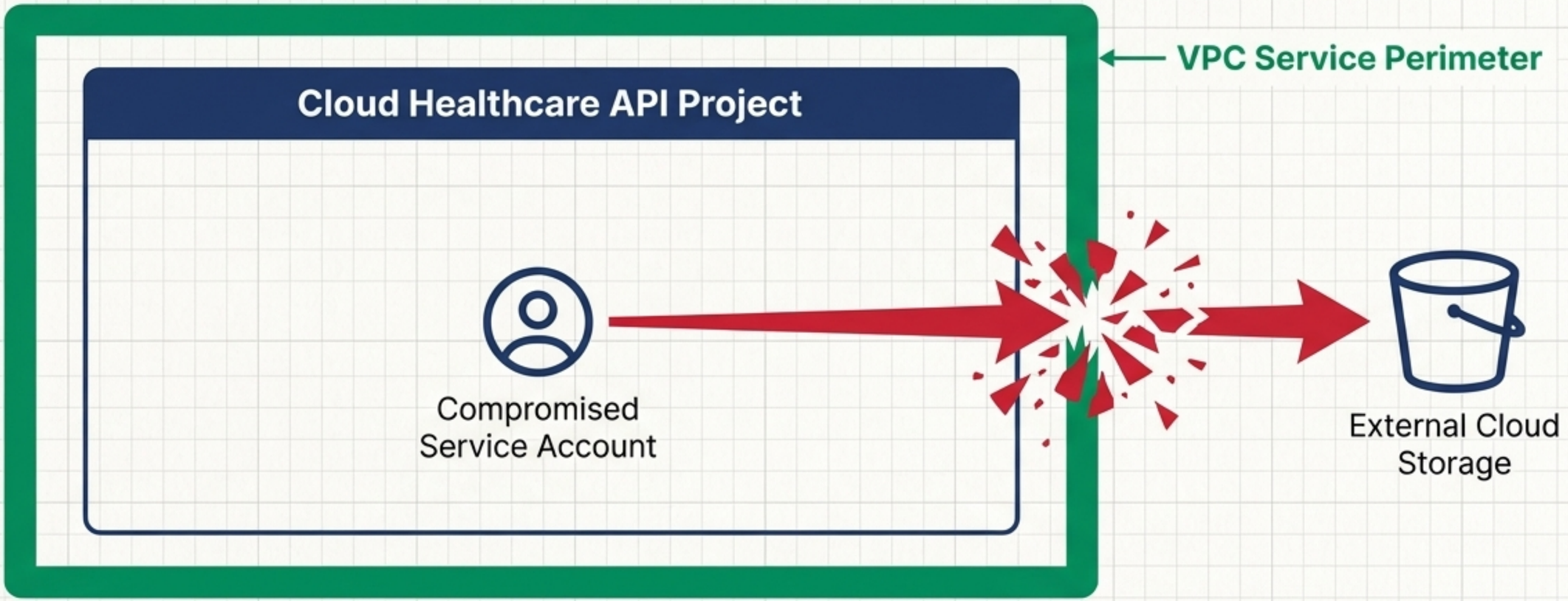
Variables: `support_users (Group 1)` maps Workspace Groups.

Custom SAs Provisioned: `cloud_run_sa`, `gke_sa`, `cloud_build_sa`

Console Location: IAM & Admin > Service Accounts

Assigned Roles:
`roles/cloudsql.client`
`roles/secretmanager.secretAccessor`

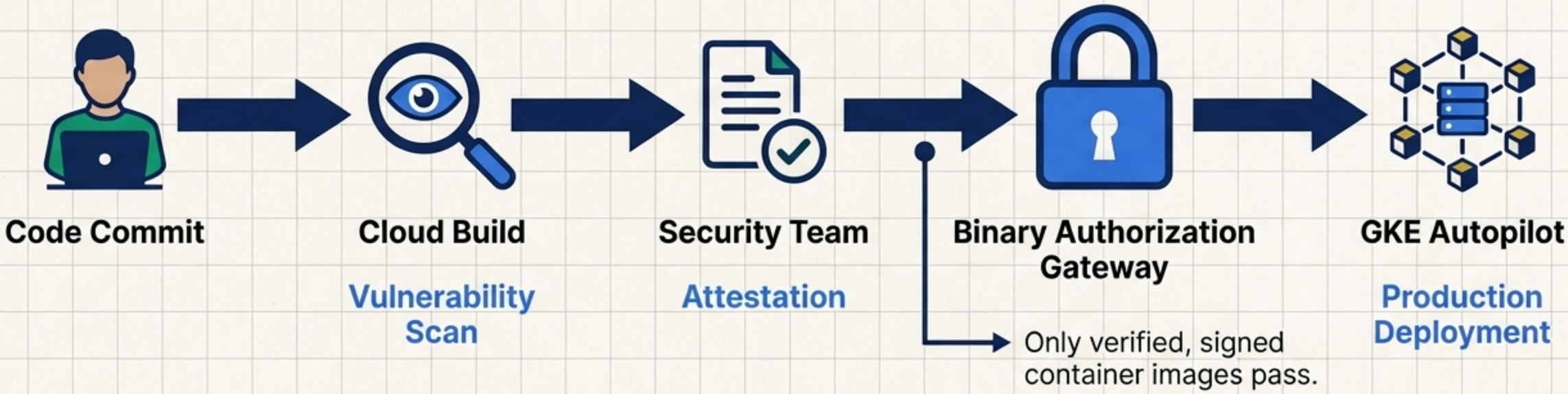
Network Data Protection: VPC Service Controls



Healthcare Mini-Case: A VPC perimeter ensures that even compromised credentials cannot be used to extract HIPAA data outside the trusted boundary.

```
RAD UI Variable: enable_vpc_sc (Group 10)
Console: Security > VPC Service Controls
```

Securing the Software Supply Chain



RAD UI Variable: enable_binary_authorization (Group 11)

Console: Security > Binary Authorization

Concept: Prevents supply-chain attacks where malicious dependencies are introduced in CI builds by enforcing deployment policies.

