Managing PCI DSS Compliance at Scale

No AI. Only Foundations

Zach Johnson

Head of Governance, Risk and Compliance

The Home Depot

Ilona Garland

PCI ISA, CISA

Senior Manager of PCI and PII Compliance

The Home Depot

Agenda

1. PCI DSS at Scale
2. Solving PCI DSS at Scale
3. Benefits Realized

PCI DSS at Scale

PCI DSS at Scale

What is your scale?

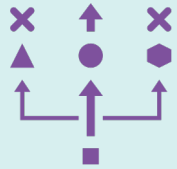
Understand the Environment

1.6B+ Annual Transactions

- 30+ Entry Flows
- Store, Online, Phone
- Multiple Processers

10K+ PCI In Scope Assets

- On Prem / Cloud
- Store / Enterprise
- Third Parties



150K+ Unique Control Testing Combinations

- Automation / Manual
- Domain / Solution
- Evidence / Validation

PCI DSS at Scale

Can we do compliance better?

Problems with Scale

Manual Overhead

PCI Compliance management historically manual and needed simplification.

Compliance Gaps

Challenges with tracking the entirety of the scope without missing anything.

Ownership Tracking

Difficulties with tracking ownership shifts and control applicability.

Scope Validation

Scoping and inventory validation at scale needed simplification.

Testing

Difficulties with validating compliance status across the environment.

Risk Planning

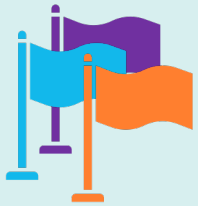
Difficulties with aligning compliance and risk.

Solving PCI DSS at Scale

Solving PCI DSS at Scale

Establishing PCI Governance for Scale

Key Steps



Identify your governance flags.

- PCI CDE
- PCI Connected
- PCI Security Impacting

Break your environment into components.

- Application
- Device / VM
- Database
- Cloud / Infrastructure
- Third-Party Integration

Define your control templates.

- SAQ D
- SAQ A
- SAQ A-EP
- POI
- Third-Party

Solving PCI DSS at Scale

Breaking down your environment into components

EXAMPLE 1

Solution 001 PCI CDE

- **Application** PCI CDE SAQ D
- **Device/ VM** PCI CDE SAQ D
- **Database** PCI CDE SAQ D
- **Third-Party Integration** PCI CDE Third-Party

EXAMPLE 2

Solution 002 PCI Security Impacting (SI)

- **Application** PCI SI SAQ A
- **Application** PCI SI SAQ A-EP
- **Cloud Project** PCI SI SAQ A-EP

EXAMPLE 3

Solution 003 PCI CDE

- **Device** PCI CDE POI

Flag Template

Solving PCI DSS at Scale

Establishing Control Templates

Identify your PCI enterprise and solution controls.

- Business
- Technology
- Cyber

Create your solution and domain control templates.

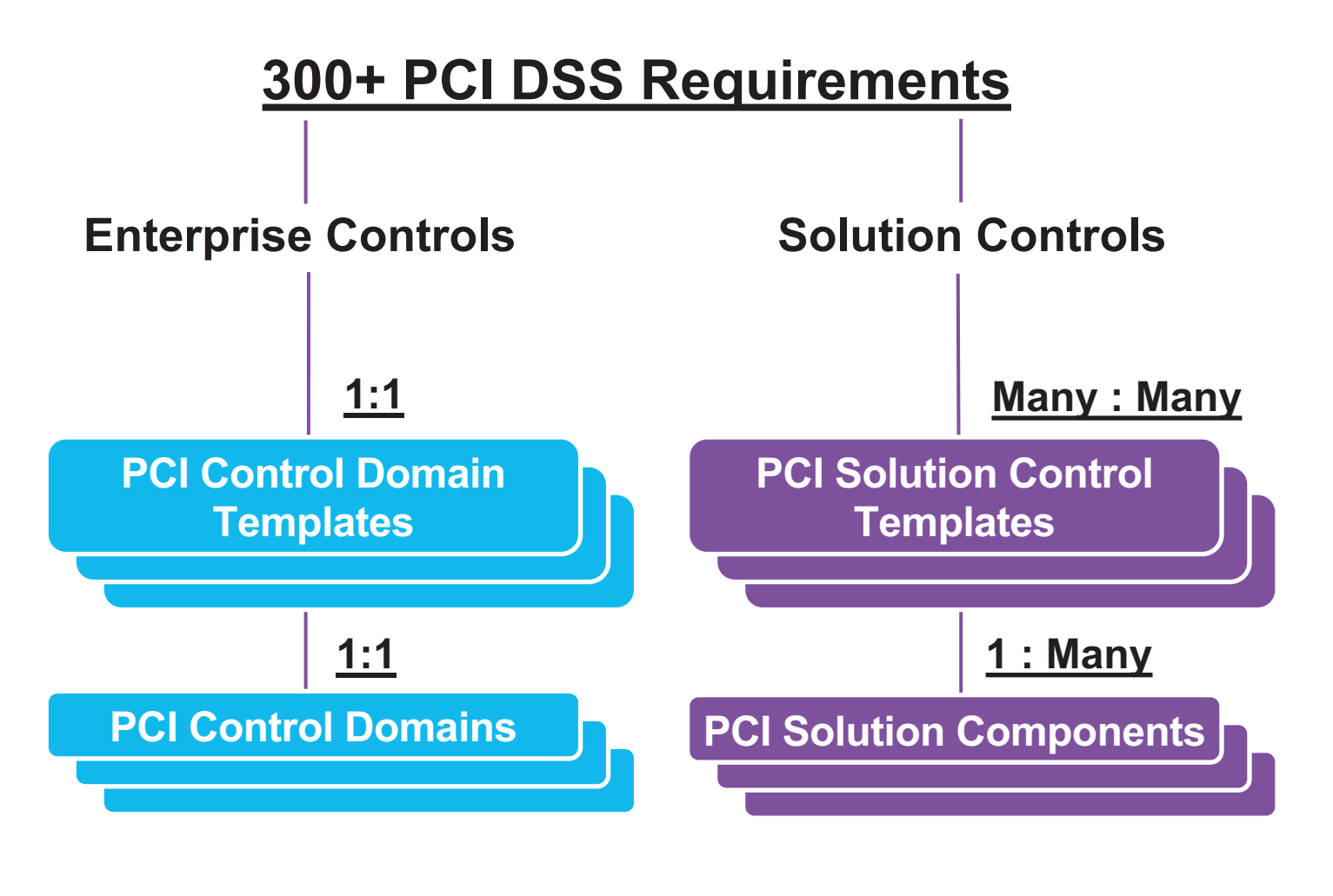
- Governance Flags
- Solution Components
- Scope Categories
- Enterprise Categories

