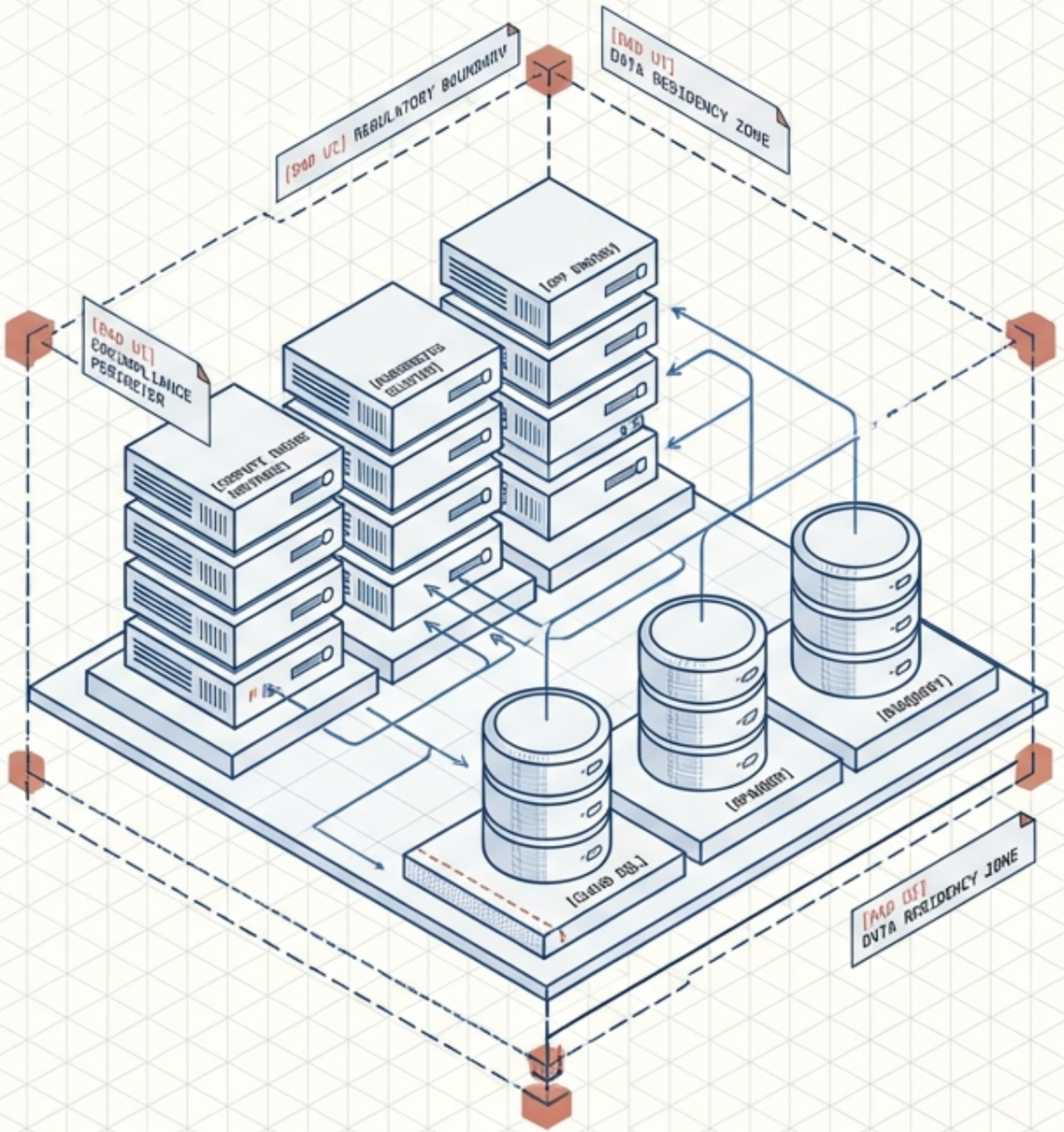
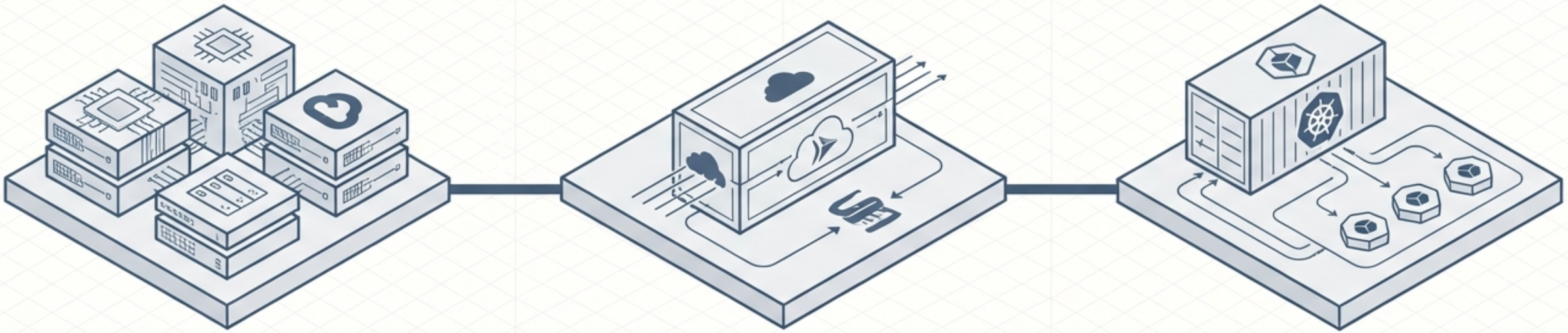
Supporting Compliance Requirements

