PCI Security Standards Council®

2025 NORTH AMERICA COMMUNITY MEETING

2025 NORTH AMERICA COMMUNITY MEETING

6.4.3 & 11.6.1: Now What?

PCI Security Standards Council

Jeff Man

Qualified Security Assessor
Sr. Information Security Consultant

obsglobal

Jeff Zitomer

Sr. Director of Product Management,
Client-Side Defense & PCI DSS

HUMAN

PCI Security Standards Council

Agenda

After a quick recap on 6.4.3 and 11.6.1, we will:

- Clarify applicability, scope, and SAQ eligibility across payment page types
- Understand the challenges of operationalizing controls in large orgs
- Learn actionable, role-specific next steps to sustain security and demonstrate compliance

6.4.3 & 11.6.1 - A Quick Recap

- What
- Why
- When

What are the New Browser Script Requirements?

6.4.3
Script Management

- Maintain inventory with written justification
- Confirm scripts are authorized
- Assure scripts' integrity

11.6.1
Change and Tamper Detection

- Alert to unauthorized modification to security-impacting HTTP headers and the script contents of payment pages, as received by the consumer browser

*Reference full requirements in Payment Card Industry Data Security Standard: Requirements and Testing Procedures, v4.0.1

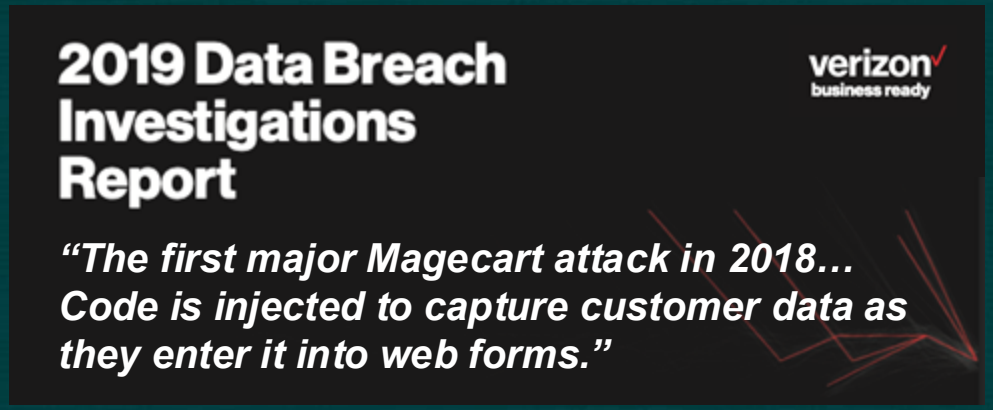
PCI Security Standards Council

Why Secure Scripts?

