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

John Bloomfield

Manager, Data Security Standards
PCI Security Standards Council

PCI Security Standards Council®

Peter O’Sullivan

QSA, Principal Information Security Consultant
Blackfoot Cybersecurity

blackfoot cybersecurity

blackfoot cybersecurity

PCI Security Standards Council®

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.

PCI Security Standards Council®

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.

Intersection of IaC and PCI DSS

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

PCI Security Standards Council®

blackfoot cybersecurity

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

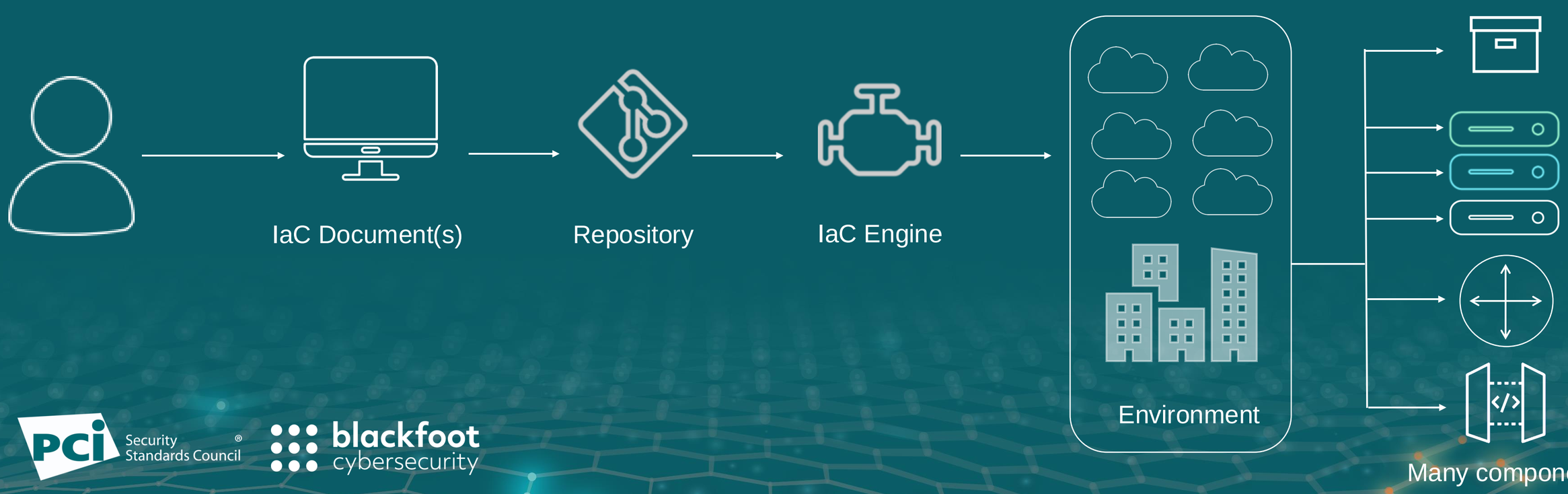
- Machine readable content convert to live configurations
- Apply multiple configurations simultaneously
- Consistent and scalable

PCI Security Standards Council®

blackfoot cybersecurity

How Might Those Differences Be Represented?

How Might Those Differences Be Represented?

