

# What Are the Implications of Infrastructure as Code and PCI DSS?





# Lauren Holloway

Director, Data Security Standards  
PCI Security Standards Council



# Peter O'Sullivan

QSA, Principal Information Security Consultant  
Blackfoot Cybersecurity



# Introduction to IaC and PCI DSS

## PCI DSS

A set of baseline technical and operational requirements designed to protect account data.

## Infrastructure as Code (IaC)

Managing and provisioning computer resources through machine-readable definition files, rather than hardware configuration or interactive tools.

# Introduction to IaC and PCI DSS

## PCI DSS

A set of baseline technical and operational requirements designed to protect account data.

## Infrastructure as Code (IaC)

Managing and provisioning computer resources through machine-readable definition files, rather than hardware configuration or interactive tools.

## Intersection of IaC and PCI DSS

Integrating IaC with PCI DSS facilitates implementation of a secure, consistent, repeatable infrastructure.

# Traditional vs IaC Infrastructures

## Hardware Devices / Traditional

- Manual, static configuration files
- Apply configurations to each device separately
- Not scalable
- High chance of misconfigurations

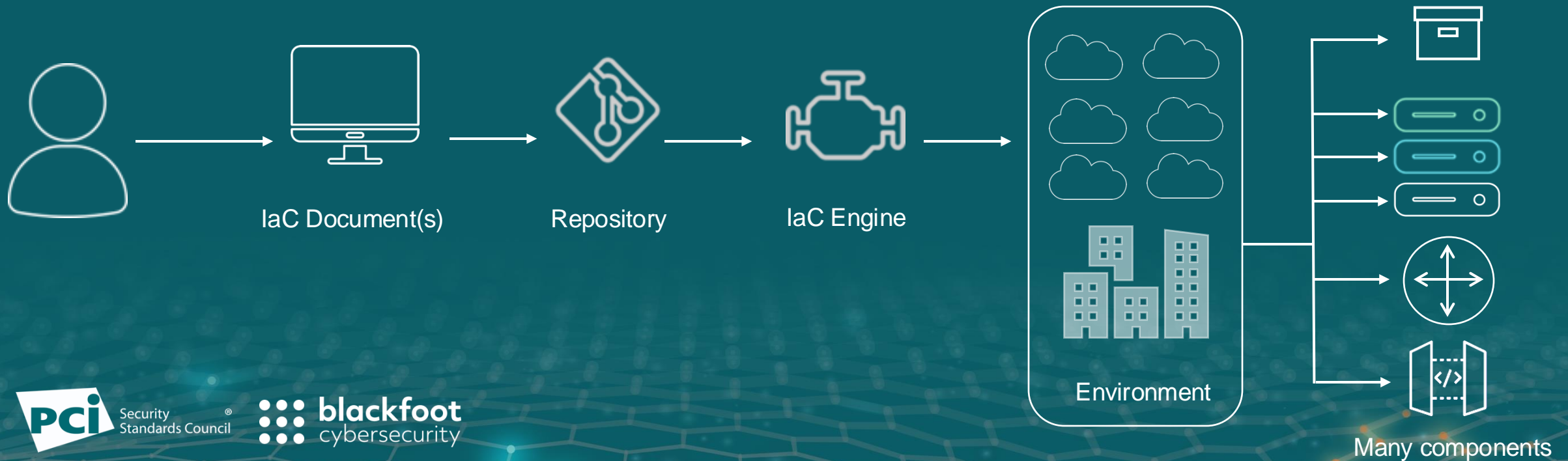
## Cloud-Based / IaC

- Configurations in IaC documents that convert to machine-readable code
- Apply configurations via dynamic automated updates
- Consistent and scalable