A lucrative, vulnerable, and widely exploited attack surface

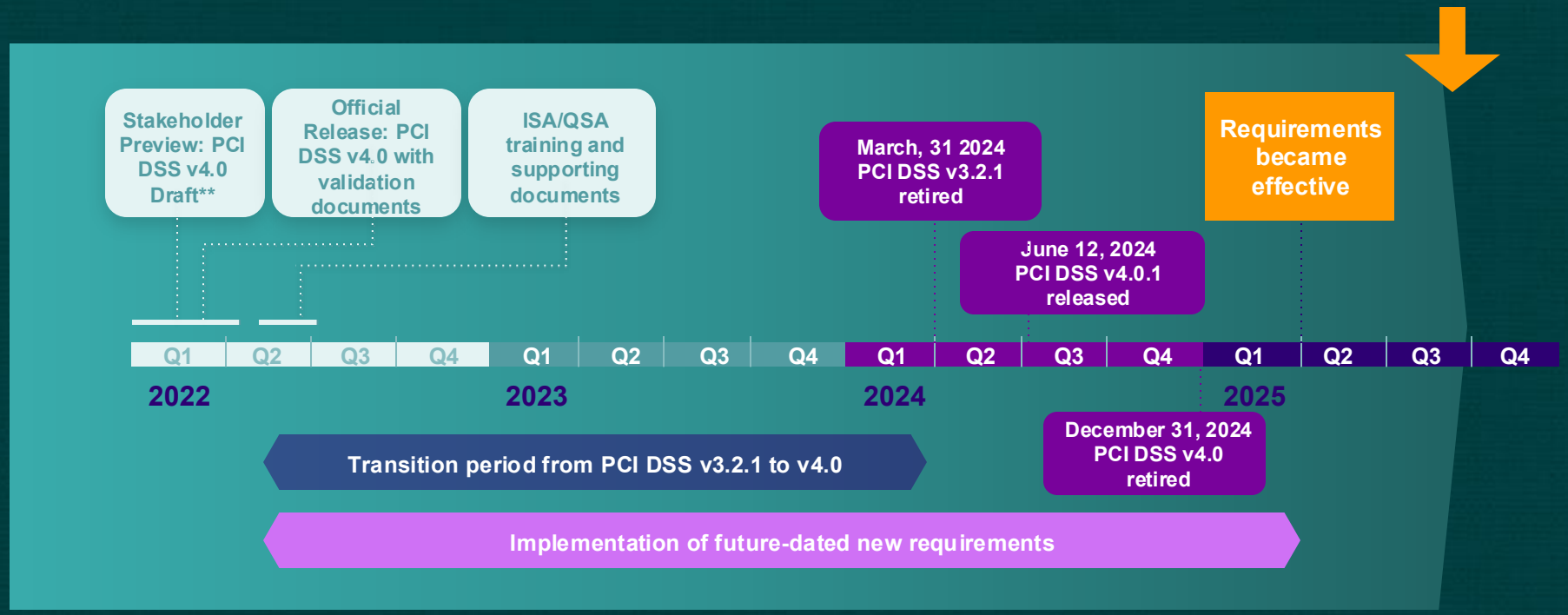
Scripts:

- Are plentiful
- Are business-critical
- Bypass change management and security controls
- Access cardholder data freely



PCI Security Standards Council

Post-Deadline: Let's Clarify and Operationalize



PCI Security Standards Council

Payment Page and Application Architecture Inform Applicability, Scope and SAQ-Eligibility

Payment page scenarios

- Merchant hosted
- Embedded payment forms (iframe)
- Redirection
- Fully outsourced

Application architectures

- Multi-page app
- Single-page app

PCI Security Standards Council

New SAQ A Eligibility Requirements

6.4.3 and 11.6.1 are gone from the applicable requirements, but…

The bigger question for merchants accustomed to completing SAQ A is not applicability - it's who is doing the required actions to meet eligibility?

erchant Eligibility Criteria for Self-Assessment Questionnaire A

Self-Assessment Questionnaire (SAQ) A includes only those PCI DSS requirements applicable to merchants with account data functions completely outsourced to PCI DSS validated and compliant third parties, where the merchant retains only paper reports or receipts with account data.

SAQ A merchants may be either e-commerce or mail/telephone-order merchants (card-not-present) and do not store, process, or transmit any account data in electronic format on their systems or premises.

This SAQ is not applicable to face-to-face channels.

This SAQ is not applicable to service providers.

SAQ A merchants confirm that, for this payment channel:

- The merchant accepts only card-not-present (e-commerce or mail/telephone-order) transactions;
- All processing of account data is entirely outsourced to PCI DSS compliant third-party service provider (TPSP)/payment processor;
- The merchant does not electronically store, process, or transmit any account data on merchant systems or premises, but relies entirely on a TPSP(s) to handle all these functions;
- The merchant has confirmed that TPSP(s) are PCI DSS compliant for the services being used by the merchant; and
- Any account data the merchant might retain is on paper (for example, printed reports or receipts), and these documents are not received electronically.

Additionally, for e-commerce channels:

- All elements of the payment page(s)/form(s) delivered to the customer's browser originate only and directly from a PCI DSS compliant TPSP/payment processor.
- The merchant has confirmed that their site is not susceptible to attacks from scripts that could affect t merchant's e-commerce system(s).

