

From Checkbox to Continuous: The Future of PCI DSS Assessments

Fieldguide

Jason Ksar

Senior Sales Manager, Enterprise

Fieldguide

20 YEARS OF SECURING PAYMENT DATA

PCI Security Standards Council



A SHOW OF HANDS

How long did it last?

Your last assessment, after the ROC was submitted.



THE ARGUMENT

Readiness is a state, not an event.



POINT ONE – THE ANNUAL MODEL IS RUNNING OUT OF ROAD

Three shifts in PCI DSS 4.x

01

The customized approach

Organizations meet the objective their own way – and the assessor designs the testing that proves it.

02

Targeted risk analyses

Frequency is no longer handed down by the document. It has to be reasoned, documented, and defended.

03

Future-dated requirements

Mandatory since March 2025, with one shared theme: ongoing verification, not annual reconstruction.

POINT ONE

More judgment per assessment.

Same calendar.



POINT TWO – WHAT CONTINUOUS ACTUALLY LOOKS LIKE

Evidence: from artifacts to pipelines

ARTIFACT

A screenshot proves a moment.

Manufactured for the assessment. Steal the moment it captured.

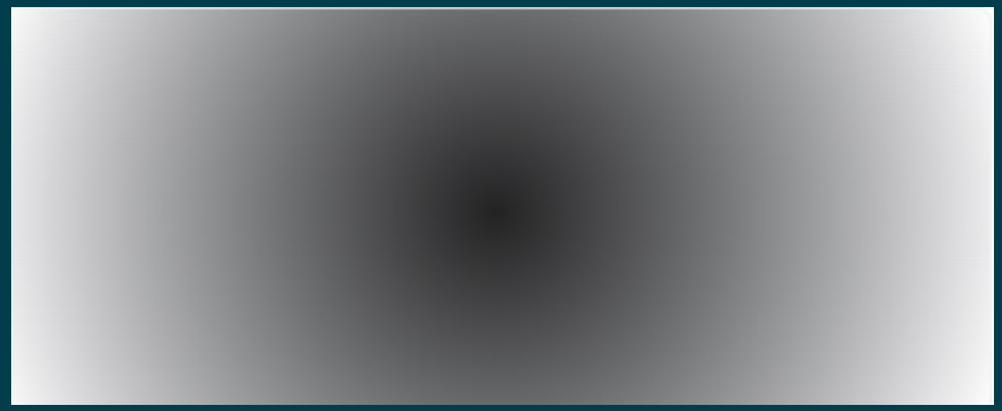
PIPELINE

A pipeline proves a period.

Generated continuously as a byproduct of operations – and it carries provenance.

POINT TWO – WHAT CONTINUOUS ACTUALLY LOOKS LIKE

Testing: sample less, watch more



Annual sampling

Twenty-five items, reasoned statistically. It made sense when looking was expensive.



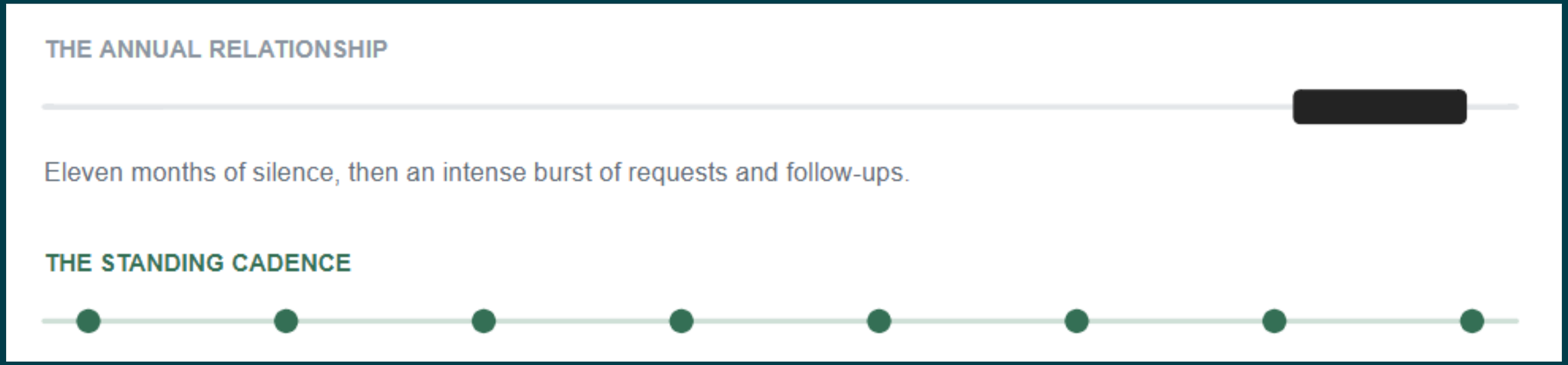
Population monitoring

Observe everything; investigate what deviates. Human attention goes to the exceptions.

