

ASSESS THE COMPUTE YOU NEVER SEE

A function can finish before the evidence request is written. A container can disappear before the assessor sees it. The assessment obligation does not disappear with the runtime.

PRACTITIONER POSITION

My practitioner position is that a serverless, functions, Lambda, managed-container, or orchestration service must be assessed as a governed operating system, not as a pile of short-lived machines and not as a provider product name. The exact provider service may be included in the provider's current PCI DSS assessment, but that fact does not automatically make the customer's account, subscription, project, resource, workload, configuration, identity, image, code, deployment path, data flow, or operating evidence compliant. Provider coverage answers a provider-assurance question. The assessed entity and assessor still need to establish what the customer deployed, how it can affect the security of the CDE, which responsibilities remain customer or shared, what population existed during the period, how changes were controlled, and what evidence supports each applicable assessment claim.

THE FIELD PATTERN

WHAT THIS LOOKS LIKE IN PRACTICE

An entity says that its payment workload is fully managed: API Gateway triggers functions, functions call managed queues and databases, container tasks scale to zero, images are replaced on every release, secrets come from a provider vault, and the cloud provider appears on a PCI DSS service list. The architecture diagram shows six service logos and no system components. The inventory lists one cloud account. The vulnerability report lists image repositories but not deployed digests. The responsibility matrix says 'AWS' or 'Azure' or 'Google' beside entire requirements. Every statement contains a useful fact. Together they still fail to identify the assessed population, the customer-controlled configuration, the influential control plane, or the proof chain for the period.

SIGNALS DETECTED

WHAT SHOULD MAKE YOU STOP

- The system inventory names a cloud account or service family but cannot enumerate the exact functions, services, clusters, task definitions, revisions, images, regions, and environments in the assessment population.
- The architecture uses provider logos where data flows, trust boundaries, identities, triggers, administrative paths, ingress, egress, and security dependencies should be shown.
- A provider AOC or services-in-scope page is treated as proof that the customer's deployed resource or workload is compliant.

- The responsibility matrix assigns whole PCI DSS requirements to the provider without resolving customer configuration, use, monitoring, evidence, and shared activities.
- Short-lived workloads are omitted from evidence because they no longer exist when the assessor requests a screenshot.
- Image tags such as 'latest' substitute for immutable digests, release manifests, deployment records, or a defensible workload population.
- Image scanning, runtime observation, configuration evaluation, penetration testing, and application testing are treated as interchangeable because they all produce security results.
- Infrastructure as code is presented as the environment without reconciling declared state to deployed state, exceptions, console changes, identities, and observed runtime behavior.

WHY IT MATTERS

THE COST OF LEAVING IT UNEXPLAINED

Ephemeral does not mean unidentifiable. The durable assessment objects are often the logical service, deployment definition, immutable artifact, account and region, identity, policy, network attachment, trigger, data store, secret, log destination, release event, and evidence-producing control. Runtime instances are occurrences of that governed design. The evidence model must preserve both the durable object and the population of relevant occurrences or revisions during the assessment period.

Provider assurance and customer implementation answer different claims. A current provider AOC and exact service coverage can support reliance on provider-performed activities. They do not prove that the customer selected an eligible architecture, configured the service securely, restricted identities and connectivity, protected secrets, retained logs, scanned images, controlled deployments, tested the application, or identified everything that can impact the security of the CDE.

Assessment testing should follow meaningful variation rather than chase every transient instance or accept one convenient example. Group resources only when the team can defend common code, artifact, configuration, ownership, deployment path, control behavior, and evidence. Split the population when runtime, region, trigger, identity, network, image, data handling, exception, or control implementation changes the claim.

The best evidence is born with the workload. Versioned infrastructure definitions, control-plane inventory, image digests, signed or attributable releases, configuration evaluations, identity and network policy, deployment logs, runtime telemetry, change records, exception state, and retained test results let the assessment reconstruct what existed even after the compute has disappeared.

QUESTIONS

QUESTIONS THAT EXPOSE THE WACK

- 01 Which exact provider services are consumed, and does the current provider evidence name those services, regions, and relied-upon activities?
- 02 Where can account data enter, move, persist, appear in logs or errors, or leave-and which services, identities, tools, people, and pipelines can impact the security of those paths?