# How Might Those Differences Be Represented?

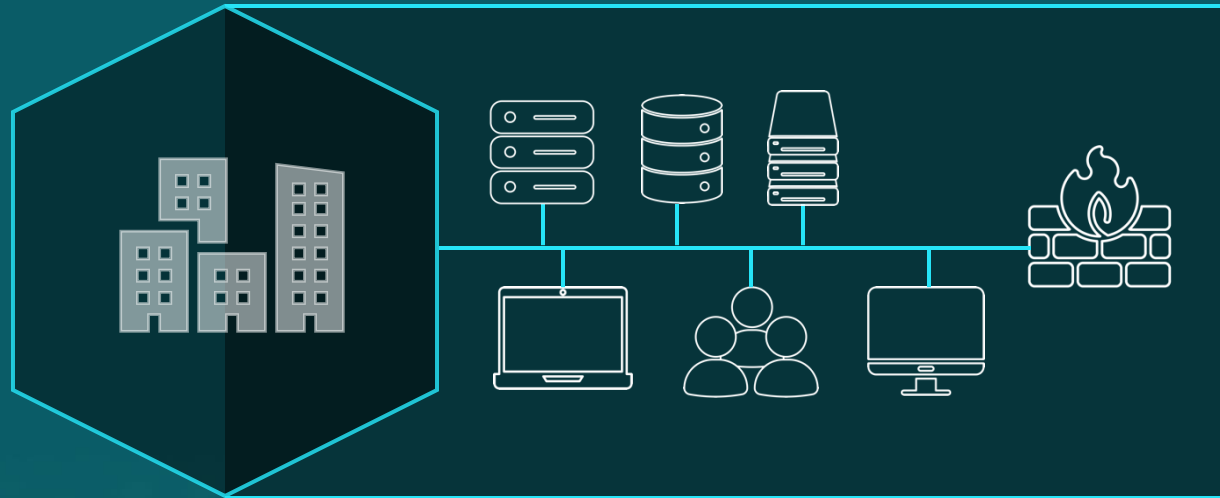


# How Might Those Differences Be Represented?



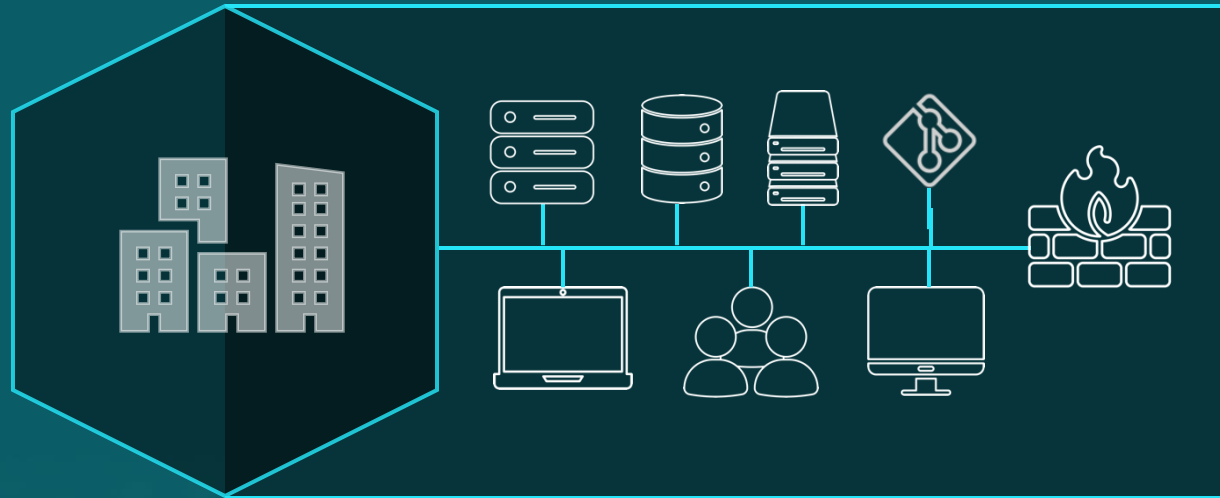
