

FACILITATOR GUIDE

THE CLUSTER OF WACK

A speaker-ready runbook for the PCI DSS practitioner community

Participants will leave with memorable language for accumulated control complexity and a five-step method for turning an uncomfortable architecture conversation into a shared map, accountable decisions, and traceable evidence.

Primary format: 45 minutes / 24 slides / facilitated mapping exercise

Cluster of Wack and related terms are independent practitioner shorthand, not PCI SSC terminology. The session is educational and does not provide an assessment conclusion or imply affiliation with or endorsement by PCI SSC.

Session at a glance

AUDIENCE

PCI DSS assessors, security leaders, program owners, architects, and control operators

LEARNING OBJECTIVES

- Recognize when several individually defensible decisions have combined into one hard-to-explain control environment.
- Separate observed facts, inherited assumptions, scope conclusions, ownership decisions, and evidence claims.
- Apply Find, Map, Explain, Reduce, and Prove to one real relationship without pretending the exercise itself determines compliance.
- Use humor to open a difficult practitioner conversation without trivializing the standard or the work.

BOUNDARY

Cluster of Wack and related terms are independent practitioner shorthand, not PCI SSC terminology. The session is educational and does not provide an assessment conclusion or imply affiliation with or endorsement by PCI SSC.

Three timing versions

30-minute session

Use 22 slides; reserve 4 minutes for the exercise and 3 minutes for questions.

45-minute session

Use 24 slides; reserve 8 minutes for the exercise and 5 minutes for questions.

60-minute session

Use 24 slides; reserve 16 minutes for the exercise and 10 minutes for questions. Invite two participant map readouts and use the Diagram Drift and Evidence Lineage Case Files as additional discussion prompts.

Room and facilitator preparation

- Confirm the meeting's recording, photography, attribution, and distribution expectations.
- Replace the speaker placeholder in the submission packet and title-slide notes.
- Complete practitioner review of PCI DSS wording and TPSP nuance before external use.
- Prepare one participant workbook per person or provide the stable digital download.
- Use a timer for the mapping exercise; protect the final five minutes for synthesis and questions.
- Invite fictional or sanitized examples only. Do not collect client facts or assessment evidence.

45-minute run of show

The slide budgets total 40 minutes. Hold five minutes for questions; recover time by compressing slides 6, 10, and 14 rather than cutting the exercise or close.

Slide	Section	Min	Facilitator job
1	THE CLUSTER OF WACK	1	Welcome the room and establish the tone: this is affectionate practitioner shorthand for a serious operating problem.
2	ONE WEIRD THING IS A FINDING.	1	Let the room laugh, then make the point.
3	COMPLEXITY IS NOT THE SAME AS WACK.	1	Do not frame complicated technology as inherently deficient.
4	THE WORKING DEFINITION	1	Walk through the terms quickly.
5	THE SENTENCES THAT SUMMON THE WACK	1	Read these as diagnostic triggers, not punchlines aimed at a team.
6	A MEMORABLE TERM SHOULD EARN ITS KEEP.	2	These terms are useful only when they improve a real conversation.
7	OUT OF SCOPE ON MONDAY. PATCHING THE CDE ON TUESDAY.	3	Tell the cold open.
8	WHAT CHANGED ON PATCH TUESDAY?	1	Pause before revealing the last line.
9	BUILD A SCOPE STORY, NOT A SCOPE ADJECTIVE.	1	A defensible scope story distinguishes the observed facts from the conclusion.
10	THE DASHBOARD WAS GREEN. THE POPULATION WAS MISSING.	2	A successful tool result can be accurate for the systems the tool observed while remaining silent about systems absent from its population.