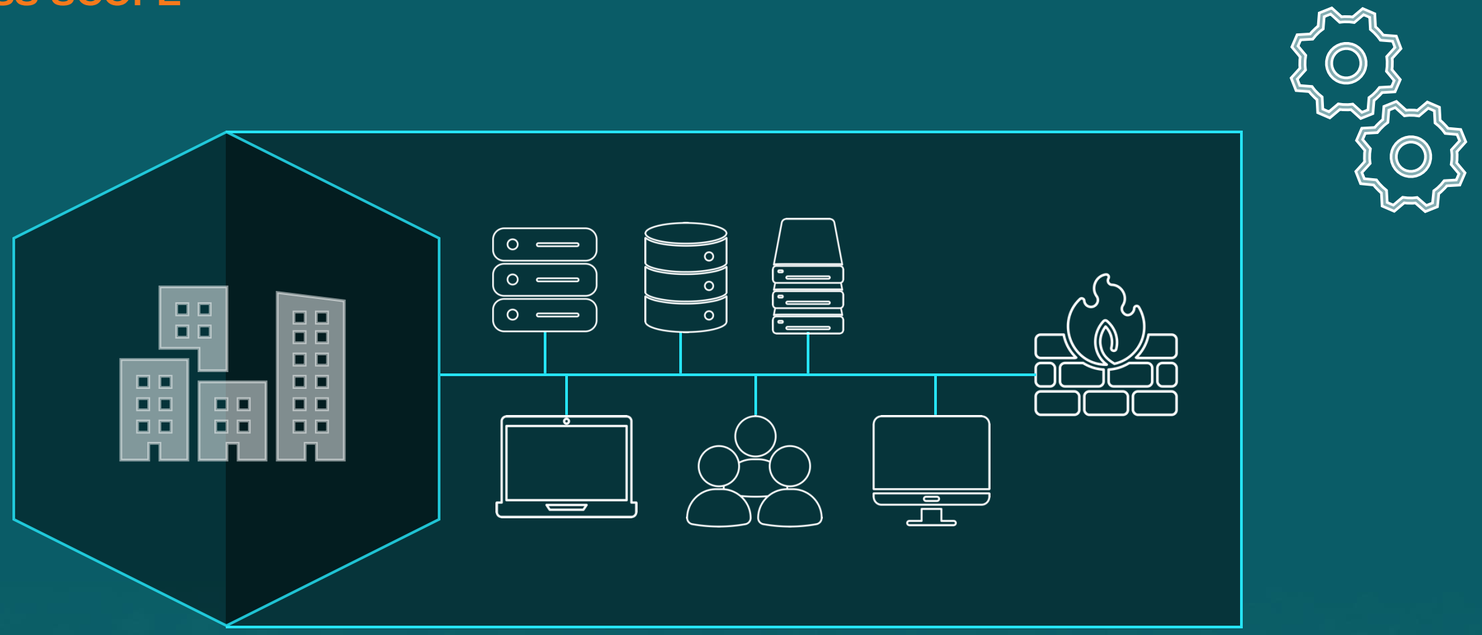


PCI Security Standards Council®

blackfoot cybersecurity

Traditional Infrastructures

PCI DSS SCOPE



Security Standards Council®

