PCI ASSESSMENTS CENTER

Haumaru Whanau · PCI QSA Company

pciassessments.com

PCI Assessments Center

The PCI DSS self-assessment, implementation and training platform, built by a QSA company.

Self-assessment | Implementation programme | Governance toolkit | Courses & certificates | Evidence intake

K

Kai — the AI PCI ISA, built into every module

Retrieval-grounded guidance on the published standard, answer review, evidence mapping and remediation planning — signed in, server-side, and always approved by a person.

10
SAQ types supported end to end

350
PCI DSS controls in the full workspace

184
Free lessons across 9 course tracks

Beta v1.62.1 · Aurora · Issued 2026-08-25

Free to download · no registration required

THE PROBLEM

Why SAQ programmes stall

Most organisations do not fail PCI DSS because the controls are impossible. They fail because the programme lives in spreadsheets, the evidence is scattered, and every annual cycle starts from a blank page.

The wrong SAQ is chosen

Eligibility criteria are skimmed rather than confirmed clause by clause, so a short-form SAQ is completed when the environment actually requires SAQ D — and the gap surfaces during an acquirer review.

Evidence is scattered

Screenshots sit in email, policies in a shared drive, scan reports with a vendor. Nobody can say which requirement a given artefact actually satisfies.

Reporting is rebuilt every cycle

The report is assembled by hand from whatever is available in the last week, rather than generated from the same record the team has been maintaining all year.

Remediation slips quietly

Findings are recorded in a document nobody revisits. Ownership, target dates and progress are invisible until the deadline arrives.

The platform answer

One record from scoping to attestation: the SAQ decision, the answers, the evidence, the programme tasks and the report all read from the same model — so the report is a view of the work, not a separate exercise.

OVERVIEW

Five pillars, one platform

PCI Assessments Center is operated by Haumaru Whanau, a PCI QSA company. Every module is built around how assessments are actually reviewed — not around a generic compliance checklist.

01

Assessments

Guided SAQ selection across all ten SAQ types, requirement-by-requirement workspace, evidence library and an SAQ-styled report you can hand to an acquirer.

02

Implementation programme

Eleven phases from environment profiling to attestation, with tasks, owners, findings and coverage tracked against the standard.

03

Governance toolkit

A QSA-authored artefact catalogue mapped to PCI DSS requirements, personalised to your organisation and released under version control.

04

Courses and exams

Nine tracks, 184 lessons and practice exams for PCIP and QSA candidates. Free, with free certificates.

05

Kai — the AI PCI ISA

An assistant grounded in the published standard that plans remediation, reviews answers and drafts guidance — always for a human to approve.

06

Free to start

A single-seat workspace costs nothing. Team and Premium add seats when more of the organisation needs to work in the same record.

ARCHITECTURE

One source of truth

The SAQ decision, the assessment answers, the evidence, the programme tasks and the report are four views of one record. Nothing is re-keyed between them.

1

Scope becomes the assessment

Environment profiling answers determine the SAQ type and pre-fill applicability, so the questionnaire opens on the requirements that actually apply to you.

2

Answers carry their evidence

Each requirement holds its own evidence items with owner, review state and history. Nothing is attached to a folder and forgotten.

3

Gaps become programme work

A non-compliant answer raises a finding with a phase, an owner and a target date inside the implementation programme.

4

The report is generated, not assembled

The SAQ-styled report renders from the live record at the moment you ask for it, with the identity of the person who generated it on every page.

No re-keying, no drift

Because every module reads the same rows, a control marked in place in September is still in place — with its evidence — when the report is produced in March.

ARTIFICIAL INTELLIGENCE

Kai, the AI PCI ISA

Kai is an Internal Security Assessor in software: a retrieval-grounded assistant that reads the published PCI DSS material and your own workspace, and works inside every module rather than in a separate chat box.

Plan the programme

Turns a scope profile into a sequenced remediation plan with phases, owners and dependencies.

Read the standard

Answers requirement questions with citations to the published requirement and testing procedure.

Map evidence

Proposes which requirement an artefact supports and flags where a baseline item is still missing.

Review answers

Re-reads a completed section and highlights answers the supporting evidence does not carry.