Core Data Layer: Secrets & Encryption

Automated Secret Rotation

RAD UI: enable_auto_password_rotation (Group 11/17)

Console: Security > Secret Manager

Mechanics: Automates credential rotation, securely passing them to workloads without exposing values in code or config files.

Architect's Annotation

Customer-Managed Encryption Keys (CMEK)

1. Create a Cloud KMS Key Ring and Key.
2. Encrypt Cloud Storage buckets or Compute Engine disks with the CMEK.

Critical Exam Concept: CMEK provides absolute control over key rotation and revocation. Revoking a CMEK immediately renders encrypted data inaccessible—the optimal architecture for satisfying GDPR right-to-erasure (data destruction).

Securing Next-Generation Workloads

Securing AI Models

Model Armor

Explores mechanisms to secure model deployment and sanitize training data against prompt injection and data poisoning attacks.

Sensitive Data Protection

DLP API

Real-time stream processing or scheduled storage scans to actively detect, redact, and mask Personally Identifiable Information (PII).

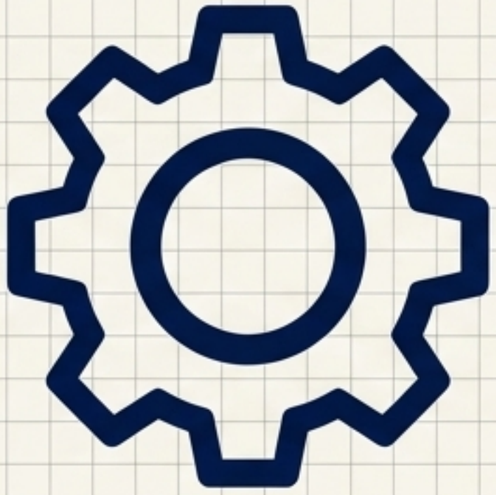
Data Sovereignty

Assured Workloads

Enforcing strict data residency and sovereignty requirements for government or heavily regulated deployments based on geographic region selection.

Oversight Layer: Cloud Audit Logs

Enabled by default. Low volume. Captures API calls that modify resource configurations or metadata.



GCP Resources

Admin Activity Logs

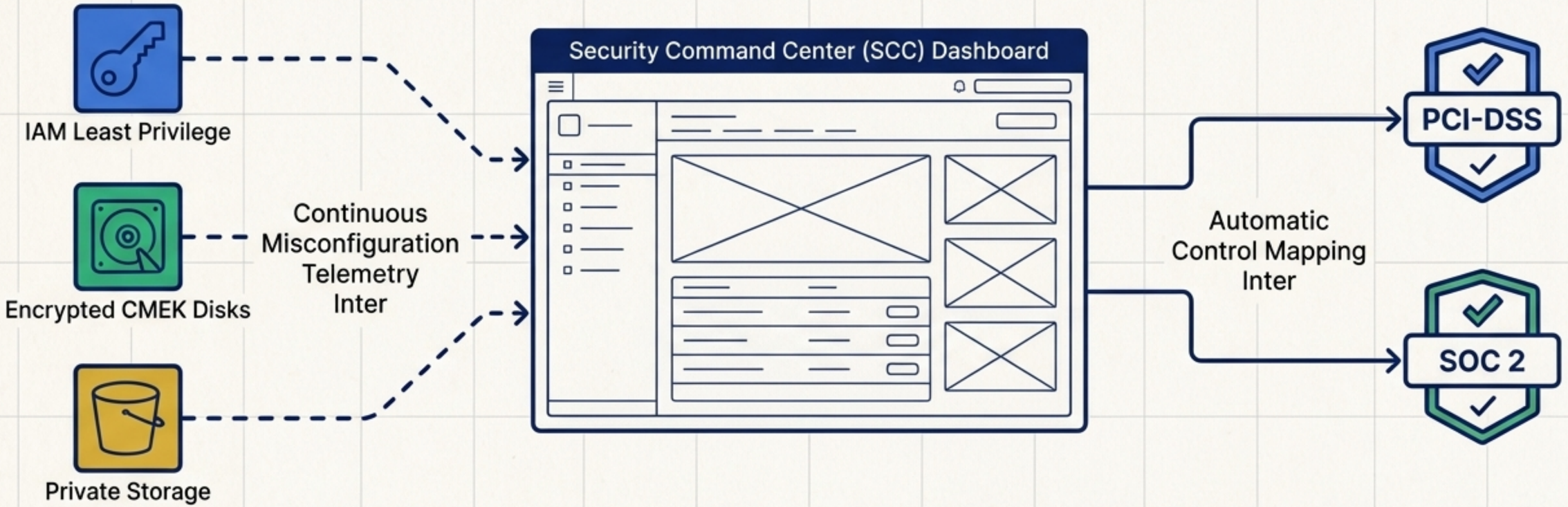
Data Access Logs

BigQuery

Must be manually enabled. High volume. Captures API calls that read metadata or read/write user-provided data.

Best Practice: Export Data Access logs to BigQuery via Log Router sinks for long-term retention, SQL-based threat hunting, and deep forensic analysis.

Synthesis: Continuous Compliance & SCC



Blueprint Callout

Payment Processor Mini-Case: SCC ingests telemetry proving no public buckets exist and CMEK is used, instantly generating evidence to satisfy PCI-DSS audit controls.

Terminal

```
RAD UI: enable_security_command_center (Group 16)

Console: Security > Security Command Center
```