Slide	Section	Min	Facilitator job
11	GREEN IS A RESULT. PROOF NEEDS A CHAIN.	1	Use the six labels as a verbal evidence chain.
12	THE AOC ANSWERED A QUESTION. NOT THIS ONE.	3	Explain the composite: a provider document described the provider's assessed services, but the customer needed to know how responsibility operated for the specific service relationship.
13	AN AOC IS NOT A RESPONSIBILITY MATRIX.	2	Walk across the seam from provider to customer.
14	WACK HAS MECHANICS.	1	Connect the vocabulary as a causal sequence.
15	THE TEMPORARY RULE BECAME LOAD-BEARING.	2	Tell the pattern: a temporary firewall exception outlived the original need, gained consumers, entered operating assumptions, and became difficult to remove because nobody could confidently predict the blast radius.
16	CHOOSE ONE RELATIONSHIP THAT MAKES PEOPLE SAY: IT'S COMPLICATED.	1	Distribute or point to the participant workbook.
17	01 / FIND THE WACK	2	Give the room about sixty seconds to write.
18	02 / MAP THE WACK	3	Ask participants to draw boxes and arrows, not a polished architecture diagram.
19	03 / EXPLAIN THE WACK	2	Push past historical origin stories.
20	04 / REDUCE THE WACK	2	Reduction should change the map, not merely improve the prose.
21	05 / PROVE WHAT REMAINS	2	Proof is the durable bridge between the current architecture and the next reviewer.
22	THE WAY OUT IS A SHARED STORY THAT CAN BE TESTED.	2	This is the synthesis.
23	SIX QUESTIONS TO TAKE TO THE NEXT MEETING	2	Read the questions slowly.
24	FIND. MAP. EXPLAIN. REDUCE. PROVE.	1	End on the method rather than a generic thank-you slide.

Slide-by-slide talk track

01 / THE CLUSTER OF WACK

Timing: 1 minute. Slide job: title.

Welcome the room and establish the tone: this is affectionate practitioner shorthand for a serious operating problem. The session is not a new framework, an assessment shortcut, or official PCI SSC terminology. It is a way to name the moment when architecture, ownership, scope, and evidence stop telling the same story.

Transition: *Start with a scene almost everyone in the room has experienced.*

02 / ONE WEIRD THING IS A FINDING.

Timing: 1 minute. Slide job: quote.

Let the room laugh, then make the point. The difficult environments are rarely created by one spectacularly bad decision. They emerge from many reasonable local decisions whose combined effect was never reviewed. Ask for a show of hands: who has heard a scope explanation begin with 'Well, historically...' this year?

AUDIENCE PROMPT

What phrase tells you an architecture explanation is about to get interesting?

Transition: *The joke works because it describes an accumulation problem.*

03 / COMPLEXITY IS NOT THE SAME AS WACK.

Timing: 1 minute. Slide job: definition.

Do not frame complicated technology as inherently deficient. A large distributed environment may be well controlled. The diagnostic concern is the loss of a shared and testable explanation: teams cannot agree what touches what, who owns the relationship, which requirements depend on it, or what evidence proves the operating claim.

Transition: *That gives us a working definition.*

04 / THE WORKING DEFINITION

Timing: 1 minute. Slide job: formula.

Walk through the terms quickly. None is automatically a finding. Each becomes dangerous when it prevents the team from forming one coherent control story. Emphasize that this vocabulary is designed to expose questions, not manufacture conclusions.

Transition: *The fastest way to see the definition is through its recurring signals.*

05 / THE SENTENCES THAT SUMMON THE WACK

Timing: 1 minute. Slide job: signals.

Read these as diagnostic triggers, not punchlines aimed at a team. Every sentence contains a potentially valid fact and an invitation to ask for the missing relationship. The method works because it turns sarcasm into a useful follow-up question.

AUDIENCE PROMPT

Which sentence consumes the most assessment time in your environment?

Transition: *The Wacktionary gives those recurring patterns handles.*

06 / A MEMORABLE TERM SHOULD EARN ITS KEEP.

Timing: 2 minutes. Slide job: vocabulary.

These terms are useful only when they improve a real conversation. Give one sentence for each and avoid teaching the entire twenty-term catalog. The goal is to show how a playful label can help a mixed technical and governance group identify the same condition quickly.

Transition: *Now open the first case file.*

07 / OUT OF SCOPE ON MONDAY. PATCHING THE CDE ON TUESDAY.

Timing: 3 minutes. Slide job: case.

Tell the cold open. A corporate utility stored no payment data and appeared outside the boundary. During a routine patching demonstration, the team used it to administer in-scope systems. No one was concealing the relationship; the scope explanation had simply frozen around data location while operational reach continued to evolve.

Transition: *The observed workflow did not automatically determine scope, but it made the current rationale incomplete.*

08 / WHAT CHANGED ON PATCH TUESDAY?

Timing: 1 minute. Slide job: question.

Pause before revealing the last line. The maintenance window exposed a relationship that had existed for some time. This distinction matters: discovery is not the same as creation, and a newly visible relationship deserves analysis before blame or a rushed label change.

