

Transforming PCI:

The ISA as a Strategic Governance Leader

Fireside Chat | PCI SSC + ISA + QSA Perspectives

Sound Familiar?

The Scramble

The Surprise

The Bottleneck

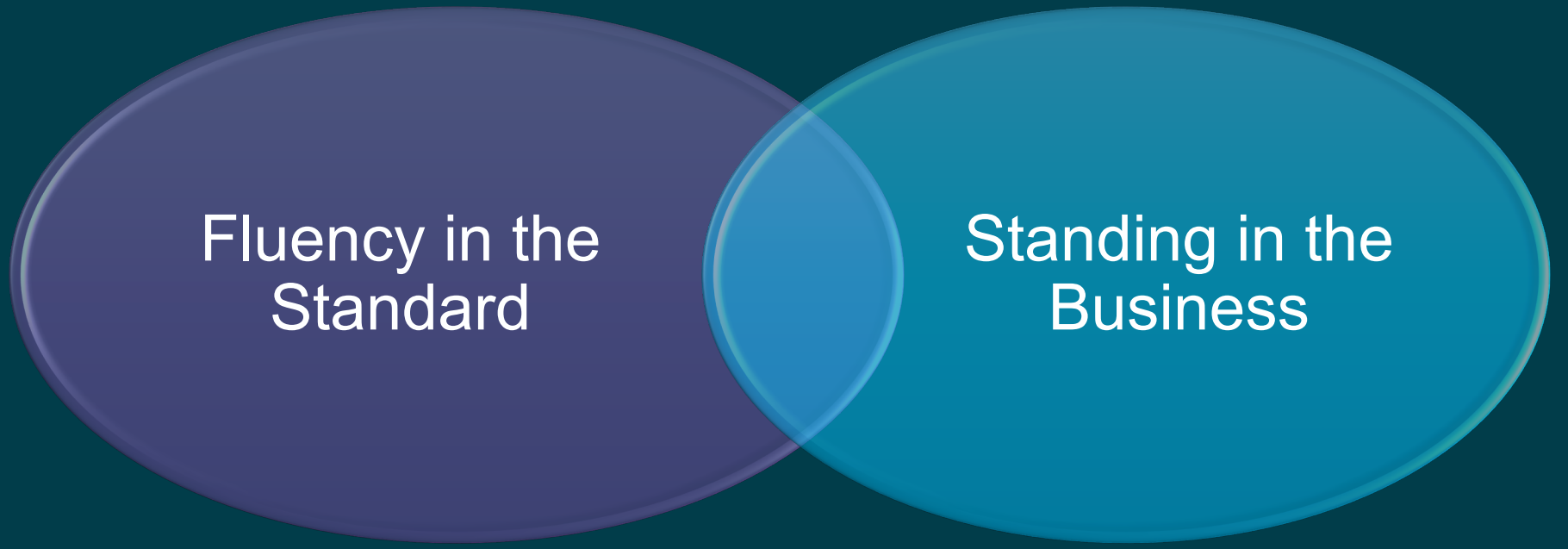
The Rework

The Amnesia

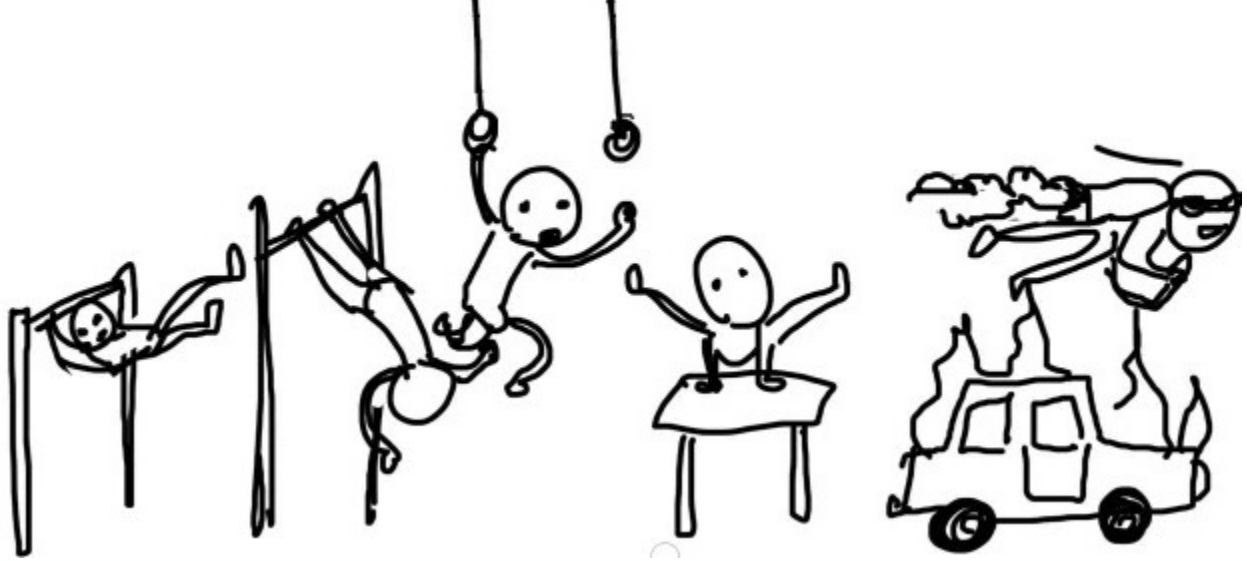
Sound Familiar?