Draft governance

Produces first-draft policy and procedure text, and reviews existing documents for PCI applicability.

Raise findings

Converts a gap into a tracked finding with a proposed remediation and target date.

Workstream: long work keeps running

A review of a whole assessment or document set is queued as a job rather than held in the page. Close the tab and it carries on; each job reports its steps, and duplicate work on the same target is refused.

ARTIFICIAL INTELLIGENCE

How Kai is kept trustworthy

An assistant that guesses about PCI DSS is worse than no assistant at all. Kai is constrained on every side — what it reads, what it can see, what it can change, and who may talk to it.

- Grounded, not generative: answers are retrieved from the published standard and cited, with live lookups limited to PCI SSC sources.
- Signed-in only: Kai is never exposed to anonymous visitors, and every model call runs server-side.
- Opaque handles: workspace record identifiers are never placed in a prompt, so the model works on content, not on your data model.
- Impact previews: a suggested change is shown as a difference against the current text and applied only when a person accepts it.
- No training on tenant data: your assessment content, evidence and documents are never used to train a model.
- Prompt-attack detection: manipulation attempts are detected and refused — a first attempt warns, a second suspends AI access.

Kai advises, the assessor decides

Kai never marks a requirement in place, never accepts evidence and never signs anything. It shortens the distance between the standard and your record; the judgement stays with your team and, where required, a QSA.

ASSURANCE

Assurance, not autocomplete

An assessment platform is only as good as what it refuses to take on trust. Every decision that matters is made on the server, against the record — never in the browser.

- Server-side authority: validation, authorisation and scoring run server-side; the browser is a view.
- Cited evidence: AI output that touches a requirement carries the source it was drawn from.
- Append-only audit trail: every server call, page view and API request is recorded and cannot be edited or deleted.
- No training on tenant data: your assessment content is never used to train a model.
- Watermarked reporting: generated reports carry the identity of the account that produced them.
- Tenant isolation: workspace data is separated at the database layer, not by application code alone.

Built by assessors

Haumaru Whanau is a PCI QSA company. The platform encodes the way a QSA actually reviews an assessment, which is why it will route you to SAQ D — or to a QSA engagement — when the short form does not fit.

MODULE ONE

Assessments and the SAQ selector

Choosing the wrong SAQ invalidates everything downstream. The selector walks the official PCI SSC decision flow and confirms every eligibility clause before it recommends a short form.

10
SAQ types supported

350
Controls in the full PCI DSS workspace

0-100
Confidence score per selector run

- Merchant and service-provider triage first: level, acquirer mandates, DESV and breach escalation.
- Every eligibility clause is confirmed; any gap routes to SAQ D or to a QSA engagement.
- "I'm not sure" answers route conservatively rather than optimistically.
- The decision trace is replayed on the server and stored, so the recommendation can be evidenced later.
- An accuracy attestation is stamped server-side against the run.
- The full questionnaire workspace covers every requirement with evidence, notes and review state.
- Beyond the SAQs, the full PCI DSS workspace tracks all 350 controls of the standard for organisations assessing in depth.

SAQ-styled reporting

The generated report follows the structure of the official SAQ document — parts 1, 2 and 4 — populated from your record, so reviewers read something they already recognise.

MODULE TWO

The implementation programme

For organisations that are not yet ready to answer the questionnaire, the programme turns PCI DSS into a project with phases, owners and dates.

Phase	What happens
0 — Understand	Cardholder data environment profiling: flows, channels, systems, third parties.
1-2 — Scope & gap	Scope definition and a gap analysis against the applicable requirements.
3-5 — Design & build	Control design, remediation work and configuration standards.
6-8 — Evidence	Evidence collection, testing, scanning and penetration testing.
9-10 — Assess	Internal review, assessment completion and attestation.

- The environment profile drives the whole programme — the wizard never asks the same question twice.
- Findings are raised automatically where the profile and answers disagree.
- Programme creation is transactional: it either completes or rolls back cleanly.
- A central tasks workspace shows everything assigned across phases.

MODULE THREE

The governance toolkit

PCI DSS asks for documented policy and procedure across nearly every requirement. The toolkit ships a QSA-authored catalogue rather than leaving you to start from a blank document.