# Traditional Infrastructures

PCI DSS SCOPE

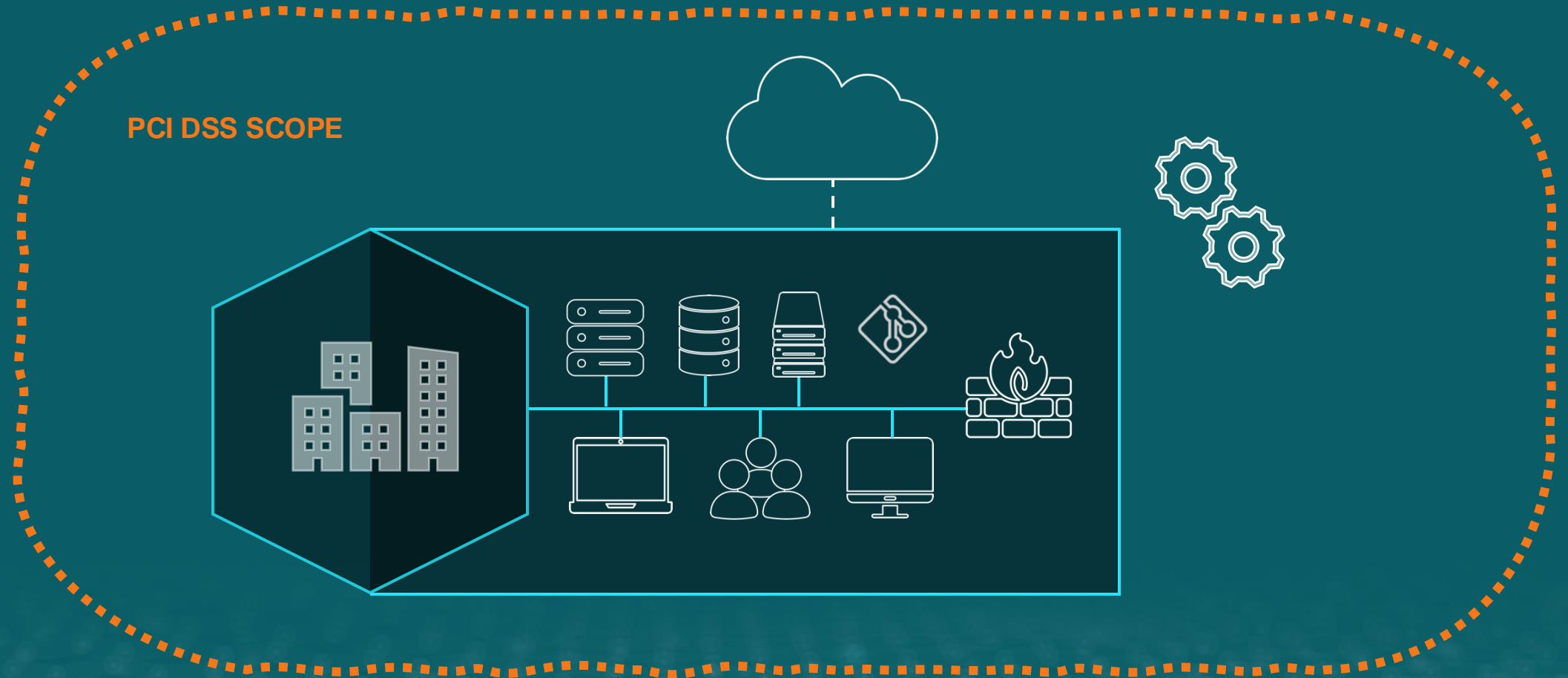


# Repository Locations and Connectivity