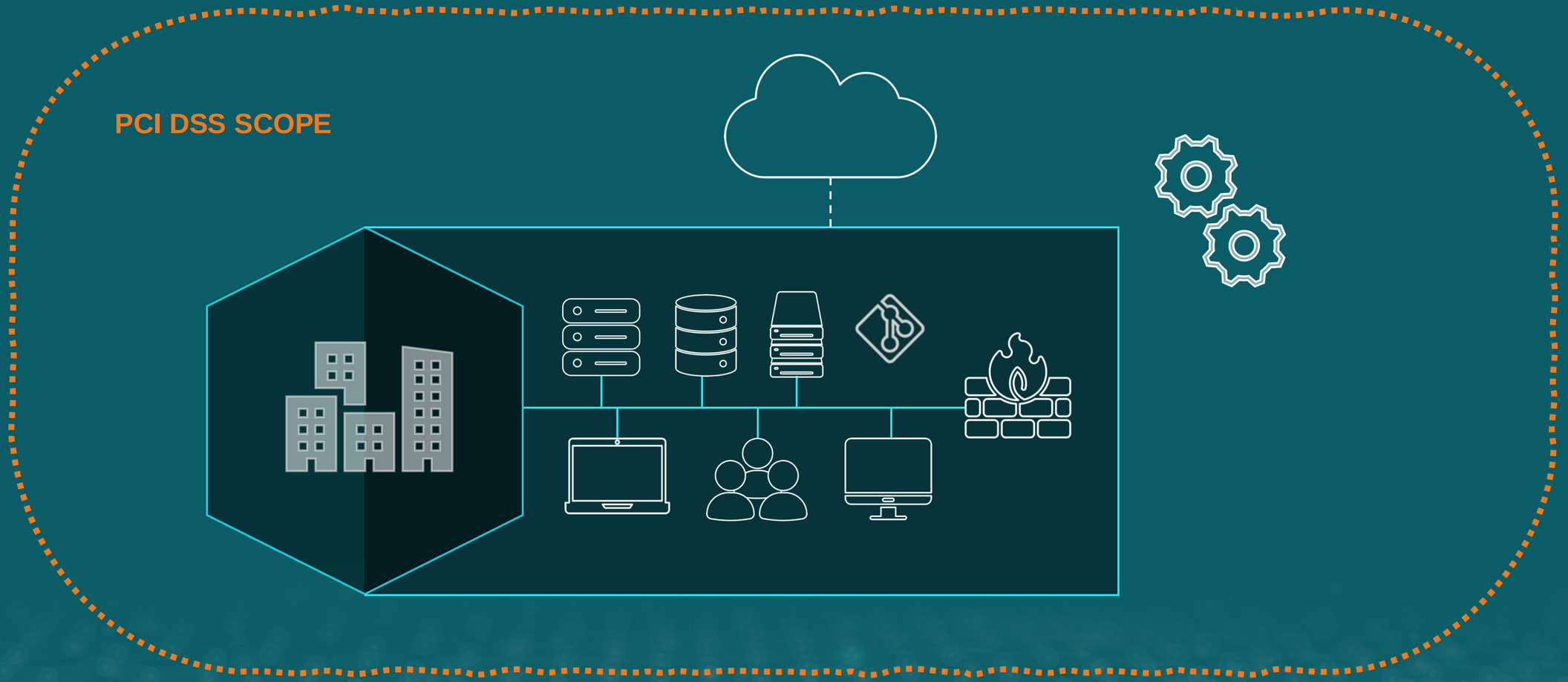
blackfoot cybersecurity

Repository Locations and Connectivity

PCI Security Standards Council®

blackfoot cybersecurity

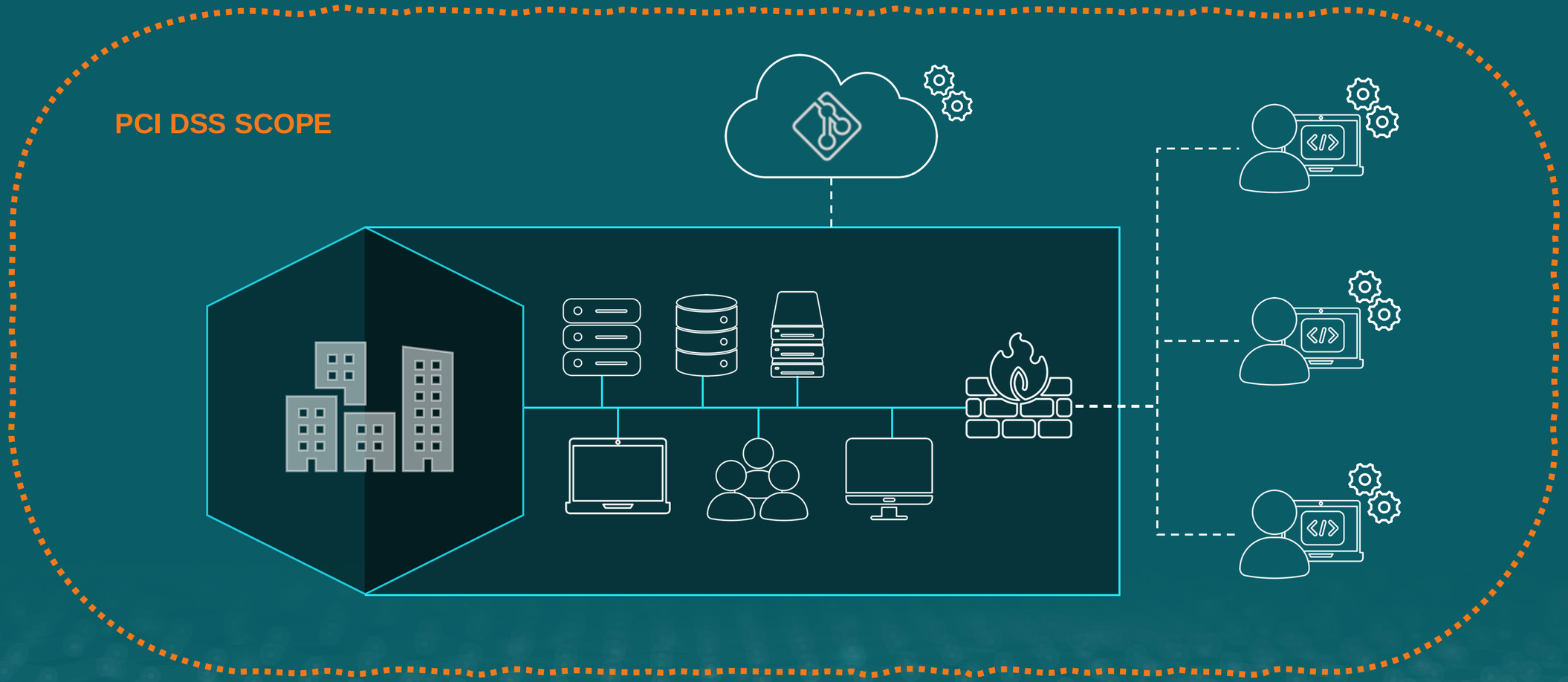