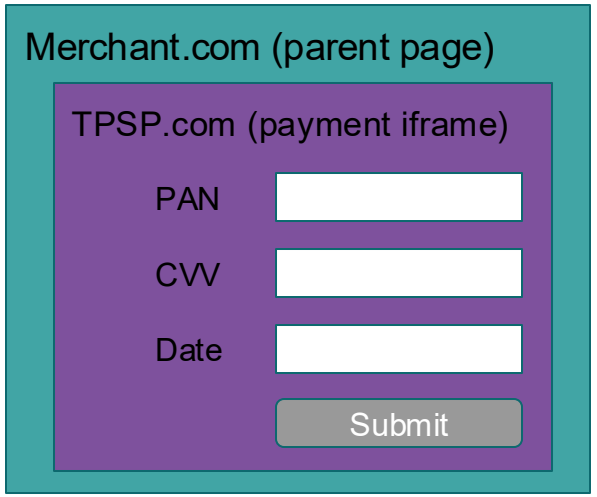
PCI Security Standards Council

Merchant Hosted

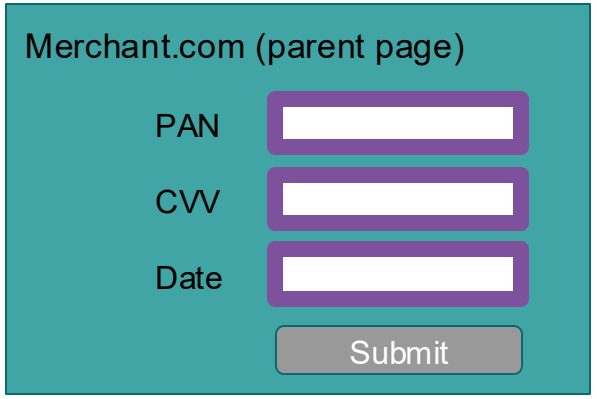
Heaviest lift – requirements fully applicable

- Form runs on your page ⇒ your scripts are in scope
- Direct-post (vs. merchant posted) changes where data submits, not your obligations on the client-side
- Full 6.4.3 + 11.6.1 on the merchant-owned payment pages (SAQ D or A-EP)

Embedded Payment Forms (iframes)