Google Cloud PSE Exam Guide (Section 5)

Mastering SCC, Shared Responsibility, and Regulatory Posture (~11% of the Exam).



THE ECOSYSTEM



[GCP Services]
Infrastructure Foundation

[App CloudRun]
Serverless Workloads

[App GKE]
Containerized Workloads

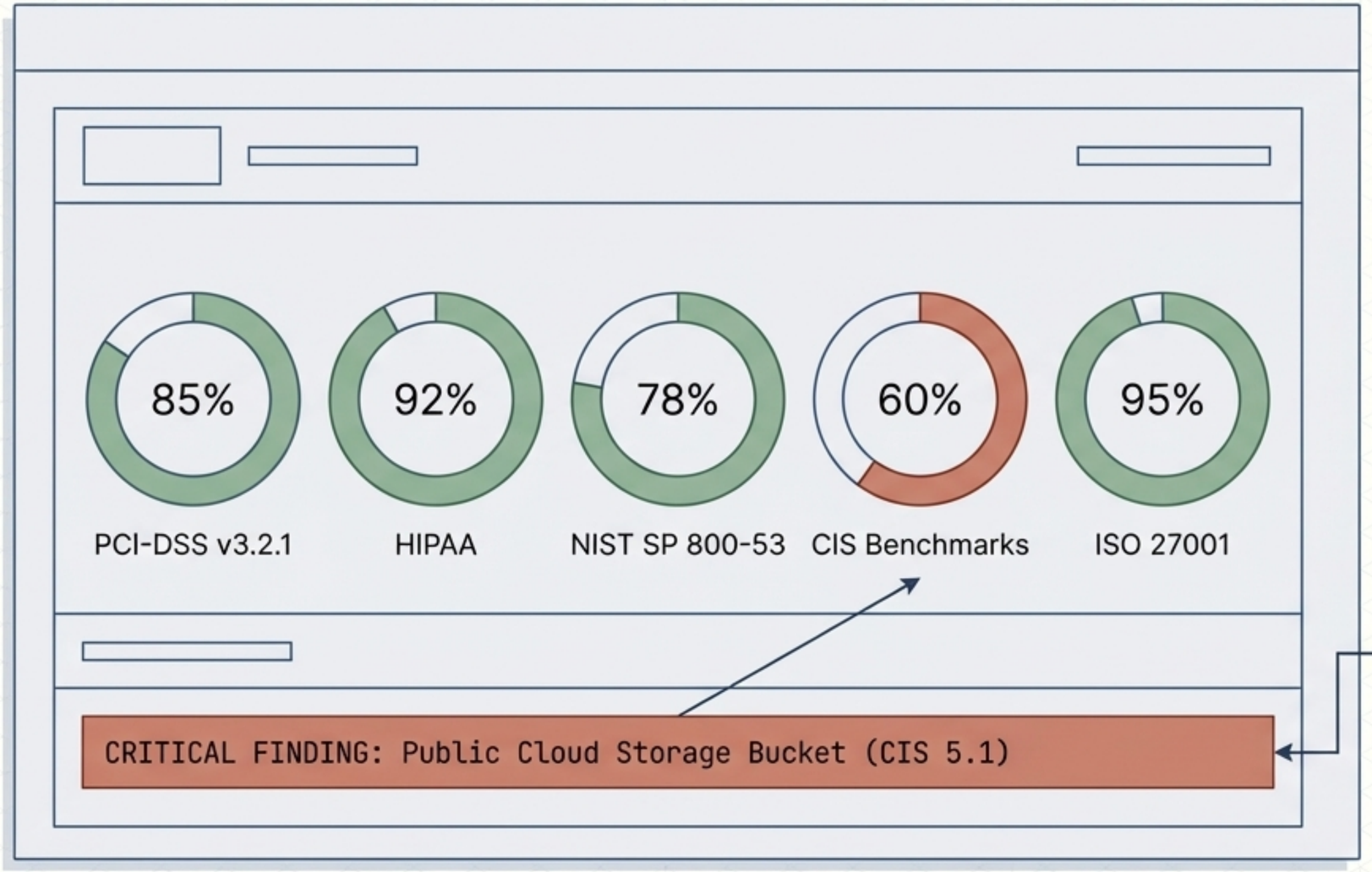
THE MANDATE

Section 5 Mandate:
Translate abstract regulatory frameworks into concrete GCP configurations.