AUDIENCE PROMPT

Which fact was observed, and which conclusion still needed to be made?

Transition: *The team needed more than a color in a workbook.*

09 / BUILD A SCOPE STORY, NOT A SCOPE ADJECTIVE.

Timing: 1 minute. Slide job: principle.

A defensible scope story distinguishes the observed facts from the conclusion. Avoid presenting this list as a substitute for PCI DSS scoping guidance; it is a communication and evidence discipline for making the rationale inspectable and maintainable.

Transition: *A different case shows the same accumulation problem in evidence.*

10 / THE DASHBOARD WAS GREEN. THE POPULATION WAS MISSING.

Timing: 2 minutes. Slide job: case.

A successful tool result can be accurate for the systems the tool observed while remaining silent about systems absent from its population. Describe the collision without asserting that every dashboard must provide every proof element. The question is what claim the artifact is being asked to support.

Transition: *A result and the evidence chain around that result are different things.*

11 / GREEN IS A RESULT. PROOF NEEDS A CHAIN.

Timing: 1 minute. Slide job: chain.

Use the six labels as a verbal evidence chain. The room should understand that evidence quality depends on the claim being tested. A beautiful dashboard can still require population, timing, exception, and ownership context before another person can interpret it responsibly.

Transition: *The same issue appears at provider boundaries.*

12 / THE AOC ANSWERED A QUESTION. NOT THIS ONE.

Timing: 3 minutes. Slide job: case.

Explain the composite: a provider document described the provider's assessed services, but the customer needed to know how responsibility operated for the specific service relationship. Keep the distinction careful and source-aware. Provider assurance material matters; it does not automatically become a service-specific responsibility matrix for the customer.

Transition: *Documents do not own shared activities; people and agreements do.*

13 / AN AOC IS NOT A RESPONSIBILITY MATRIX.

Timing: 2 minutes. Slide job: principle.

Walk across the seam from provider to customer. The practical output is not distrust of third parties; it is explicit mapping of relied-upon activities, customer obligations, shared handoffs, evidence, and escalation. Cite PCI SSC TPSP guidance in the notes and avoid quoting standard text on the slide.

Transition: *These cases look different, but the accumulation mechanics are the same.*

14 / WACK HAS MECHANICS.

Timing: 1 minute. Slide job: model.

Connect the vocabulary as a causal sequence. This is not a quantitative risk model. It is a way to explain why a local exception becomes hard to remove and why assessment effort grows even when no single control changed dramatically.

Transition: *The fourth case makes those mechanics visible.*

15 / THE TEMPORARY RULE BECAME LOAD-BEARING.

Timing: 2 minutes. Slide job: case.

Tell the pattern: a temporary firewall exception outlived the original need, gained consumers, entered operating assumptions, and became difficult to remove because nobody could confidently predict the blast radius. The answer was not one heroic deletion; it was a controlled sequence of mapping, narrowing, observation, and evidence.

Transition: *Now let the audience apply the method to one relationship of their own.*

16 / CHOOSE ONE RELATIONSHIP THAT MAKES PEOPLE SAY: IT'S COMPLICATED.

Timing: 1 minute. Slide job: exercise.

Distribute or point to the participant workbook. Ask each person to choose one relationship they can describe without including sensitive data. They may work alone or with a neighbor. The exercise is diagnostic and educational; it does not decide compliance.

AUDIENCE PROMPT

Write one sentence that your team currently uses to explain the relationship.

Transition: *Work the five moves in order.*

17 / 01 / FIND THE WACK

Timing: 2 minutes. Slide job: method.

Give the room about sixty seconds to write. Encourage observation over opinion: a maintenance action, authentication path, provider handoff, exception renewal, or evidence reuse. A good Find statement describes what happened and why it contradicts or exceeds the existing explanation.

Transition: *Once the contradiction is visible, draw the relationship.*

18 / 02 / MAP THE WACK

Timing: 3 minutes. Slide job: method.

Ask participants to draw boxes and arrows, not a polished architecture diagram. Use white for known facts, orange for assumptions, and red for decisions or disputed edges. Include human approval and evidence handoffs when they determine how the control operates.

AUDIENCE PROMPT

Circle the edge that would be hardest to explain to a new owner.