Repository Locations and Connectivity



PCI Security Standards Council®

blackfoot cybersecurity

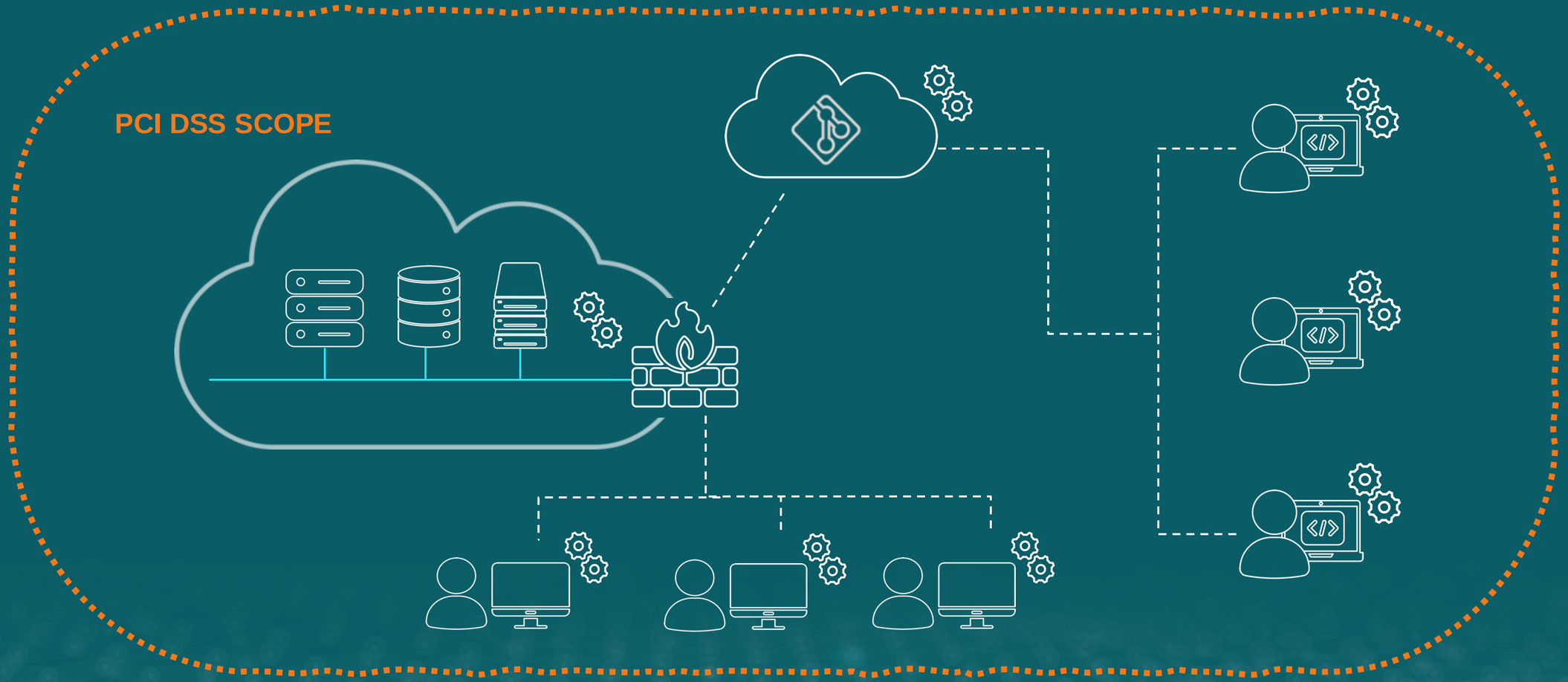
Endpoint Considerations and Scope Validation



