Cartelta

IMPLEMENTATION WORKBOOK • VERSION 3.0

Payment page control for PCI DSS 6.4.3 and 11.6.1

A practical workbook for scope decisions, script governance, change and tamper detection, response testing, ownership, and reviewable evidence.

PCI DSS v4.0.1 | 6.4.3 | 11.6.1

Define scope

Map real payment journeys, browser states, providers, and decision owners.

Operate control

Govern scripts, approve baselines, detect meaningful change, and respond.

Prove operation

Retain source records that an independent reviewer can retrieve and trace.

DOCUMENT CONTROL

Review basis: PCI DSS v4.0.1 and PCI SSC e-commerce guidance

Updated: 27 July 2026

Language: English

01

Scope and applicability decision

Record the architecture before selecting the control or validation path.

Complete this page for each materially different payment journey. The same domain can contain redirect, embedded, and merchant-originated patterns with different responsibilities.

01

Map the journey

URLs, locales, mobile states, consent states, tag managers, CDN behavior, and provider boundaries.

02

Name the decision owner

Record the merchant, provider, assessor, acquirer, or payment brand responsible for each conclusion.

03

Attach source evidence

Architecture, provider instructions, configuration, observed page state, and the signed scope decision.

Architecture decision record

Payment pattern	Decision to document	Minimum supporting record
Server-side redirect	Determine whether scripts can influence the redirect and have the QSA document any non-applicability conclusion for a ROC.	HTTP behavior, source page, provider destination, change owner, QSA or compliance-program decision.
Embedded TPSP form / iframe	For SAQ A, record how the site meets the script-attack eligibility criterion: protection techniques or TPSP confirmation.	Provider confirmation and conditions, implementation settings, merchant-page controls, tested page states.
Merchant-originated form / direct post	Confirm the applicable SAQ or ROC path and the full merchant responsibility for browser-delivered content.	Architecture, payment-page inventory, control design, assessment decision, service-provider dependencies.

Keep controls separate FAQ 1604 states that SAQ A external ASV scanning applies to merchant webpages using redirects or embedded iframes. ASV scanning does not replace script governance or browser-side change detection.

Journey / system _____

Production URL or pattern _____

Architecture owner _____

Validation method _____

Compliance-program owner _____

Decision / review date _____

02

Script governance for Requirement 6.4.3

Connect what the browser executes to owner, authorization, necessity, and integrity.

Build the governed register from observed payment-page states, not from a repository list alone. Include first-party bundles, third-party SDKs, tag-manager rules, widgets, and dynamic loaders.

ID	Control outcome	Verification question	Expected evidence
643-01	Complete observed inventory	Were all scripts and loaders observed across relevant journeys, states, and release variants?	Browser export, URL/state map, source, first and last seen, loader relationship.
643-02	Named ownership	Does each script have accountable business and technical owners?	Governed register, service record, owner acceptance, escalation path.
643-03	Explicit authorization	Can the team trace every active script to an approved decision?	Change ticket, approval date, approver, environment, exception reference.
643-04	Written necessity	Is the business or technical reason specific enough to support removal decisions?	Purpose, affected journey, dependency, data boundary, review date.
643-05	Integrity approach	Is the selected integrity or authenticity method documented and operating for this script type?	SRI or signature record, controlled delivery, CSP support, monitoring rule, test result.
643-06	Lifecycle reconciliation	Is the observed population reconciled after releases and material third-party changes?	Before/after export, release reference, additions/removals, decision and reviewer.

Minimum script-register fields

Script ID and observed URL _____

Journey / page state _____

First or third party _____

Business and technical owner _____

Purpose / necessity _____

Authorization reference _____

Integrity method _____

First and last seen _____

Review / removal date _____

Implementation note SRI, CSP, signatures, controlled delivery, and monitoring can support different parts of the control. Do not label one technique as automatic compliance; document why it is suitable for the actual script and delivery model.

03

Change and tamper detection for Requirement 11.6.1

Approve expected states, detect meaningful deviations, and preserve the response.

Monitoring should evaluate the payment page and security-impacting HTTP headers as received by the consumer browser. Define how dynamic values are normalized without hiding security-relevant change.

ID	Control outcome	Verification question	Expected evidence
1161-01	Approved baseline	Are relevant page states, content, scripts, resource origins, and headers versioned and approved?	Baseline ID, snapshot, release, owner, approval, effective date.
1161-02	Meaningful comparison	Can the mechanism distinguish expected dynamic content from unexplained change?	Comparison rules, normalization, exclusions, tuning decision, negative test.
1161-03	Required cadence	Does execution meet at least once every seven days or the applicable targeted-risk-analysis frequency?	Schedule, execution history, TRA where used, failures, retries, gap decision.
1161-04	Actionable alert	Does an unauthorized addition, deletion, or modification create a reviewable event?	Diff, timestamp, affected page/header, source, severity, recipient.
1161-05	Response and closure	Can personnel assign, investigate, contain or approve, retest, and close the event?	Alert, case timeline, decision, action, closure, linked incident or change.
1161-06	Control availability	Are missed runs, collection failures, and blind spots detected and owned?	Health signal, failure alert, retry history, outage ticket, coverage review.

