

PCI AT THE KITCHEN LINE

Pickleball rewards the same habits sustainable compliance programs need: know the boundaries, control the pace, communicate early, and stop trying to smash every ball.

By Scott Norton / PCI DSS QSA | Johanson Group, LLP

PRACTITIONER POSITION Not every ball is yours, not every shot should be hard, and the kitchen is still a boundary even when nobody drew it on your spreadsheet.

Pickleball looks easy from outside the fence. The court is small, the rules seem familiar, and somebody is always having a surprisingly serious conversation about whether the ball touched a line. Then you play. Pace changes. Angles matter. Partners collide because both assume the middle ball belongs to the other person. A patient dink creates more advantage than an ambitious smash from the wrong position.

That sounds uncomfortably familiar to PCI DSS operations. Programs struggle less from an absolute absence of activity than from uncertain boundaries, badly timed force, unclear ownership, and teams optimizing their own shot without understanding the rally. The metaphor is playful. The operating lesson is not: mature programs win through positioning, communication, and repeatable decisions more often than through heroic power.

KNOW THE KITCHEN BEFORE YOU ATTACK

The non-volley zone changes which shots are legal depending on where the player stands and how the ball arrives. Scope and control boundaries have a similar practical effect: the same component, connection, identity, or service may carry different implications because of its relationship to the payment environment. The line matters, but the situation around the line determines the play.

A weak program paints a boundary in a diagram and assumes the point is over. A stronger program knows what crosses the line, who can influence what sits behind it, which administrative paths exist, and what evidence proves the boundary is operating as described. 'Out' is a conclusion. The team still needs the line call.

CALL THE MIDDLE BALL

Doubles teams lose easy points when both players hesitate or both swing. Shared compliance responsibility behaves the same way. Security assumes infrastructure owns the configuration. Infrastructure assumes the provider owns the platform. The provider documents its portion. Nobody names who detects the condition, makes the decision, communicates the result, and closes the loop.

Good partners call the ball before it becomes an emergency. Responsibility maps should name the action and the handoff, not merely list two teams in the same cell. When the event occurs, one party should know

it acts first, another should know what it receives, and both should know which record proves the exchange.

STOP SMASHING EVERY CONTROL

Power feels decisive. So do emergency projects, giant evidence requests, universal escalations, and sweeping remediation plans. But a hard swing from poor position often produces an unforced error. Some problems need containment. Others need patient discovery: one dependency mapped, one population reconciled, one exception priced, one decision owner named.

The dink is not timid. It controls pace until the right opening appears. In compliance operations, that means choosing the smallest intervention that produces reliable information or removes a real source of Wack. A focused question asked repeatedly can change the operating model more effectively than a dramatic annual campaign nobody can sustain.

MAKE THE LINE CALL VISIBLE

Recreational pickleball depends on players making honest calls, especially when nobody else has the angle. Compliance also depends on people reporting what they observed without turning uncertainty into embarrassment. A control owner should be able to say the population was incomplete, the evidence source changed, or the exception returned without being pressured to convert the observation into a premature pass.

Trust grows when the call is visible and reviewable. Record what was observed, which rule or decision boundary applied, who made the call, and what happens next. The point is not to eliminate disagreement. It is to prevent the score from depending on whichever team tells the most confident story after the rally.

FIVE QUESTIONS FOR THE NEXT WORKING SESSION

- Which boundary is drawn but not operationally understood?
- Which middle ball currently belongs to two teams and therefore neither?
- Where is the program using force because it lacks positioning?
- What small, repeatable move would control the pace?
- Which line call needs an observed fact and a named decision owner?

ONE MOVE TO MAKE NOW

Run a kitchen-line review on one shared control: draw the boundary, name every crossing, call the first responder, and identify the record that proves the handoff.

THE PRACTITIONER POSITION

My practitioner position is that sustainable compliance is usually a positioning game. Know the boundary, communicate with the partner, preserve the line call, and use force only when the situation deserves it.

Also: stay out of the kitchen unless the ball bounced. Some rules become memorable because the metaphor does part of the teaching.

AUTHORITY AND SOURCES

Independent practitioner perspective. These dispatches are Scott Norton's practitioner analysis and recommendations, not PCI SSC terminology or guidance, not a formal position of Johanson Group, LLP, and not an assessment conclusion about any entity. AI assistance is recorded as production provenance; accountable professional judgment remains human.

Authority classification: PRACTITIONER_POSITION / PRACTITIONER_METHOD / AI_ASSISTED. Authorship and authority classification do not determine legal intellectual-property ownership.

- PCI DSS v4.0.1 - PCI Security Standards Council: https://www.pcisecuritystandards.org/document_library/?class=pcidss&doc=pci_dss