Map PCI controls to your templates.

- Solution Templates
- Domain Templates

Solving PCI DSS at Scale

Example of Control Templates



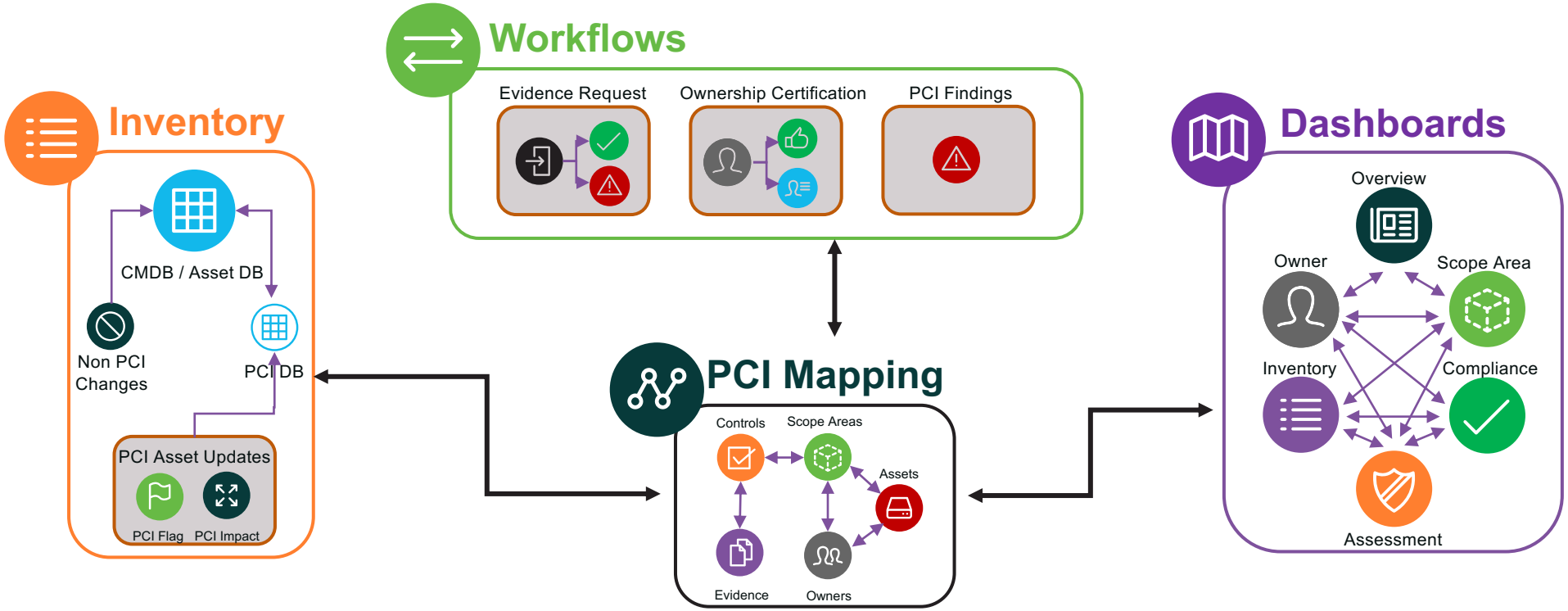
Control Template Examples

- Application_PCI CDE_SAQ D
- Application_PCI SI_SAQ A
- Cloud Project_PCI CDE_SAQ D
- Third Party Integration_PCI CDE_Third-Party
- Device_PCI CDE_POI
- Physical Security (Domain)
- Authentication Mgmt (Domain)

Benefits Realized

Benefits Realized

Compliance at scale



Benefits Realized

Simplifying compliance

Benefits

Reduction in Resources

Eliminated the need to manually assign PCI controls.

Streamlining Assessments

Ability to schedule assessments for any requirement, template, component with a push of a button.

Confidence in Scoping

PCI scope validation is completely automated. Any updates are synched with the IT Governance process.

PCI DSS Shift Readiness

PCI Control Owners sign off on their roles and responsibilities during the annual scope validation with no additional effort from the PCI team.

Inventory Quality

Raising the inventory and ownership quality standards across the environment.

Risk Alignment

Through clearer scoping risk and compliance can work together.

Thank you!

PCI Security Standards Council®

2025 NORTH AMERICA COMMUNITY MEETING