Monitoring surface

Surface	Examples to evaluate	Typical context to retain
Page content	DOM-relevant content, forms, iframes, resource references	Journey, state, snapshot, normalized and raw comparison references
Scripts	Additions, deletions, source changes, loader behavior	Script ID, origin, owner, authorization, integrity method
HTTP headers	CSP and other headers that affect page or script security	Header name/value, response path, baseline, observed difference

Frequency decision

Where a targeted risk analysis is used to define a periodic frequency, retain the current analysis, approval, review date, and evidence that the configured schedule matches it. Confirm applicability with the assessor.

04

Operating model and definition of done

Treat the control as a repeatable workflow, not a configured dashboard.

Start with one real production-equivalent journey. Expand only after the team can explain the observed state, process a controlled deviation, and retrieve the complete evidence chain.

01

Scope

Map journeys, states, dependencies, owners, and validation assumptions.

02

Observe

Capture scripts, resource origins, page content, and relevant headers.

03

Authorize

Link owner, necessity, approval, integrity method, and review date.

04

Baseline

Approve expected states and narrowly document normalization rules.

05

Detect and respond

Route deviations, investigate context, decide, act, retest, and close.

06

Retain and review

Preserve source records and independently test retrieval and control health.

Mark a journey ready only when all conditions are true

Scope	Real variants and responsible parties are documented; applicability is not assumed.
Governance	Observed scripts reconcile to approved owner, purpose, authorization, and integrity records.
Monitoring	Expected states are approved; meaningful change and control failure create events.
Response	Positive, negative, routing, failure, and closure tests have actual results.
Evidence	An independent reviewer can retrieve design and operating records without oral reconstruction.
Open gaps	Every exception or failed test remains visible with owner, due date, and escalation.

Pilot exit criterion

A green dashboard is not the exit criterion. The pilot is complete when a reviewer can trace one expected release, one unexplained deviation, one monitoring failure, and the related decisions from source to closure.

05

Control and evidence matrix

Use one row per payment journey; link status to a source record.

Copy these rows into the editable CSV control worksheet when owners, due dates, or exceptions need active management. A status without a source record is a planning statement, not evidence.

ID	Control outcome	Verification focus	Primary owner	Result / reference
SCOPE-01	Journey scope	All variants and browser-impacting pages are mapped.	PCI owner / architecture	Result: Ref:
VAL-01	Validation path	SAQ or ROC path and applicability decision are documented.	PCI owner / assessor	Result: Ref:
643-01	Script inventory	Observed scripts match the governed register.	AppSec / application	Result: Ref:
643-02	Authorization	Every script has approval and written necessity.	Business / technical owner	Result: Ref:
643-03	Integrity	A suitable integrity or authenticity method operates.	Engineering / AppSec	Result: Ref:
1161-01	Baseline	Expected page and header states are approved.	Application owner	Result: Ref:
1161-02	Detection	Meaningful change creates a reviewable event.	Security operations	Result: Ref:
1161-03	Cadence and gaps	Schedule, failures, retries, and risk decision are evidenced.	Control / platform owner	Result: Ref:
1161-04	Response	Events are assigned, decided, acted on, and closed.	SOC / incident response	Result: Ref:
EVID-01	Evidence retrieval	A sample can be reproduced without rebuilding history.	Internal audit / control owner	Result: Ref:
GOV-01	Governance	RACI, retention, exceptions, and review are accepted.	Control owner	Result: Ref:

Journey / scope ID _____

Review period _____

Worksheet owner _____

Independent reviewer _____

Open exceptions _____

Next review date _____

06

Acceptance and operating-effectiveness tests

Preserve expected and actual results; do not convert failed tests into generic acceptance.

Run the suite against a controlled environment that faithfully represents production behavior. Use synthetic values and avoid collecting cardholder data in the test evidence.

Test	Scenario	Expected result	Evidence to retain
T-01	Approved release changes a governed script.	Change is linked to release; baseline updates through approval.	Before/after, ticket, approver, baseline version.
T-02	Unexpected script or loader is introduced.	Event identifies page, source, difference, and route.	Test input, alert, timestamps, owner, triage.
T-03	Security-impacting header is modified or removed.	Difference is detected with raw and normalized context.	Response headers, baseline, diff, decision.
T-04	Legitimate dynamic value changes.	Noise is normalized without suppressing security-relevant change.	Rule, sample, rationale, reviewer, negative test.
T-05	Observation or scheduled run fails.	Health event, retry, ownership, and gap decision are visible.	Failure event, retry history, outage or gap ticket.
T-06	High-severity event is routed.	Named on-call path receives and acknowledges within target.	Notification, acknowledgement, escalation timeline.
T-07	Independent reviewer requests a sample.	Complete chain is retrieved by journey, date, and requirement.	Query, export, source references, access record.

Test environment / version _____

Test window _____

Executor _____

Independent reviewer _____

Failed tests / tickets _____

Retest approval _____

Data boundary Evidence should explain the control without storing PAN, sensitive authentication data, secrets, session tokens, or unnecessary customer data. Document redaction and access controls.