THE LEGEND

`[RAD UI: variable_name]` Identifies deployment variables.

`[Console: Navigation > Path]` Identifies verification paths.



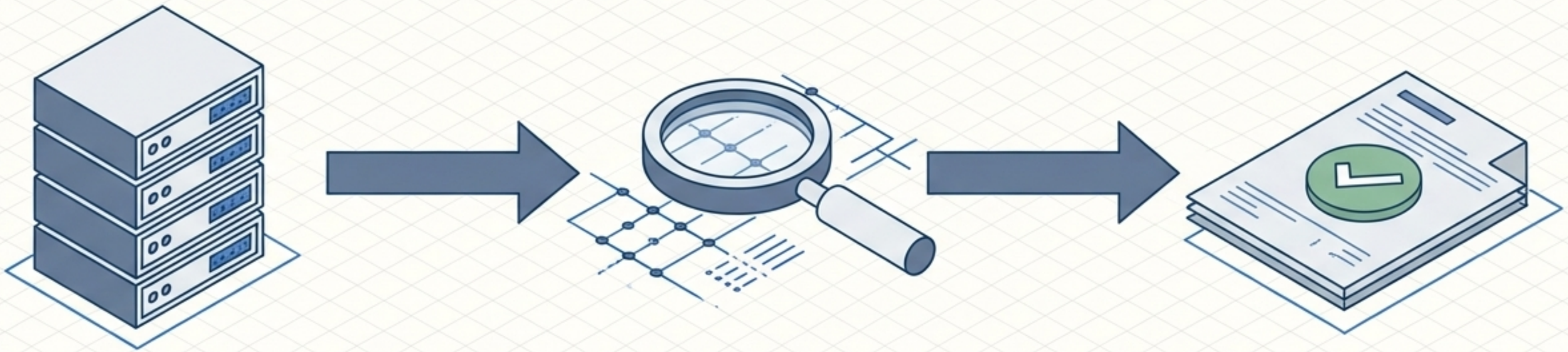
SCC: Continuous Compliance Posture

SCC continuously scans deployed resources for misconfigurations, directly mapping findings to exact compliance control IDs and providing remediation guidance.