Entire payment form in iframe

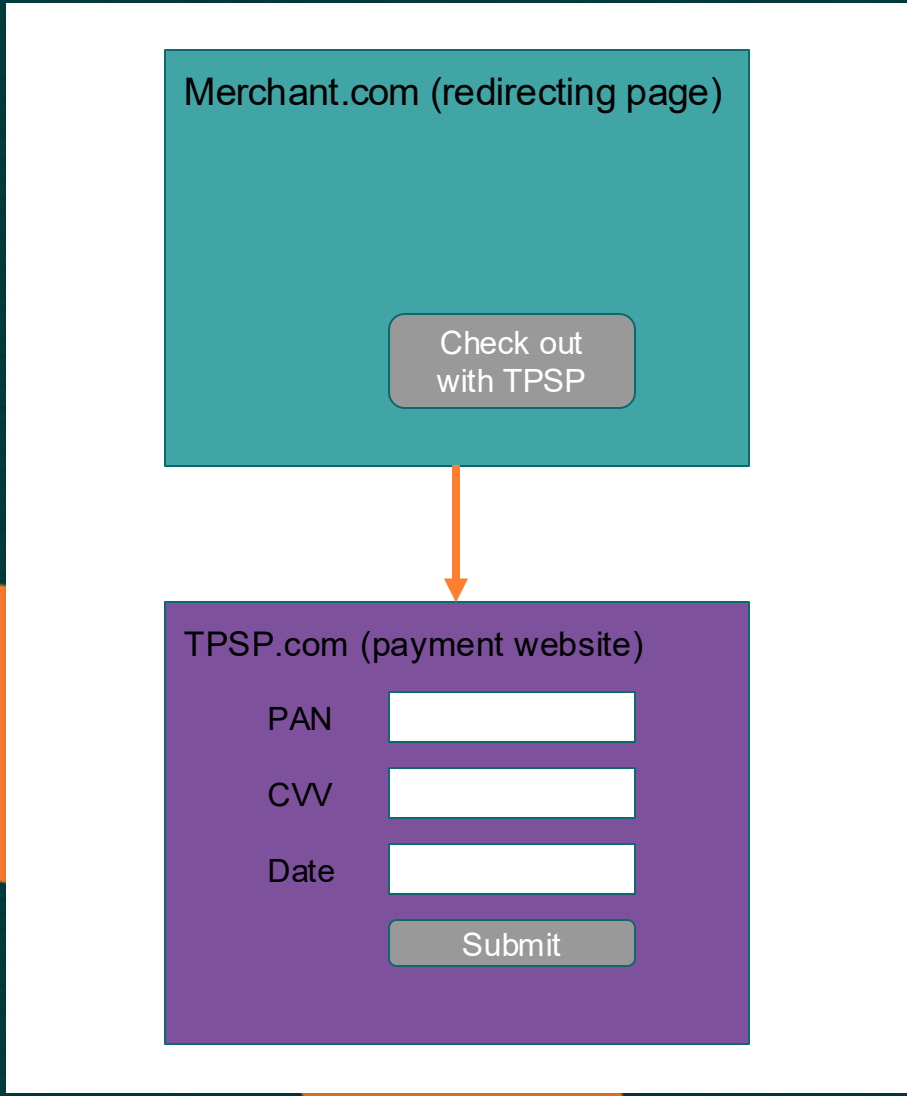


Each field in separate iframe

- TPSP form in an iframe; parent page stays in scope
- You own parent-page scripts; TPSP owns iframe scripts
- Iframe-creating scripts are explicitly in scope, as they are especially susceptible to script-based attacks

→ **Script-created iframes may necessitate additional parent page controls to assure SAQ A eligibility**

PCI Security Standards Council



Redirection

- Shopper leaves your site to a TPSP page
- TPSP owns target page scripts
- Script-driven redirects ⇒ Your redirecting page is in-scope

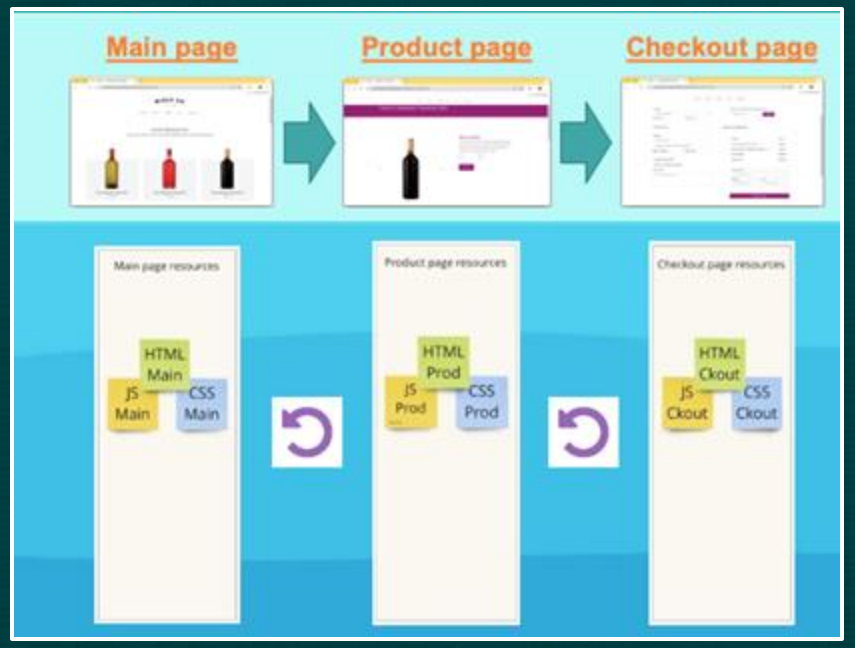
Fully Outsourced

Lightest lift

- Entire flow on TPSP site (e.g., no merchant website redirecting to TPSP)
- No 6.4.3/11.6.1 duties for the merchant
- Still confirm TPSP AOC and clear responsibility split