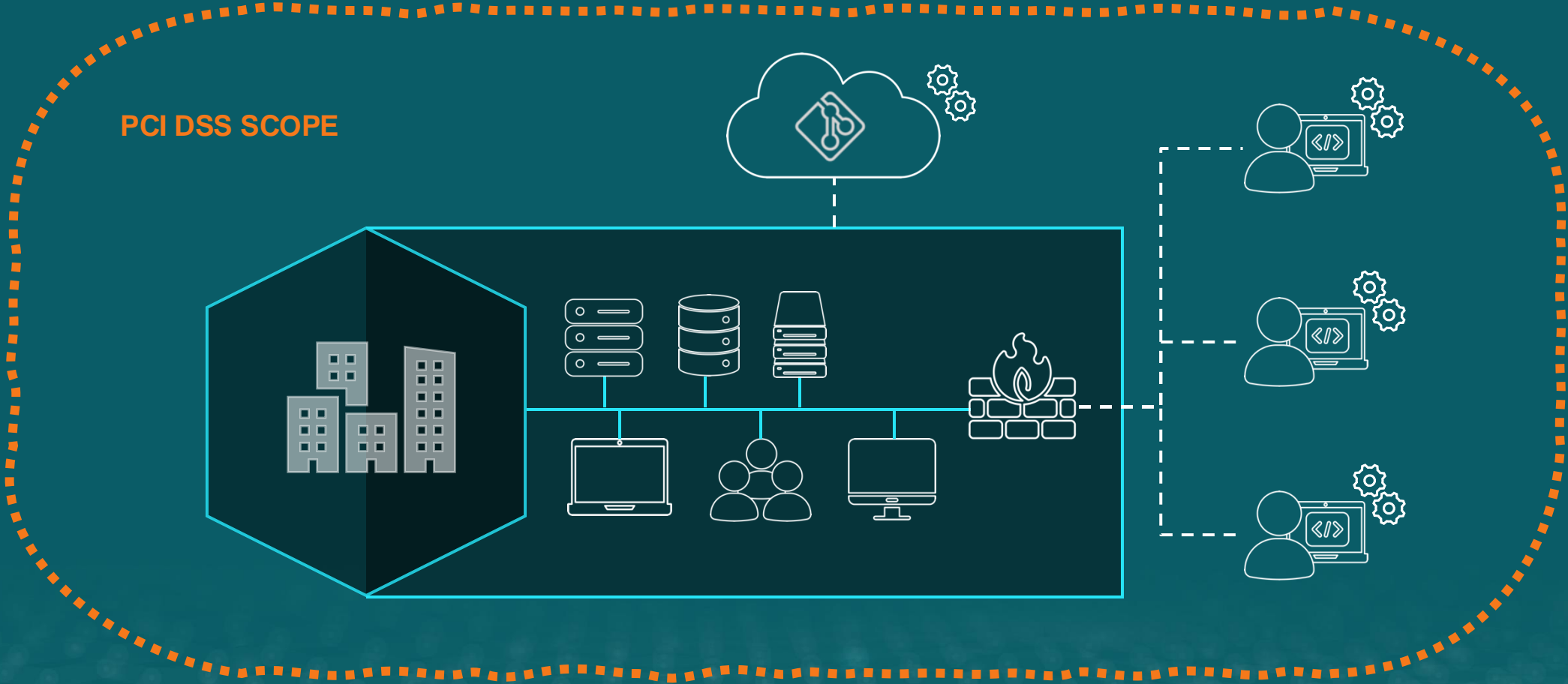
PCI DSS SCOPE



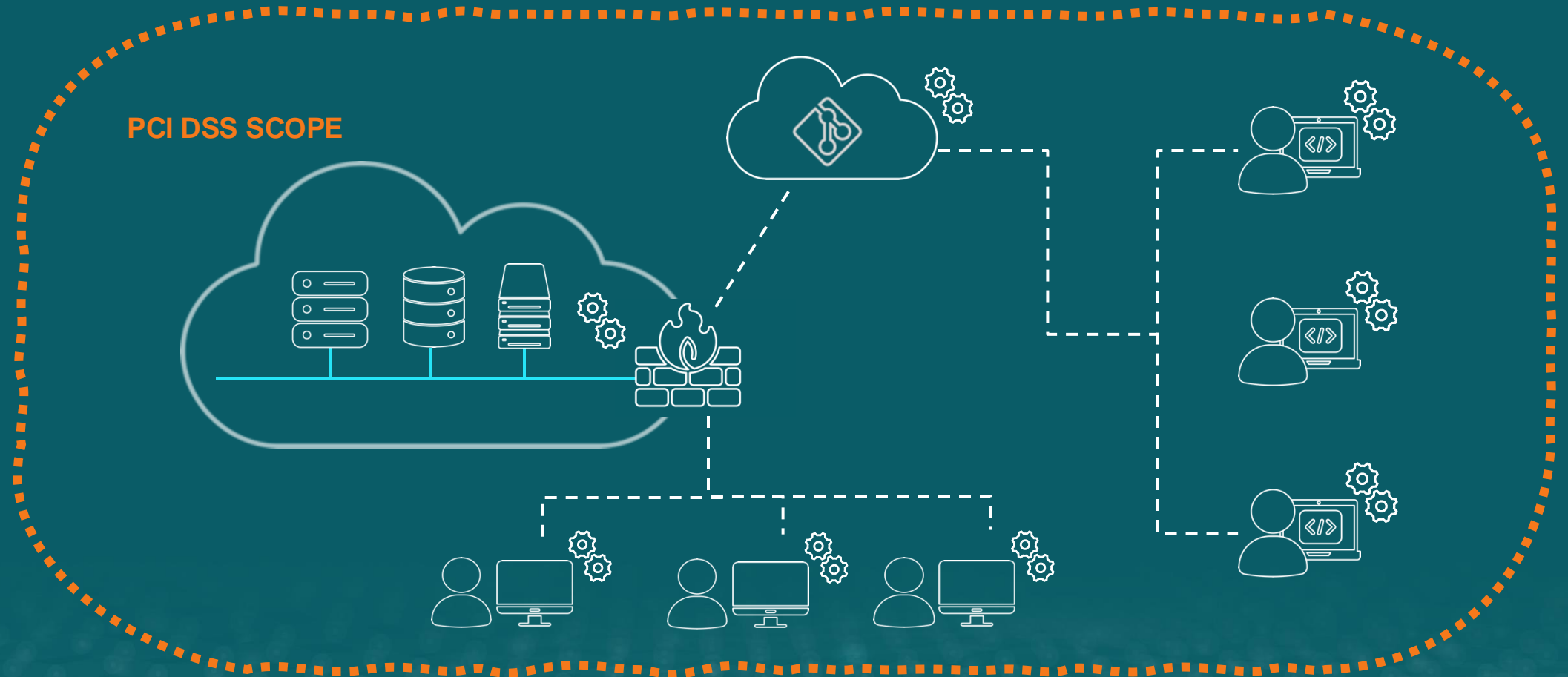
# Repository Locations and Connectivity



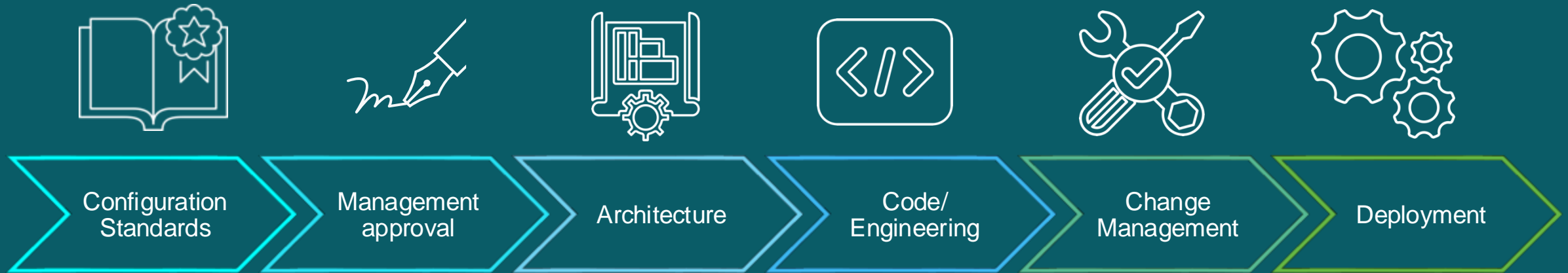