- 03 What is the durable identity for every function, service, cluster, task definition, image, revision, account, subscription, project, region, and environment?
- 04 Which provider, customer, and shared activities apply at the service, configuration, workload, deployment, monitoring, and evidence seams?
- 05 How is the complete in-period population reconstructed when instances scale, restart, move, or disappear?
- 06 Which differences require separate populations or tests rather than one representative sample?
- 07 How are declared infrastructure, deployed configuration, emergency or console changes, runtime observations, exceptions, and evidence reconciled?
- 08 What change to code, image, runtime, region, identity, trigger, network, data flow, provider coverage, or responsibility assignment reopens the assessment claim?

THE CLUSTER OF WACK

FIND / MAP / EXPLAIN / REDUCE / PROVE

ESCAPE THE WACK

01 / FIND

Inventory the exact services and durable workload identities. Collect the provider AOC and service coverage, accounts and regions, resource inventory, code and image artifacts, deployment definitions, triggers, identities, networks, secrets, data stores, logs, pipelines, runtime records, exceptions, and tests.

02 / MAP

Draw two connected views: the account-data flow and the influence/control plane. Join each logical resource to its revisions and runtime occurrences, provider service coverage, customer and shared responsibilities, owners, applicable claims, evidence sources, and change triggers.

03 / EXPLAIN

State provider assurance and customer implementation separately. For each assessment claim, identify the exact subject, period, population, responsibility seam, test, evidence, exceptions, and limitation. Use 'covered by the provider's assessment' only for the supported provider service claim; do not promote it into 'this resource is compliant.'

04 / REDUCE

Remove unused services, broad identities, ambiguous triggers, unmanaged deployment paths, mutable image tags, duplicate environments, direct console changes, unnecessary data handling, and unsupported provider assumptions. Standardize only where the common control and evidence model is real.

05 / PROVE

Reconstruct one release from source and infrastructure definitions through immutable artifact, approval, deployment, observed configuration, runtime evidence, security testing, exception state, and retirement. Then compare the reconstructed population with the inventory, diagrams, scan targets, penetration-test scope, and claims ledger.

THE FIELD LAW

THE LINE WORTH REMEMBERING

THE RUNTIME MAY BE EPHEMERAL. THE ASSESSMENT STORY MUST BE DURABLE.

Download the Ephemeral Compute Assessment Map. Choose one payment-related function or container service and trace its provider coverage, customer configuration, identity, data and influence paths, immutable artifact, deployment history, in-period population, tests, evidence, owner, and reopening triggers. If the story ends at a service logo, the assessment has not reached the workload.

TECHNICAL GROUNDING

START WITH THE SOURCE MATERIAL

These references ground the practitioner interpretation. They do not turn the metaphor or method into official PCI DSS terminology.

- WACK-SOURCE-0001 / PCI DSS v4.0.1 / PCI Security Standards Council / [Open source](#)
- WACK-SOURCE-0002 / How is an entity's PCI DSS compliance impacted by using TPSPs? / PCI Security Standards Council / [Open source](#)
- WACK-SOURCE-0023 / FAQ 1065: What is a TPSP expected to provide to customers as evidence of PCI DSS compliance? / PCI Security Standards Council / [Open source](#)
- WACK-SOURCE-0036 / Information Supplement: PCI SSC Cloud Computing Guidelines v3 / PCI Security Standards Council / [Open source](#)
- WACK-SOURCE-0037 / FAQ 1252: PCI DSS applicability to system components / PCI Security Standards Council / [Open source](#)
- WACK-SOURCE-0038 / FAQ 1579: TPSPs that can impact the security of payment account data / PCI Security Standards Council / [Open source](#)
- WACK-SOURCE-0039 / PCI DSS v4.0 SAQ D for Service Providers / PCI Security Standards Council / [Open source](#)
- WACK-SOURCE-0040 / AWS Services in Scope by Compliance Program: PCI DSS / Amazon Web Services / [Open source](#)
- WACK-SOURCE-0041 / Amazon ECS security and compliance / Amazon Web Services / [Open source](#)
- WACK-SOURCE-0042 / Azure PCI DSS compliance offering / Microsoft / [Open source](#)
- WACK-SOURCE-0043 / PCI DSS compliance in Google Cloud / Google Cloud / [Open source](#)

AUTHORITY CLASSIFICATION / PCI_SSC_SOURCE / PRACTITIONER_POSITION / PRACTITIONER_METHOD / AI_ASSISTED

Practitioner reviewed by Scott Norton on 2026-09-09 against canonical digest eb1299eec010be618405f4122340a5d1f8d992406063fa8114c1c2bb348c1787. Educational content, not a compliance determination. Independent practitioner resource; not affiliated with or endorsed by PCI SSC. Authorship and authority classification do not determine legal intellectual-property ownership.