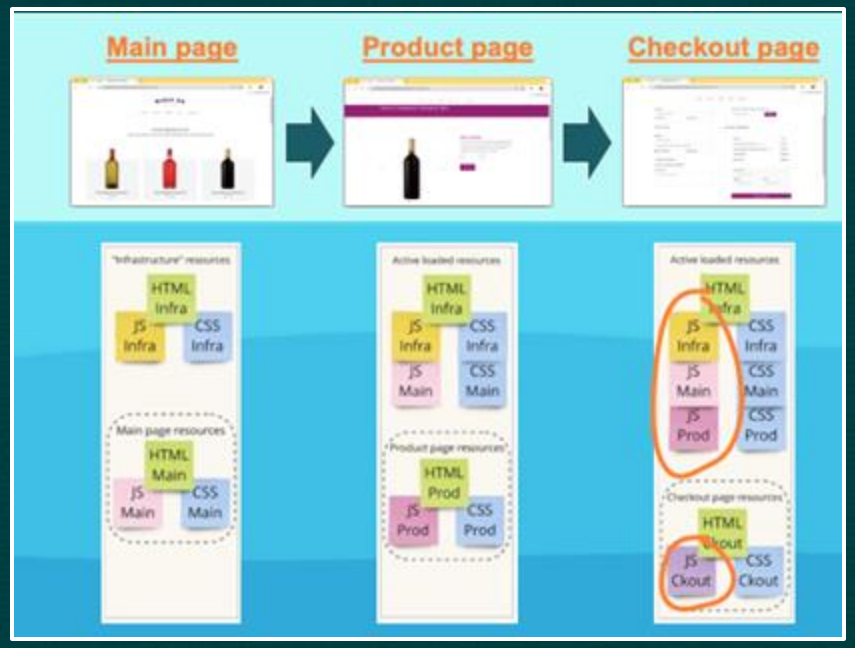
Reminder: Website Architecture Impacts Scope

”Classic” Multi-page App



Only payment and/or “parent” pages in scope

”Modern” Single-page App



Entire application in scope!

PCI Security Standards Council

Operationalizing 6.4.3 and 11.6.1

- **Goal:** stop unauthorized code on payment pages; **catch tampering fast**
- **Mindset:** improve what's deployed; close gaps; demonstrate
- **Levers:**
  1. **Evolve architecture**
  2. **Deploy tools**
  3. **Align people**
  4. **Streamline process**
  5. **Prep for assessment**

PCI Security Standards Council

Evolve Architecture

One-time heavy lift for large ongoing benefit

- Split SPA at checkout or render payment in its own page
- Prefer embedded/redirected/outsourced payment pages
- Switch embedding/redirecting mechanism from script-based to html-based
- Minimize scripts on payment/parent pages

Deploy Tools

A wide range of approaches and tradeoffs…

Content Security Policy & Subresource Integrity

Pros:
- Proactive
- Free

Cons:
- Complex to manage
- Blunt & brittle
- No inventory management
- No header change alerts