# Endpoint Considerations and Scope Validation



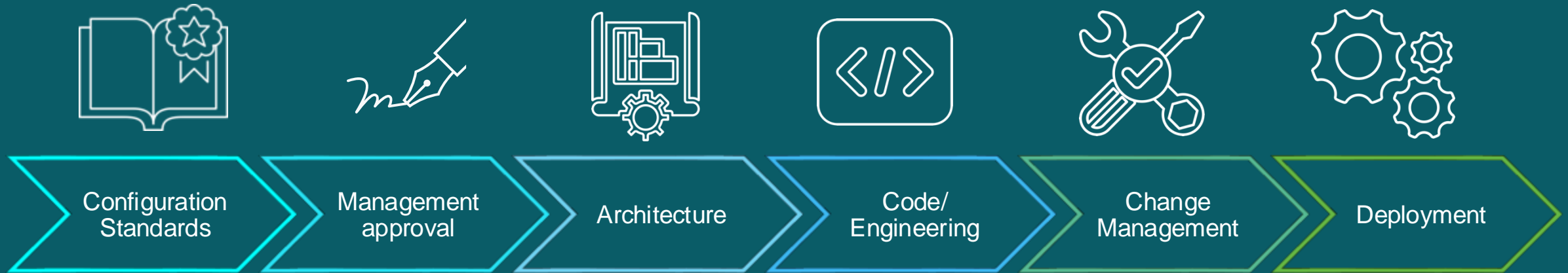
# Cloud Considerations and Scope Validation