Monitoring is not assessment. A flag is where the assessor’s work begins, not where it ends.

POINT TWO – WHAT CONTINUOUS ACTUALLY LOOKS LIKE

Collaboration: from fieldwork season to standing cadence



Issues surface the month they occur – when they are cheap to fix, not expensive or embarrassing.

POINT THREE – ROLES ARE CHANGING

What stays human

Agent executed

- Evidence gathering and completeness checks
- Configurations compared against baselines
- Routine portions of documentation, drafted
- Change detection --- noticing, tirelessly

Practitioner led

- Scoping judgement
- Whether a customized approach meets the objective
- Whether a TRA or compensating control holds up
- The conversation about what a finding means

Practitioner led, agent executed. The judgment — and the signature — stay with you.

POINT THREE

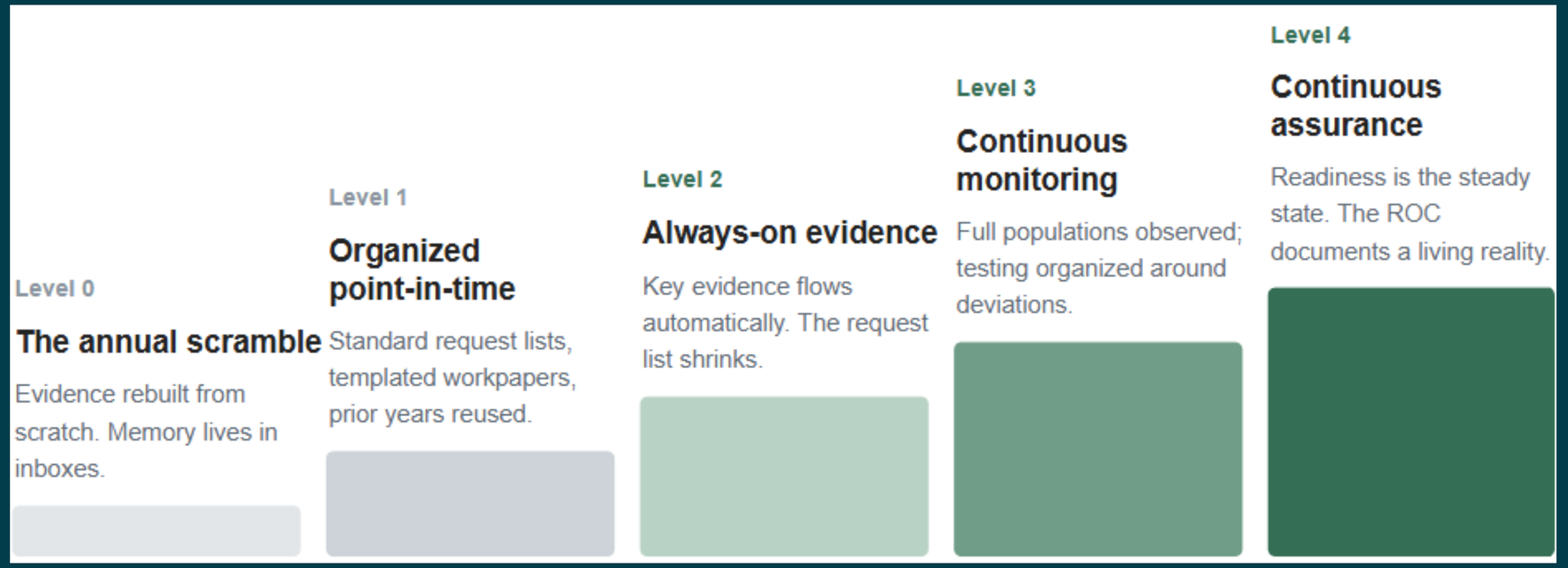
No tool signs a ROC.

Your signature is the product. Everything else is in service of it.



THE FRAMEWORK

The Continuous Readiness Curve



Each level pays for itself – and you can’t skip levels. The curve is climbed in order.

THE PLAYBOOK

Five moves for the next two quarters

1	**Run an evidence audit**	Mark every item on last year's request list that a system could have produced. That's your level 2 backlog.
2	**Shift the request list left**	Turn your top ten recurring requests into standing pipelines with named owners. Start with access reviews.
3	**Run one control family continuously**	One family, one quarter. Prove the model on a narrow slice before you generalize.
4	**Make TRAs living documents**	Owner, review date, trigger conditions for revisiting — not an annual document in continuous clothing.
5	**Change the cadence before the tooling**	A quarterly thirty-minute scope conversation per client. Highest return on this list; zero technology.

THE QUESTION THAT MATTERS

“Were you secure on the day you looked?”

“Are you secure today?”

Fieldguide

Thank you

Jason Ksar

From Checkbox to Continuous – Find me this week at the Fieldguide **Booth 39.**