An Owner



“Why wouldn’t I arm my people with the same training the external assessors get?”



PM wants a new report

Devs copy CHD to reporting DB

QSA finds new CDE

Apply controls to systems

Create CCs and gather evidence before deadline

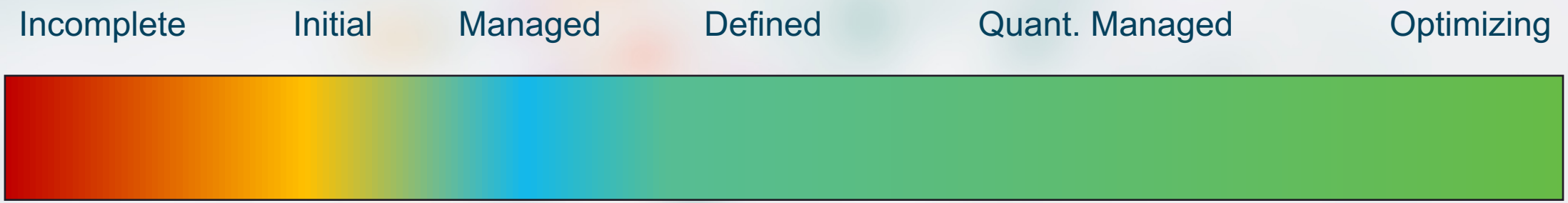


PM wants a new report

ISA advises truncated data

No change to scope

Maturity Model



ISA

ISA as a Governance Leader



pathward®

Tracey Hughes

Vice President, Information Security



RSM

Brian Frey

Director, RSM US LLP

The Three-lens Conversation

PCI SSC

Program intent
ISA purpose
Community context

ISA

Year-round governance
Internal influence
Business enablement

QSA

External perspective
What maturity looks like
Assessment readiness signals

What the PCI Council envisioned. What the ISA can lead. What the QSA can see.

The Core Shift

From a compliance event to a governance capability

Assessment readiness



Continuous governance

The ISA Governance Framework

A simple way to explain the year-round value of the ISA role.

ENABLE

- Engage early
- Projects
- Vendors
- Architecture

PROTECT

- Strengthen controls
- Risk-informed decisions
- Cross-functional partnership

IMPROVE

- Measure outcomes
- Lessons learned
- Automation
- Continuous monitoring

Focus on Behaviors - Not requirements.

ISA + QSA: Partnership Without Outsourcing Ownership



The QSA can assess, clarify, and validate.
The organization must still own the controls.

The ISA should help make the organization stronger, not merely make the assessment easier.

What Maturity Looks Like to a QSA

SCOPE

Proactively managed and identified before the assessment

EVIDENCE

Collected proactively from normal operations, not last-minute

CONTROL OWNERS

Able to explain controls, not just provide evidence

Readiness is not a checklist – it is how the program operates

A strong ISA makes the program easier to assess because ownership, scope, evidence, and decisions are already governed

Earlier Conversations Reduce Late-stage Surprises

- Architecture Reviews
- Vendor Onboarding
- Change Governance
- Risk Committees
- Executive Reporting



Challenge

1. Invite the ISA into one earlier business conversation
2. Reframe one recurring issue as a governance opportunity
3. Strengthen the ISA-QSA dialogue without outsourcing ownership



“If your ISA disappeared tomorrow, would your PCI program continue improving?”

Compliance passes assessments. Governance builds trust.