[RAD UI: enable_security_command_center (Group 16)]

[Console: Security > Security Command Center > Posture management]

SCC in the Real World: The Auditor's Artifact



Cloud Resource Scanning

SCC Finding Match

```
Mapping: Requirement 6.3.3
         Requirement 7.2
```

Exported Defensible Report

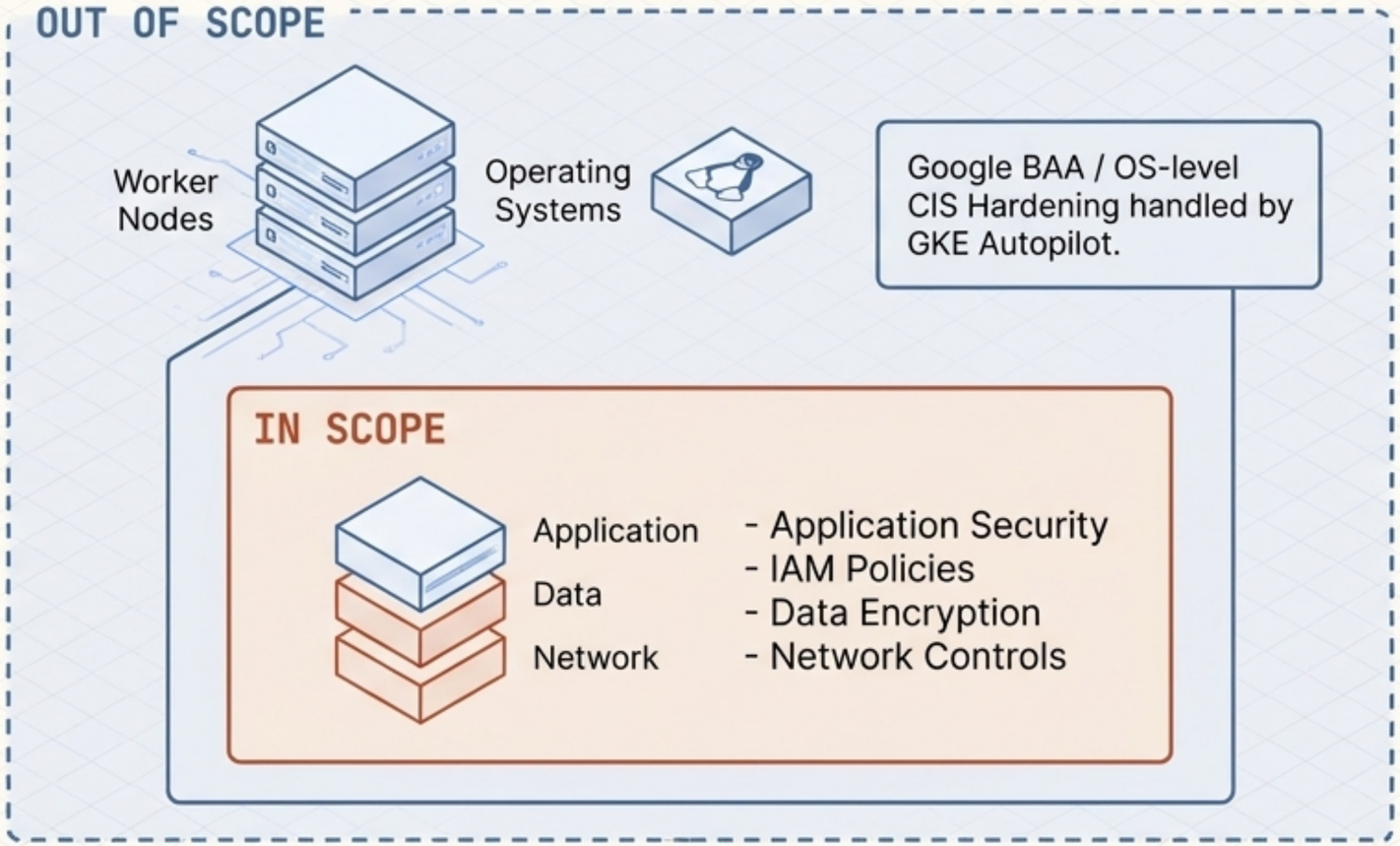
The Payment Processor Scenario: During an annual **PCI-DSS QSA** audit, SCC automatically identifies vulnerabilities and least-privilege violations, mapping them directly to **PCI requirements**. This transforms weeks of manual spreadsheet tracking into hours of automated evidence generation.