07

Ownership, RACI, and response workflow

Separate accountability, operation, review, and assessment.

Replace role names with actual teams and on-call paths. QSA or internal audit participation does not transfer ownership of the control from the entity.

Activity	PCI owner	App / Eng	AppSec	SOC / IR	Audit / QSA
Confirm scope and validation path	A	C	C	I	C
Maintain script register	C	R	A	I	I
Approve integrity method	I	R	A	C	I
Approve baseline / release	I	A/R	C	I	I
Triage and contain event	I	C	C	A/R	I
Retain evidence / exceptions	A	R	R	R	C
Independently test and sample	C	I	C	C	A/R

A = accountable, R = responsible, C = consulted, I = informed. One activity can have several responsible roles, but accountability must be explicit.

Minimum event timeline

01

Receive

Record event time, affected journey, source, severity, and notification path.

02

Triage

Compare release context, baseline, inventory, owner, and indicators of compromise.

03

Decide

Authorize, contain, remove, escalate, or open an incident with named approver.

04

Recover

Restore expected state, validate page behavior, and address monitoring gaps.

05

Close

Retest, preserve the complete chain, link follow-up, and record closure approval.

06

Learn

Update inventory, baseline, runbook, tuning, training, and risk assumptions.

Retention principle Define retention from the assessment period, applicable PCI requirements, internal policy, legal needs, and assessor expectations. Do not assume one universal period for every artifact.

08

Professional evidence package

Make design and operation independently traceable.

Use stable identifiers across architecture, script records, change events, tickets, and exports. The reviewer should move from requirement to control, event, owner, action, and source record without relying on screenshots alone.

Package section	Minimum context	Representative artifacts
01 Scope and architecture	Journey, states, provider boundary, owner, validation path.	Diagram, URL map, data-flow record, scope decision.
02 Script governance	Observed source, purpose, owner, approval, integrity, lifecycle.	Register export, tickets, exceptions, removal record.
03 Monitoring design	Baseline, comparison scope, normalization, cadence, routing.	Configuration, baseline manifest, TRA if used, runbook.
04 Operating samples	Normal run, approved release, unexplained change, failed run.	Execution history, diffs, alerts, tickets, decisions.
05 Response and incidents	Severity, assignment, investigation, action, recovery, closure.	Case timeline, incident link, retest, approval.
06 Governance	RACI, access, retention, exceptions, periodic review.	Procedure, access review, exception register, review minutes.
07 Independent retrieval	Selection method, source links, gaps, reviewer conclusion.	Evidence index, retrieval log, follow-up tickets.

Review session agenda

20m

Architecture

Walk one real journey and explain scope, browser influence, and the validation decision.

25m

Control operation

Trace one approved release, one unexpected change, and one failed observation.

15m

Evidence retrieval

Let the reviewer select a date, journey, script, and event without prior staging.

Quality gate

Screenshots can support context but should not be the only source record. Prefer exports, immutable event IDs, configuration versions, tickets, and access-controlled originals that preserve dates and ownership.

09

Official sources and document limits

Use current PCI SSC publications as the authority.

The links below were reviewed when this workbook was issued. Check the PCI SSC Document Library and your compliance-program owner for later revisions, regional instructions, and the validation method applicable to your entity.

Primary PCI SSC references

01	**PCI SSC Document Library - PCI DSS v4.0.1 and current supporting documents**	www.pcisecuritystandards.org/document_library/
02	**PCI SSC - Payment Page Security and Preventing E-Skimming**	blog.pcisecuritystandards.org/new-information-supplement-payment-page-security-and-preventing-e-skimming
03	**PCI SSC - 2025 updates for merchants validating to SAQ A**	blog.pcisecuritystandards.org/important-updates-announced-for-merchants-validating-to-self-assessment-questionnaire-a
04	**PCI SSC FAQ 1588 - SAQ A eligibility criteria for scripts**	www.pcisecuritystandards.org/faqs/1588/
05	**PCI SSC FAQ 1331 - SAQ criteria and applicability in a ROC**	www.pcisecuritystandards.org/faqs/1331/
06	**PCI SSC FAQ 1604 - SAQ A ASV scans for redirects and embedded iframes**	www.pcisecuritystandards.org/faqs/1604/

What this workbook does not do

01	It does not reproduce or replace PCI DSS, an SAQ, a ROC template, or PCI SSC guidance.
02	It does not decide applicability, scope, sampling, compensating controls, customized approach, or assessment sufficiency.
03	It does not certify Cartelta, another product, or a specific implementation as compliant.
04	It does not replace secure architecture, vulnerability management, ASV scanning, incident response, or provider governance.
05	It should be tailored, version-controlled, approved, and retained with the source evidence for the actual environment.

Continue the working set

Use the localized HTML guide and editable control worksheet at cartelta.com/resources/pci-dss-6-4-3-11-6-1-checklist. Cartelta JSIR is designed to support payment-page script inventory, change monitoring, and reviewable evidence workflows.

Document owner _____

Environment / journey _____

Approver _____

Next review date _____