Mapped catalogue

An artefact set mapped to the PCI DSS requirements each document is expected to satisfy.

Personalisation tokens

Organisation, scope and role tokens are resolved to your details, so a released document reads as yours.

Version control

Every release is versioned, with the previous version retained and comparable.

Release and revocation

Packs are released to workspaces and can be revoked; revocation removes access immediately at the data layer, not just in the interface.

Already run ISO 27001?

Existing governance is reused rather than duplicated. The toolkit shows which PCI DSS requirements your current documents already carry and which need PCI-specific language added.

MODULE FOUR

Evidence, from inbox to requirement

Evidence is where most assessments lose time. The platform gives every workspace one library, an email address that files attachments for you, and the ability to reuse a single artefact wherever it applies.

One workspace library

Every artefact sits in a single library with its owner, review state, history and the requirements it supports — not in a folder tree nobody maintains.

Email it in

Each workspace has its own intake address. Forward a scan report, a signed policy or a screenshot and the attachment arrives in the evidence inbox ready to file.

Notified either way

The workspace is notified when an intake is accepted and when one is refused, so nothing sits unnoticed and nothing fails silently.

Reuse, don't re-upload

One artefact can be attached to many controls and many assessments in the same workspace. The file is stored once and every attachment points at it.

- Evidence attached during the year is the evidence the report reads from — there is no separate collection exercise.
- Baselines show which artefacts a requirement expects and which are still missing.
- Removing one attachment never breaks the others; the stored file is retained while any reference remains.
- Files are held in private storage and streamed through the platform rather than shared as links.

MODULE FIVE

Courses, exams and certificates

Requirement 12.6 asks for security awareness. Preparing for PCIP or QSA asks for a great deal more. Both are free on this platform.

9	184	Free
Course tracks	Lessons	Certificates, no watermark

- Tracks span PCI DSS foundations, network security, security testing, and programme management.
- Practice exams for PCIP and QSA candidates, drawn from a maintained question bank with randomised options.
- Every course can be downloaded as a handbook PDF, typeset by the platform and personalised to the learner.
- Progress is tracked per learner and visible to the workspace owner.
- Completion certificates are issued free of charge, carry no watermark, and can be verified online by anyone holding the code.

Example only. Completion and achievement certificates are issued in exactly this form — free of charge, without a watermark, and verifiable at ${PUBLIC_SITE_URL}/verify.

ENGINEERING

How the platform is built

The platform holds assessment detail about payment environments, so it is engineered to the same standard it helps you demonstrate.

Tenant isolation

Row-level security separates workspaces in the database; no privileged table is reachable with a browser token.

Multi-factor authentication

TOTP MFA is available to every account and enforced server-side for sensitive operations.

Abuse controls

Protective lockouts, rate limits and strike-based suspension operate across the whole portal.

Outbound email budget

Every outbound message passes a daily ceiling per platform, account, recipient and source address.

Append-only audit trail

The ledger cannot be updated, deleted or truncated by any role, including the platform itself.

Private storage

Evidence and documents live in private storage, streamed through the platform — never a public link.

Governed file handling

Uploads are inspected and quota-controlled server-side, and every file action is written to an access ledger.

Workspace notifications

Members are alerted in the portal when documents are released, evidence arrives or an action needs attention.

Responsible disclosure

The platform runs a recognition-based disclosure programme. Findings from security researchers are acknowledged publicly and fixed in the open changelog.

GETTING STARTED

Four steps to your first report

1

Create a free workspace

Any real email address works. Verification and, if you want it, TOTP MFA take about a minute.

2

Run the SAQ selector

Answer the triage and eligibility questions to get a scored, evidenced SAQ recommendation.

3

Work the questionnaire

Answer requirement by requirement, attaching evidence as you go and raising findings where you cannot.

4

Generate the report

Produce the SAQ-styled report from the live record whenever you need it.

Plan	Seats	Best for
Free	1	An individual completing a single SAQ.
Team	5	A small compliance team sharing one record.
Premium	20	Larger programmes with separate owners per phase.

Talk to a QSA

When the assessment needs a signed attestation, or the selector routes you away from a short form, Haumaru Whanau can take the engagement. Start at ${PUBLIC_SITE_URL}/contact.