Shifting the Burden: The Shared Responsibility Model

By deploying workloads on GKE Autopilot, organizations dramatically shrink their infrastructure hardening scope.

Control Domain	GKE Standard Customer	GKE Autopilot Google
Node OS Security	Customer Managed	Google Managed
Node Pool Configuration	Customer Managed	Google Managed
System Pod Management	Customer Managed	Google Managed
Node-level Patching	Customer Managed	Google Managed
Application Code	Customer Managed	Customer Managed

Scope Reduction in Action: HIPAA Compliance

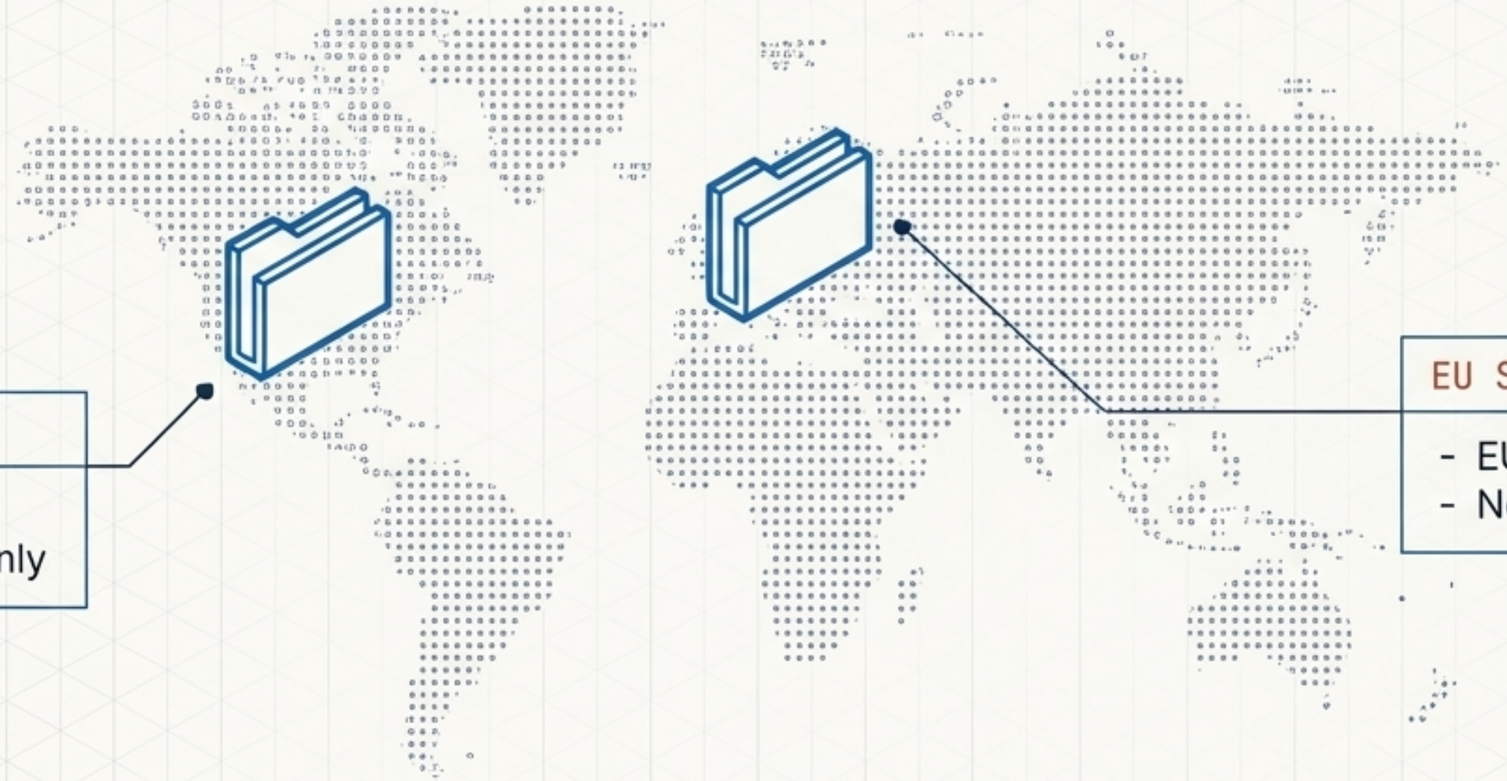


With Autopilot, the healthcare startup avoids the operational drain of OS hardening. Google's BAA covers the underlying infrastructure, narrowing the focus to application-layer controls.

[Console: Kubernetes Engine > Clusters > Security Tab]