Synthetic Scanner

Pros:
- Inventory/management
- Unintrusive

Cons:
- Incomplete & bypassable
- Setup & maintenance
- Monitoring only

Reverse Proxy

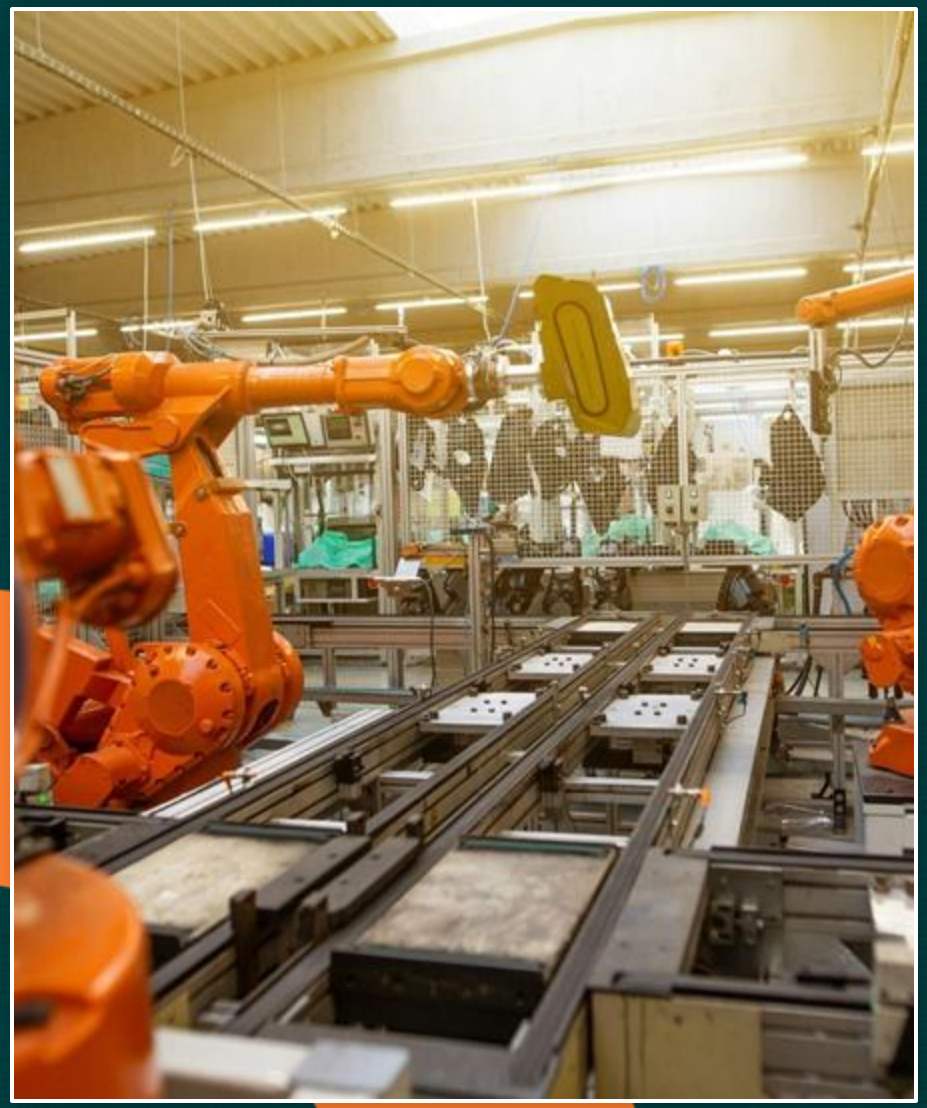
Pros:
- Inventory management
- Fully block changed scripts

Cons:
- Full block is overkill
- Setup & maintenance
- Performance
- CDNs/WAFs avoid this

Real-user Monitoring & Defense

Pros:
- Inventory/management
- Setup & maintenance
- Precision mitigation
- Hard to evade

Cons:
- Yet another script



Deploy Tools

The right tool will streamline security & compliance

One-stop shop

- Header & script monitoring “as received by the consumer browser”
- Complete system of record (e.g., audit report on-the-fly)
- Workflow & collaboration

Total cost of ownership

- Extra $$ for services or blocking?
- Upfront effort (e.g., integration, auto-discovery)
- Ongoing effort (e.g., noise, automation)

