

GET YOUR PCI HOUSE IN ORDER BEFORE THE YEAR-END SLOWDOWN

The calendar does not become a control because everybody is out of office. Evidence windows keep moving, remediation still needs decisions, providers still have lead times, and assessors take time off too.

PRACTITIONER POSITION

My practitioner position is that year-end PCI readiness is capacity planning, not a universal PCI DSS deadline. The standard does not declare one common holiday cutoff, and every entity must follow its own applicable obligations, validation schedule, assessor plan, and compliance-accepting entity instructions. The operating problem is predictable: internal owners, approvers, change teams, service providers, ASVs, penetration testers, and assessors often have less shared availability late in the year while recurring control windows continue to expire. A responsible program creates a year-end landing zone before that compression begins. It identifies the claims that must mature, the occurrences that must happen on time, the evidence that must remain accessible, the exceptions that need decisions, and the people who can make those decisions while the normal bench is thin.

THE FIELD PATTERN

WHAT THIS LOOKS LIKE IN PRACTICE

In early December, an entity expects to finish its annual assessment before a business deadline. The last evidence request reveals an incomplete three-month occurrence, an unresolved scan exception, a provider AOC that needs service-level interpretation, and a network diagram update waiting on an engineer who is already out. The QSA has limited review days left, the compliance-accepting entity needs time to process the package, and a production freeze blocks the remediation path everyone assumed would remain open. No single person failed. The plan simply treated December as a normal month with extra decorations.

SIGNALS DETECTED

WHAT SHOULD MAKE YOU STOP

- The target completion date is known, but the entity has not worked backward through assessor review, internal approval, remediation, evidence refresh, and compliance-accepting entity processing time.
- The year-end plan assumes every control owner, provider contact, tester, approver, and assessor will be available during the same final two weeks.
- Recurring activities are scheduled around the assessment project rather than their actual fixed, risk-defined, change-triggered, or remediation timeframes.

- Open evidence questions have owners but no last responsible decision date before reduced staffing or a production freeze.
- The organization expects one final upload to resolve scope, population, exception, and evidence-sufficiency questions that have not yet been stated as claims.
- Provider attestations, ASV work, penetration testing, and other externally supplied evidence are requested without accounting for service lead times or clarification cycles.
- Only one person can explain a material scope or control position, and there is no delegated authority or durable decision record.
- The plan has a due date but no protected landing zone in which the evidence set, claims, exceptions, and report language stop changing long enough to review coherently.

WHY IT MATTERS

THE COST OF LEAVING IT UNEXPLAINED

A late-year crunch magnifies ordinary assessment friction. A missing owner becomes a stalled clarification. A small evidence defect becomes a lost review cycle. An ambiguous provider responsibility becomes a meeting that cannot happen until January. The resulting delay is often blamed on the assessor or the holiday calendar even though the underlying problem was an unmodeled dependency on scarce people and externally supplied work.

The year-end landing zone is a controlled readiness state, not a promise that nothing will change. Material changes, failed controls, new exceptions, and updated evidence must remain visible and may reopen affected claims. The landing zone gives those changes an explicit intake and decision path while protecting a coherent baseline for review.

This approach also protects technical honesty. PCI SSC FAQ 1572 explains that periodic controls cannot be performed retroactively after a required timeframe is missed. Pulling work forward, preserving every occurrence, and escalating gaps early cannot repair the past, but it can prevent a known upcoming window from expiring while the required people are unavailable.

QUESTIONS

QUESTIONS THAT EXPOSE THE WACK

- 01 What date must the final package reach the compliance-accepting entity, and what review and processing time exists between that date and the desired assessment completion?
- 02 Which fixed, risk-defined, change-triggered, remediation, and evidence-refresh clocks will mature during the reduced-availability period?
- 03 Which claims still depend on a scope decision, complete population, provider clarification, technical test, remediation result, or accountable approval?
- 04 What are the last responsible dates for evidence intake, entity response, assessor review, correction, retest, and report approval?

05 Who is available to make each decision, and who has delegated authority when the primary owner is absent?

06 Which planned changes, freezes, migrations, acquisitions, or provider renewals can alter the assessment story before completion?

THE CLUSTER OF WACK

FIND / MAP / EXPLAIN / REDUCE / PROVE

ESCAPE THE WACK

01 / FIND

Start with the real acceptance date and work backward. Inventory remaining assessment claims, recurring occurrences, evidence refreshes, provider dependencies, remediation, report reviews, approvers, and the availability constraints attached to each one.

02 / MAP

Build a single readiness countdown with last responsible dates, accountable owners, delegates, inputs, outputs, dependencies, and reopen triggers. Join every item to the claim or control occurrence it advances.

03 / EXPLAIN

Separate standard-driven timeframes, entity-defined operating dates, assessment milestones, and stakeholder preferences. Record who owns each date and what happens if it is missed instead of letting urgency blur the authority boundary.

04 / REDUCE

Close stale evidence requests, split oversized claims, resolve easy scope and provider questions early, eliminate duplicate approval loops, and reserve scarce specialist time for the decisions only they can make.

05 / PROVE

Run a readiness review before the slowdown. Demonstrate that each material claim has a current owner, review path, evidence contract, exception path, remaining occurrence schedule, delegated coverage, and a realistic completion window.

THE FIELD LAW

THE LINE WORTH REMEMBERING

A HOLIDAY CALENDAR IS NOT AN EXTENSION OF A CONTROL WINDOW.

Open the Year-End PCI Readiness Countdown ninety days before your real completion target. If the plan assumes that every owner, provider, approver, and assessor will rescue the same final week, the house is not in order yet.

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-0015 / FAQ 1566: Use of evidence obtained outside the current assessment / PCI Security Standards Council / [Open source](#)
- WACK-SOURCE-0031 / FAQ 1572: Periodic controls cannot be completed retroactively / PCI Security Standards Council / [Open source](#)
- WACK-SOURCE-0032 / FAQ 1485: Meaning of an initial PCI DSS assessment / PCI Security Standards Council / [Open source](#)
- WACK-SOURCE-0033 / FAQ 1087: Quarterly vulnerability scanning timeframes / PCI Security Standards Council / [Open source](#)
- WACK-SOURCE-0034 / Best Practices for Maintaining PCI DSS Compliance / 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

ce6efb05db10b7d1ef88de19e6aec206483af94bbd08a12967d5f870a35d8a6a. 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.