Assured Workloads: Sovereign & Regulated Enclaves

Automatically enforcing Organization Policies to constrain data location and support access.



FedRAMP High

- US Regions Only
- Cleared US Staff Only

EU Sovereign Controls

- EU Data Processing
- No non-EU Staff Access

`[Console: Compliance > Assured Workloads]`

Auditing the Provider: Transparency vs. Approval

Access Transparency

`Type: PASSIVE LOGGING`

Captures Google's administrative actions on your resources (Justification, Data Location, Employee Role).

```
[Console: Logging > Logs Explorer (filter:
cloudaudit.googleapis.com%2Faccess_transparency)]
```

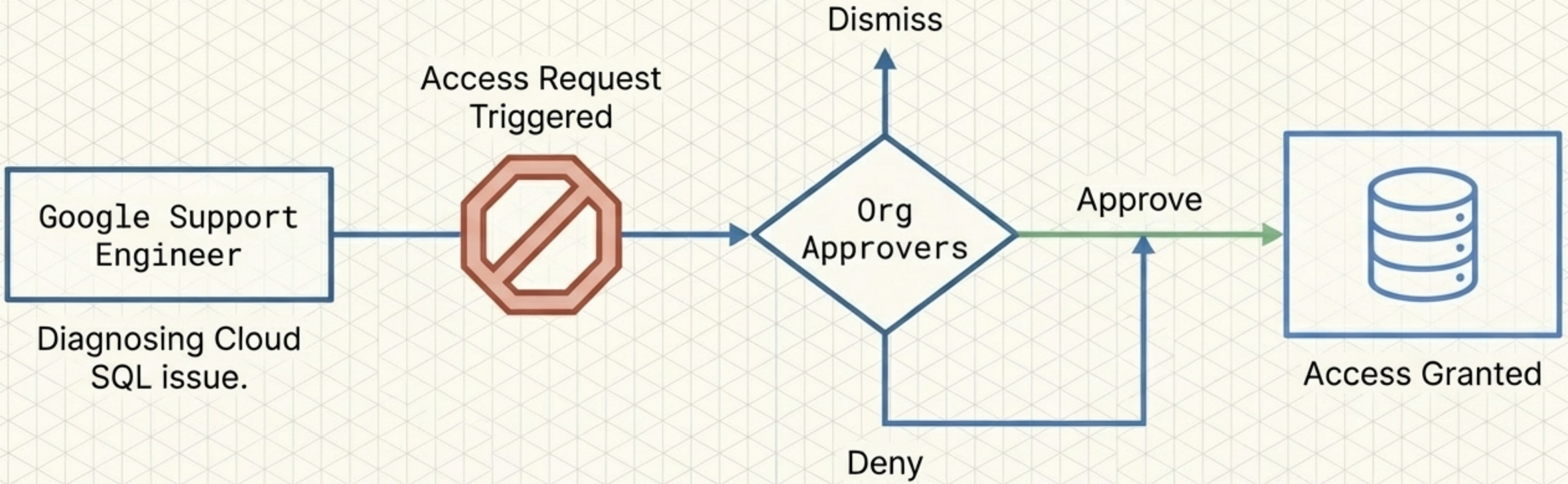
Access Approval

`Type: ACTIVE CONTROL`

An explicit approval gate requiring customer consent before Google staff can access configurations or content.

