

HOW TO RUN A CLUSTER MAPPING SESSION

Do not start the meeting by asking whether the environment is compliant. Start by asking everyone to draw the environment they think exists.

PRACTITIONER POSITION

A useful Cluster mapping session turns conflicting explanations into visible architecture, assigns uncertainty instead of hiding it, and produces a short list of facts the team can verify after the room clears.

THE FIELD PATTERN

WHAT THIS LOOKS LIKE IN PRACTICE

Security brings a network diagram. Compliance brings a scope inventory. Engineering brings a cloud account list. The TPSP manager brings three contracts and an AOC. Each artifact is internally reasonable, but the system names, boundaries, owners, and dependencies do not line up. The team has been trying to reconcile them in prose, one evidence request at a time.

SIGNALS DETECTED

WHAT SHOULD MAKE YOU STOP

- Participants use different names for the same system or service.
- A scope statement cannot be traced to a current connection, data flow, or security dependency.
- Exceptions appear as meeting lore rather than marked objects on the diagram.
- The person who can explain a dependency is not the person recorded as its owner.
- The meeting repeatedly debates conclusions before agreeing on observable facts.

WHY IT MATTERS

THE COST OF LEAVING IT UNEXPLAINED

The session is not a substitute for validation or assessment. Its purpose is to create a shared fact model: components, data flows, administrative paths, trust boundaries, third-party services, exceptions, owners, and evidence sources. Unknowns are valid outputs when they are named, assigned, and time-bounded.

A strong session reduces the Wack Tax on every later activity. Scope review, control testing, remediation, and evidence collection can refer to the same objects and relationships instead of reconstructing context from scratch.

QUESTIONS

QUESTIONS THAT EXPOSE THE WACK

- 01 Which current artifact is authoritative for each kind of fact-and where do authoritative artifacts conflict?
- 02 What connects to, administers, authenticates, monitors, configures, or can affect the security of the CDE?
- 03 Which statement in the room cannot yet be represented as an object or relationship on the map?
- 04 Who owns the next verification step for every unknown, and by what date?

THE CLUSTER OF WACK

FIND / MAP / EXPLAIN / REDUCE / PROVE

ESCAPE THE WACK

01 / FIND

Bring the current diagrams, inventories, data-flow records, exception lists, TPSP records, and evidence indexes into one working session.

02 / MAP

Draw components and relationships first; label each with source, owner, confidence, and last verification date.

03 / EXPLAIN

Capture disagreements as explicit hypotheses and assign the evidence needed to resolve each one.

04 / REDUCE

Remove duplicate labels, obsolete artifacts, and unnecessary dependencies revealed by the shared map.

05 / PROVE

Publish a dated baseline plus an action register for every unknown, conflict, and unverified boundary.

THE FIELD LAW

THE LINE WORTH REMEMBERING

IF THE ARCHITECTURE NEEDS THREE NARRATORS, IT NEEDS ONE SHARED MAP.

Which two teams would draw your CDE differently today?

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-0004 / Guidance for Compensating Controls and the Customized Approach / PCI Security Standards Council / [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

4262e88bce38bd3480e91095e49feefc0ca0382f21241ae5197b35fe70cd8de0. 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.