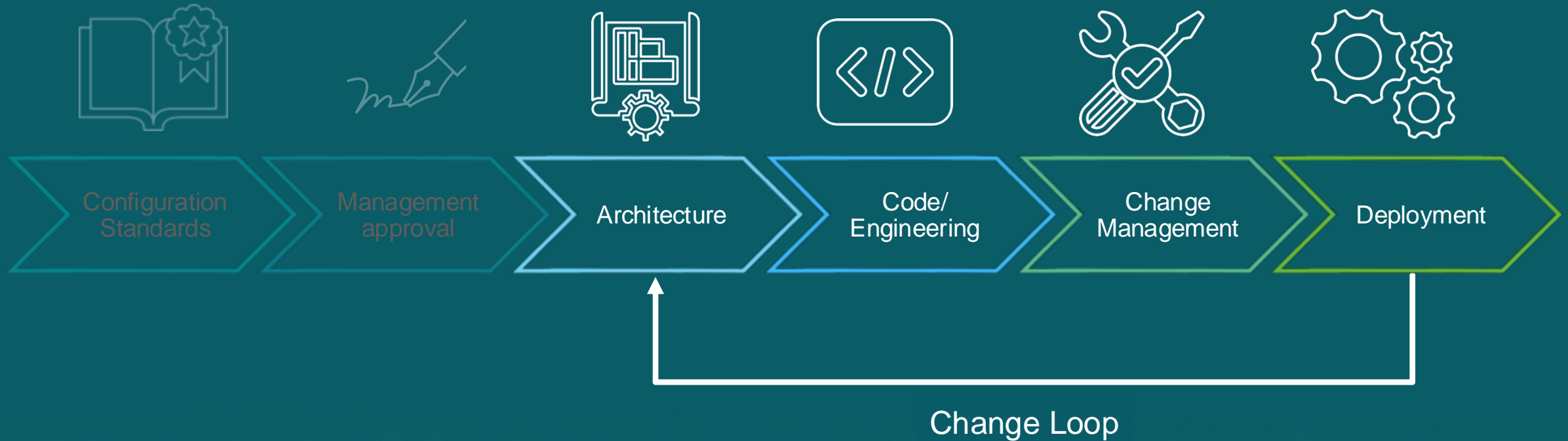
# Steps to Infrastructure as Code



# Steps to Infrastructure as Code



# Steps to Infrastructure as Code



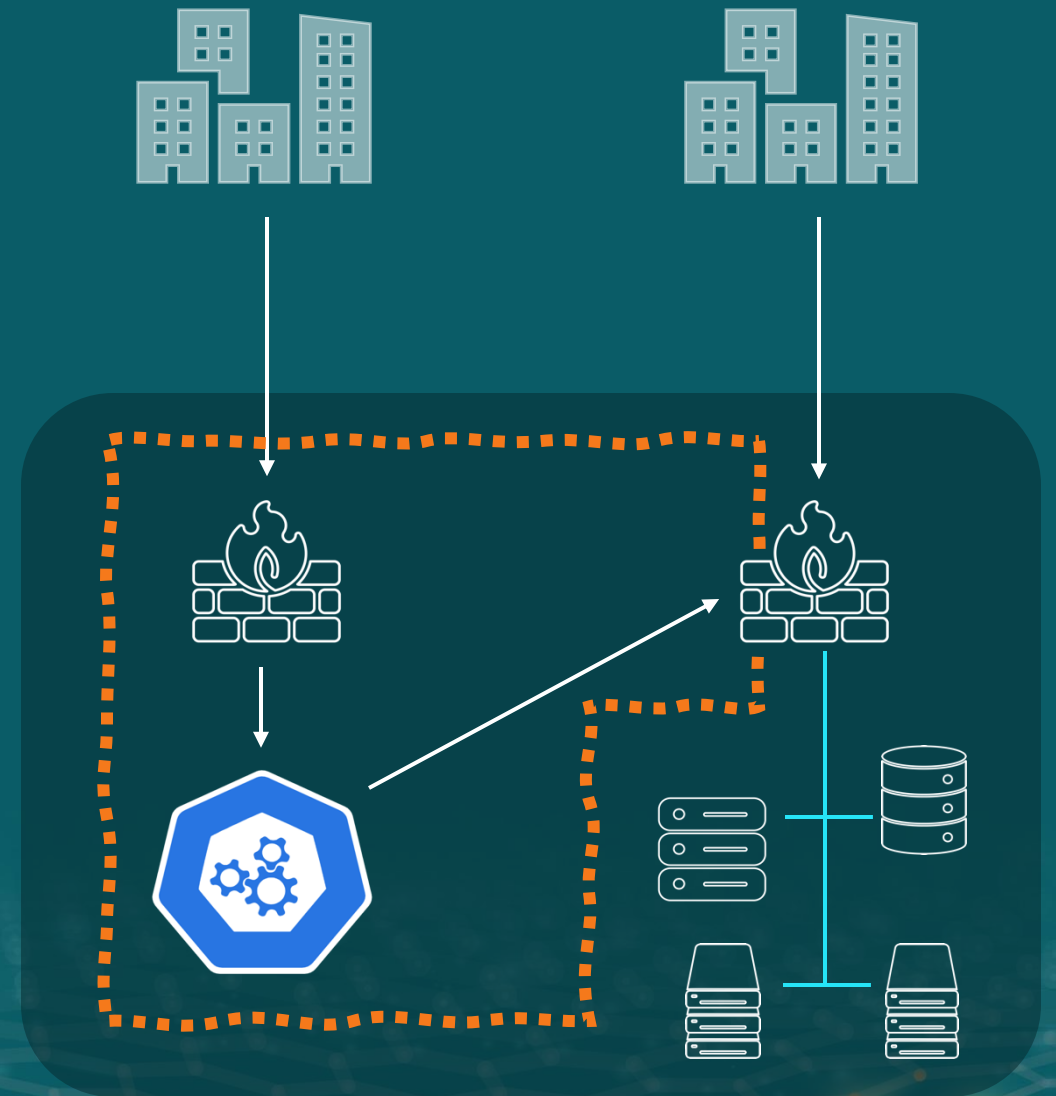
# Pop Quiz | Ask a QSA

## Scenario:

- Launch of an **externally-facing API** to transmit and process **cardholder data (CHD)**.
- The organization's first implementation of IaC, and first implementation of an API for CHD.