Transition: *A map without ownership is only a better-looking mystery.*

19 / 03 / EXPLAIN THE WACK

Timing: 2 minutes. Slide job: method.

Push past historical origin stories. The practical question is why the relationship remains necessary now, who can change it, who owns the resulting decision, and which control or scope claims rely on it. Different ownership roles can be legitimate; ambiguity should not be mistaken for distributed accountability.

Transition: *Explanation creates the conditions for safe reduction.*

20 / 04 / REDUCE THE WACK

Timing: 2 minutes. Slide job: method.

Reduction should change the map, not merely improve the prose. Encourage the smallest safe experiment: remove one consumer, constrain one path, assign one owner, or test one retirement step while observing the result. Do not prescribe technical change without the owner's change and risk processes.

Transition: *What remains must be provable after the people in this room move on.*

21 / 05 / PROVE WHAT REMAINS

Timing: 2 minutes. Slide job: method.

Proof is the durable bridge between the current architecture and the next reviewer. Evidence should let another person reconstruct what exists, why it exists, who accepted it, how it operates, and when the rationale must be revisited.

Transition: *The method changes the quality of the conversation even before it changes architecture.*

22 / THE WAY OUT IS A SHARED STORY THAT CAN BE TESTED.

Timing: 2 minutes. Slide job: before after.

This is the synthesis. The desired state is not a perfectly simple environment. It is an environment whose important relationships are understandable, attributable, constrained, and supported by evidence that matches the claim.

Transition: *Close with the questions the audience can carry into Monday morning.*

23 / SIX QUESTIONS TO TAKE TO THE NEXT MEETING

Timing: 2 minutes. Slide job: takeaway.

Read the questions slowly. They work across scope, TPSP responsibility, evidence, exceptions, diagrams, and inherited controls. Invite the room to photograph the slide or use the workbook, subject to the meeting's rules.

Transition: *Return to the mantra and resolve the opening joke.*

24 / FIND. MAP. EXPLAIN. REDUCE. PROVE.

Timing: 1 minute. Slide job: close.

End on the method rather than a generic thank-you slide. Reinforce the boundary: the vocabulary is independent practitioner shorthand; the discipline is to make real relationships explainable and testable. Invite questions and practitioner counterexamples.

AUDIENCE PROMPT

Where does the Wack hide in otherwise reasonable systems?

Facilitating the mapping exercise

Set the boundary

Participants choose one relationship but exclude identifying system names, client data, evidence, and incident details.

Keep the drawing rough

Boxes and arrows are enough. The exercise rewards visible relationships, not architecture-diagram polish.

Separate statement types

Known facts go in white, assumptions in orange, and decisions or disputed edges in red.

Protect the method order

Do not jump from discovery directly to remediation. Map and explain the relationship before proposing reduction.

Debrief without judging compliance

Ask what became visible, which owner was missing, and what the next useful question is.

Likely questions

Is this a new PCI SSC framework?

No. It is independent practitioner shorthand for organizing accumulated complexity and the questions needed to examine it.

Does administrative reach automatically make a system in scope?

The talk deliberately does not make that conclusion. It shows why an observed relationship must be evaluated using applicable PCI DSS scoping guidance and the entity's facts.

Are dashboards or AOCs inadequate?

Not categorically. The question is whether the artifact and its context support the specific claim being made.

Is the Wack Score a compliance score?

No. It is an educational prioritization aid, not an assessment result.

Can we use a real client example?

Use a fictional composite or thoroughly sanitized pattern. Do not expose client facts, evidence, or identifying incident details.

Sources and review status

The session is speaker-ready as an internal draft. Normative phrasing remains pending named practitioner review before external submission or delivery.

- **PCI DSS v4.0.1 - PCI Security Standards Council.**

https://www.pcisecuritystandards.org/document_library/?class=pcidss&doc=pci_dss

- **How is an entity's PCI DSS compliance impacted by using TPSPs? - PCI Security Standards Council.** <https://www.pcisecuritystandards.org/faqs/1312/>

- **Is sampling allowed in PCI DSS v4.x? - PCI Security Standards Council.**

<https://www.pcisecuritystandards.org/faqs/1569/>

- **Guidance for Compensating Controls and the Customized Approach - PCI Security Standards Council.** <https://blog.pcisecuritystandards.org/pci-ssc-publishes-new-guidance-on-compensating-controls-and-the-customized-approach>