The Access Approval Workflow

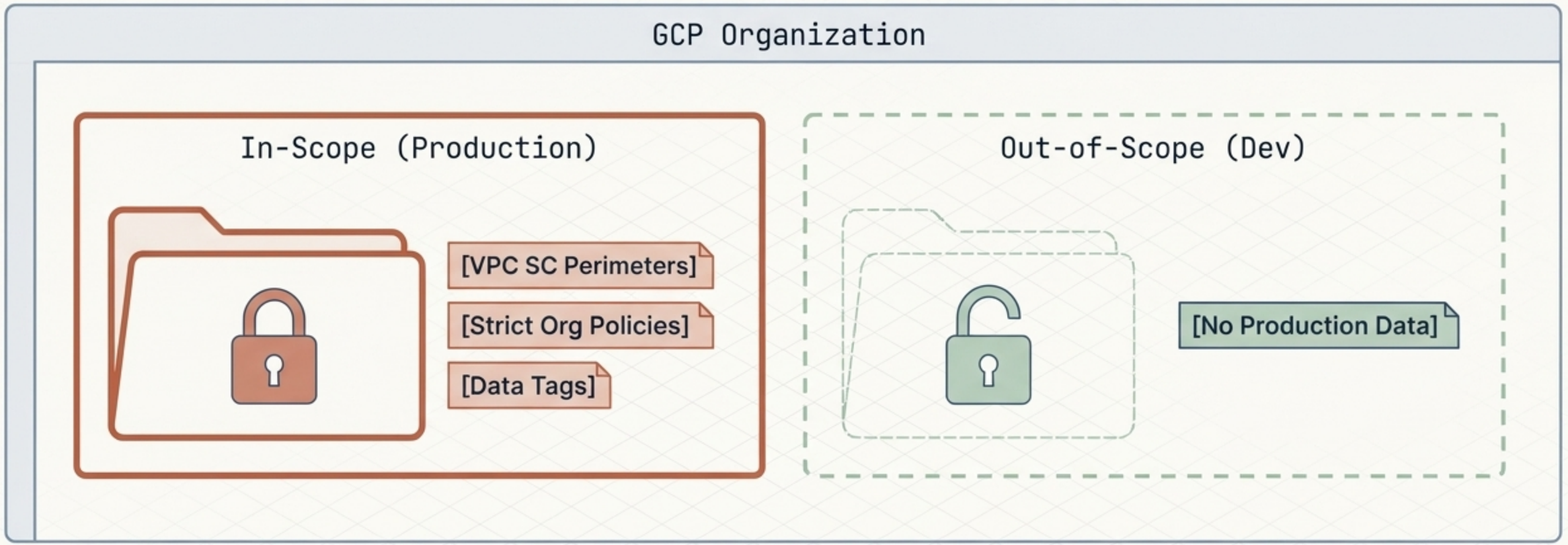
Google staff cannot bypass this gate without explicit customer authorization.



[Console: IAM & Admin > Access Approval]

Demarcating the Compliance Boundary

Compliance scope is targeted, not universal. Isolate regulated data to save operational overhead.



Use tags and labels to demarcate in-scope resources. Relaxing controls on out-of-scope environments reduces friction without increasing regulatory risk.