## Consider:

1. Infrastructure as Code
2. CDE components



# Pop Quiz | IaC Components

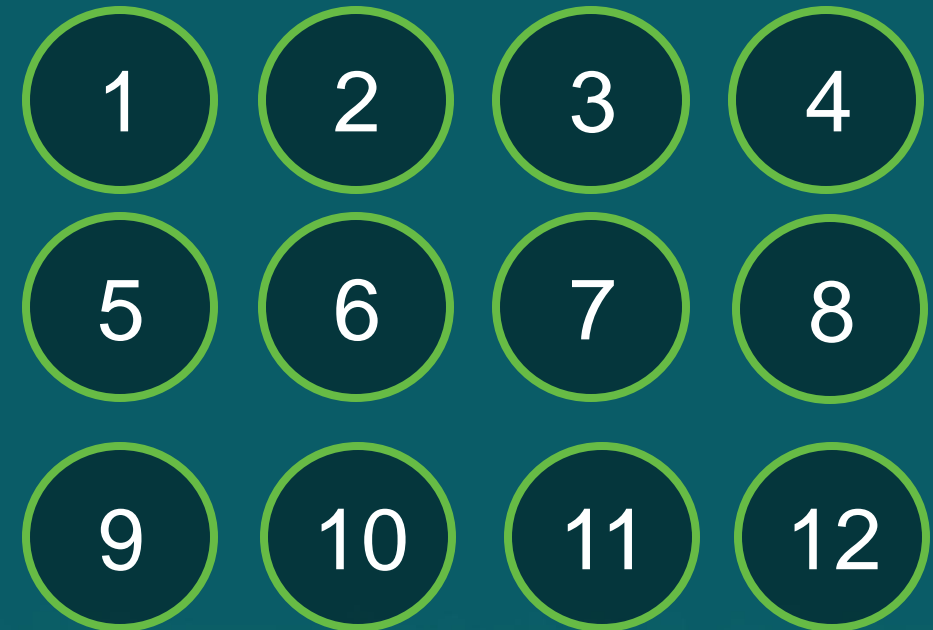
## Scenario:

- Launch of an **externally-facing API** to transmit and process **cardholder data (CHD)**.
- The organization's first implementation of IaC, and first implementation of an API for CHD.

## Consider:

1. Infrastructure as Code
2. CDE components

## PCI DSS Requirements



 CDE Components  IaC Components

# Pop Quiz | IaC Components

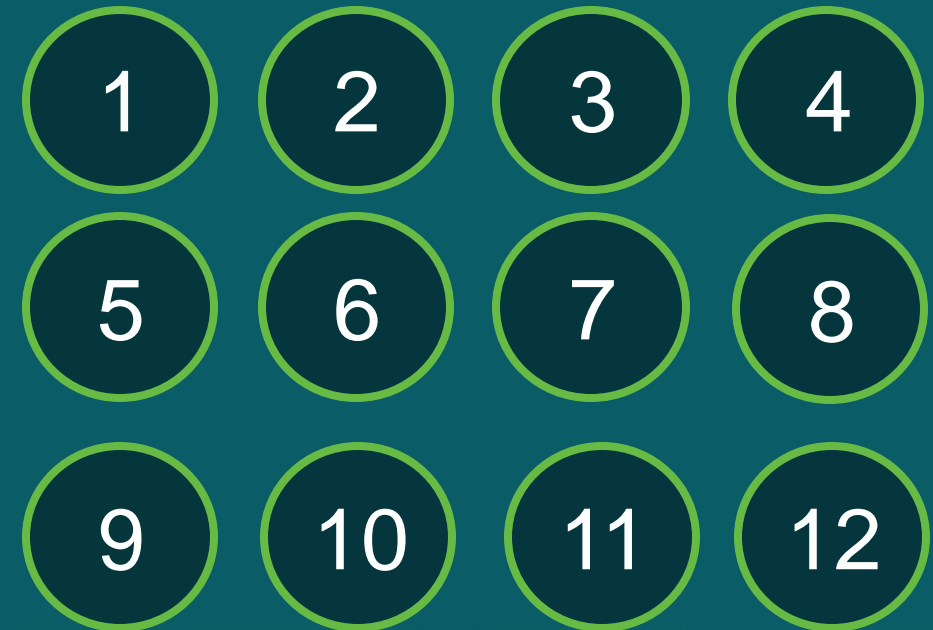
## Scenario:

- Launch of an **externally-facing API** to transmit and process **cardholder data (CHD)**.
- The organization's first implementation of IaC, and first implementation of an API for CHD.

## Consider:

1. Infrastructure as Code
2. CDE components

## PCI DSS Requirements



● CDE Components ● IaC Components

# Pop Quiz | CDE Components

## Scenario:

- Launch of an **externally-facing API** to transmit and process **cardholder data (CHD)**.
- The organization's first implementation of IaC, and first implementation of an API for CHD.

## Consider:

1. Infrastructure as Code
2. CDE components

## PCI DSS Requirements



 CDE Components  IaC Components

# Pop Quiz | CDE Components

## Scenario:

- Launch of an **externally-facing API** to transmit and process **cardholder data (CHD)**.
- The organization's first implementation of IaC, and first implementation of an API for CHD.