Balance security with business needs

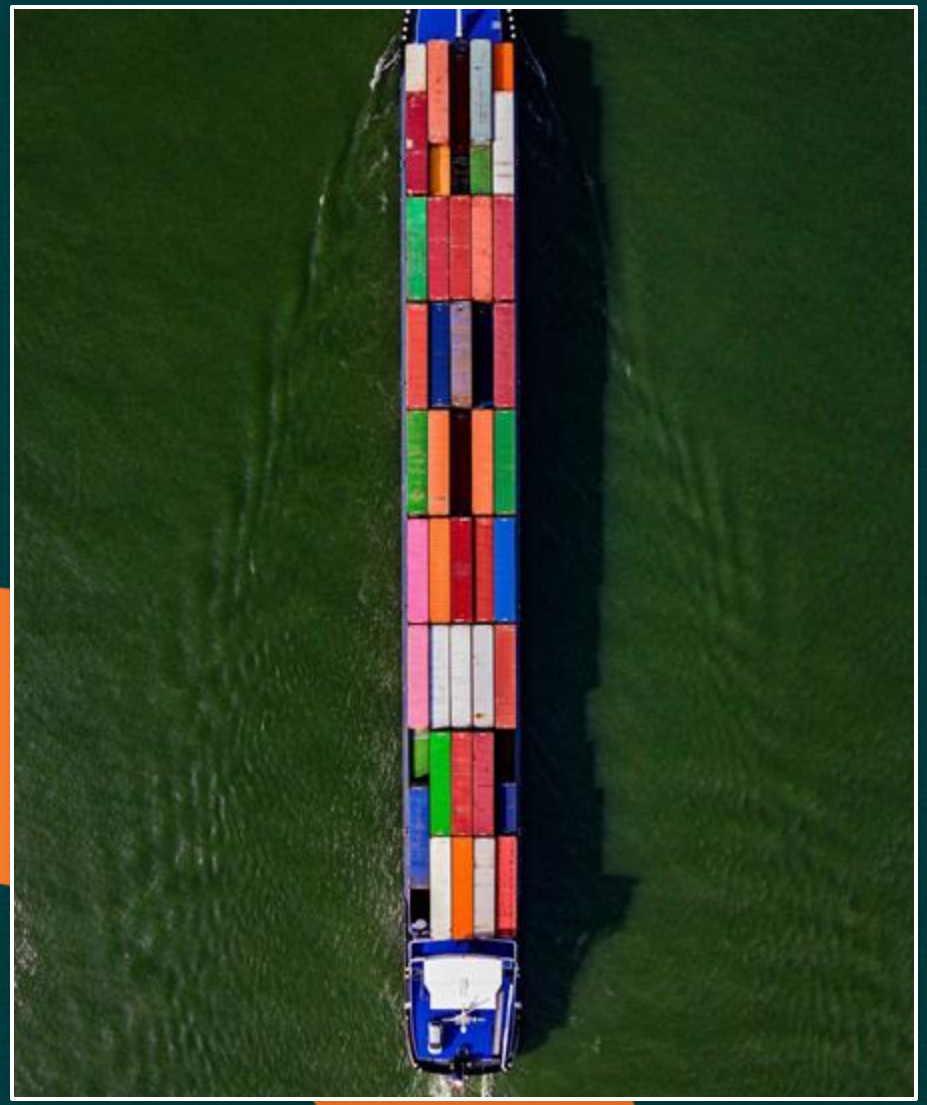
- Decision-aiding analysis
- Authorize the script, protect the data
- Neutralize scripts until fully removed

PCI Security Standards Council

Align People

Clear owners and accountability

- Name **owners**: payment/parent pages, first-party scripts, and each vendor
- Establish a **cross-functional working group** (security, compliance, devs, marketers, procurement)
- **Define RACI + SLAs** for alerts, approvals, exceptions, and escalations
- **Train** owners on policy, tooling, and standard operating procedures



Streamline Process

Tighten existing Standard Operating Procedures

- **Inventory stays live**; every script has a written **business/technical justification** and **auth state**
- **Risk-based authorization**; fast-path known low-risk, escalate unknown/high-risk
- **Change handling:** pre-announced changes follow a lightweight path; **unexpected** ones trigger triage/escalation
- **Automate** where safe (policy rules, integrations to SIEM/Jira/Chat) and **periodically re-baseline**.

Prep for Assessment

The right tool will provide much of this out-of-the-box

- **Policies & procedures** for 6.4.3; **roles & responsibilities** per 6.1.1/6.1.2
- **Inventory + justification**; **method(s)** proving script integrity & auth
- **11.6.1 mechanism** configured to evaluate headers + page content; **evidence of frequency** (weekly or TRA)
- **Outputs:** logs/alerts/reports from monitoring or scans; config screenshots
- **IR plan** includes monitoring & responding to these alerts (table-tops if no incidents).

Takeaways

Goals checklist

- ☑ Clarify applicability, scope, and SAQ eligibility across payment page types
- ☑ Understand the challenges of operationalizing controls in large orgs
- ☑ Learn actionable, role-specific next steps to sustain security and demonstrate compliance

Thank You

PCI Security Standards Council