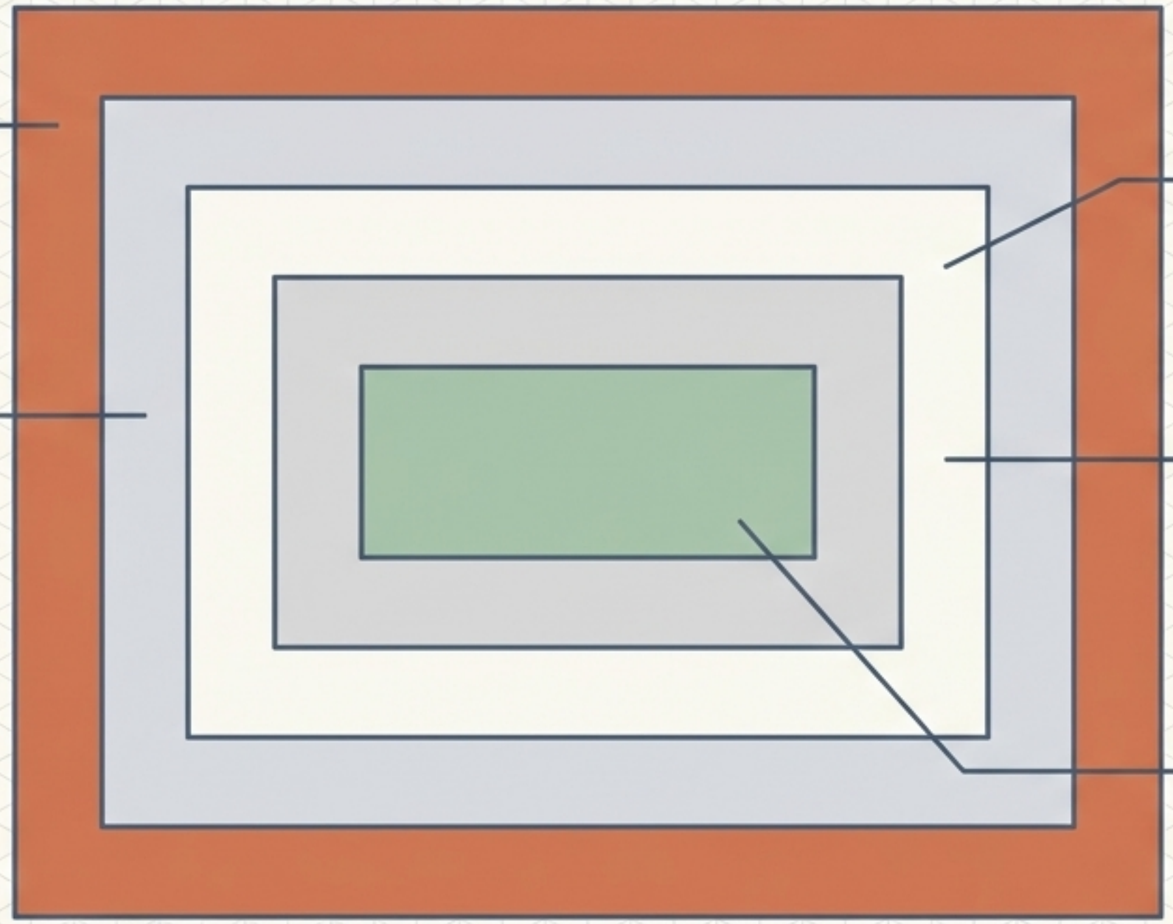
SYNTHESIS 1: Mapping Law to Cloud Control

A key PSE exam skill: linking legal mandates directly to specific GCP services.

Regulation	Requirement	GCP Service Implementation	Architecture Layer
PCI-DSS (8.4)	MFA for Admin Access	Cloud Identity 2-Step + IAP	Access Control
PCI-DSS (10.5.1)	Protect Audit Logs	Cloud Logging + Bucket Lock (WORM) + restricted logging.admin	Audit/Storage
GDPR (Art. 17)	Right to Erasure	CMEK Key Revocation + SDP De-identification	Data/Encryption
HIPAA (164.312)	Transmission Security	TLS 1.2+ Enforced at Load Balancer + Direct VPC Egress	Network

SYNTHESIS 2: The Composite Security Architecture

No single control satisfies a regulatory framework. They must be composed together.



JetBrains Mono

Summary & Console Action Plan

Theory into Practice: Execute these workflows to solidify Section 5 mastery.

- [x] Deploy JetBrains Mono “enable_security_command_center” via JetBrains Mono ‘RAD UI” and review JetBrains Mono ‘Posture Management’.
- [ ] Inspect the Security Tab on a JetBrains Mono “GKE Autopilot” cluster.
- [ ] Configure a compliant folder in JetBrains Mono “Assured Workloads”.
- [ ] Set up Access Approval routing for an JetBrains Mono “Org Approver”.
- [ ] Query Logs Explorer for JetBrains Mono “cloudaudit.googleapis.com%2Faccess_transparency”.