## Consider:

1. Infrastructure as Code
2. CDE components

## PCI DSS Requirements



 CDE Components  IaC Components

# Ongoing Considerations



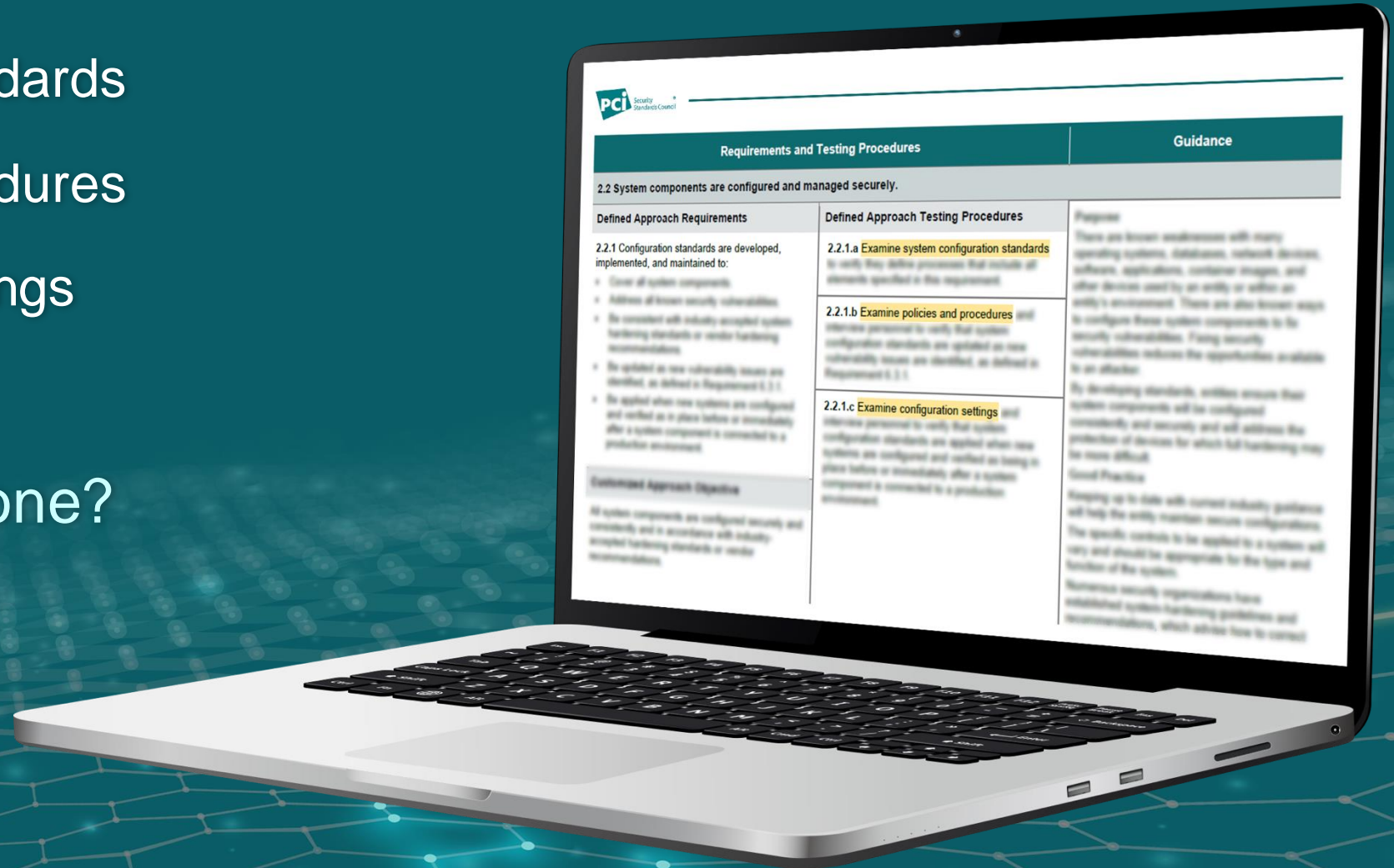
# Ongoing Considerations



# IaC (Relationship) with PCI DSS Requirements

- Configuration Standards
- Policies and Procedures
- Configuration Settings

Where has IaC gone?



# Governance Controls



Policies and procedures for operating IaC



Secure configuration of repository and use of features



Multi-tiered change control processes



Access control (IaC vs target system components)

# Governance Controls



Policies and procedures for operating IaC



Secure configuration of repository and use of features



Multi-tiered change control processes



Access control (IaC vs target system components)

# Infrastructure as Code – Considerations for PCI DSS



# Infrastructure as Code – Considerations for PCI DSS



# Infrastructure as Code – Considerations for PCI DSS



# Key Takeaways



Requirements  
6.5 & 12.5



Assessment Time



Direct Component  
Review

# Key Takeaways



Requirements  
6.5 & 12.5



Assessment Time



Direct Component  
Review



# Lauren Holloway

Director, Data Security Standards  
PCI Security Standards Council



# Peter O'Sullivan

QSA, Principal Information Security Consultant  
Blackfoot Cybersecurity





Security Standards Council<sup>®</sup>