PCI Security Standards Council®

blackfoot cybersecurity

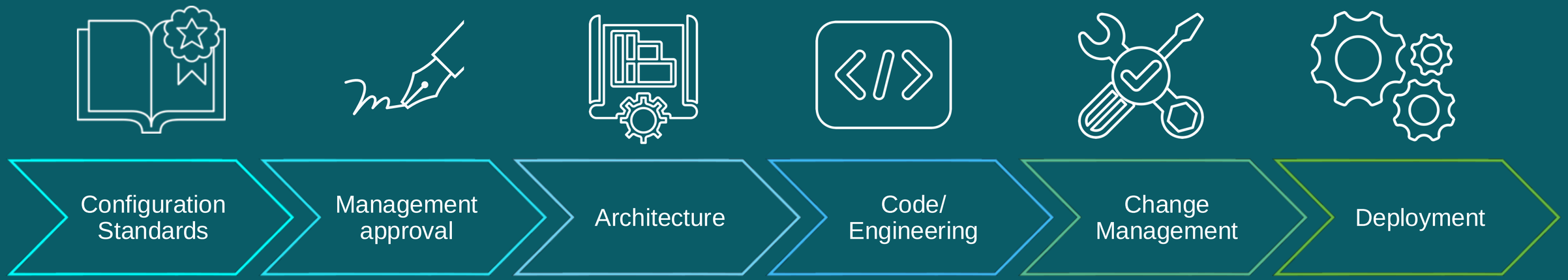
Cloud Considerations and Scope Validation



PCI Security Standards Council®

blackfoot cybersecurity

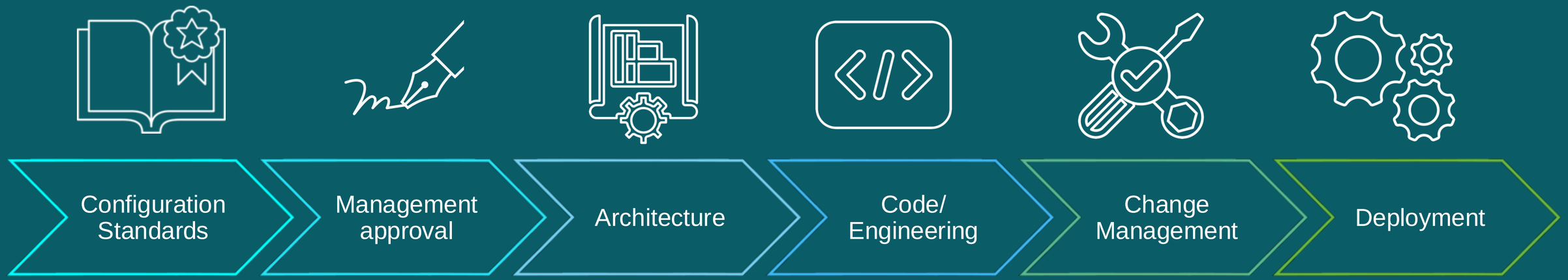
Steps to Infrastructure as Code



PCI Security Standards Council®

blackfoot cybersecurity

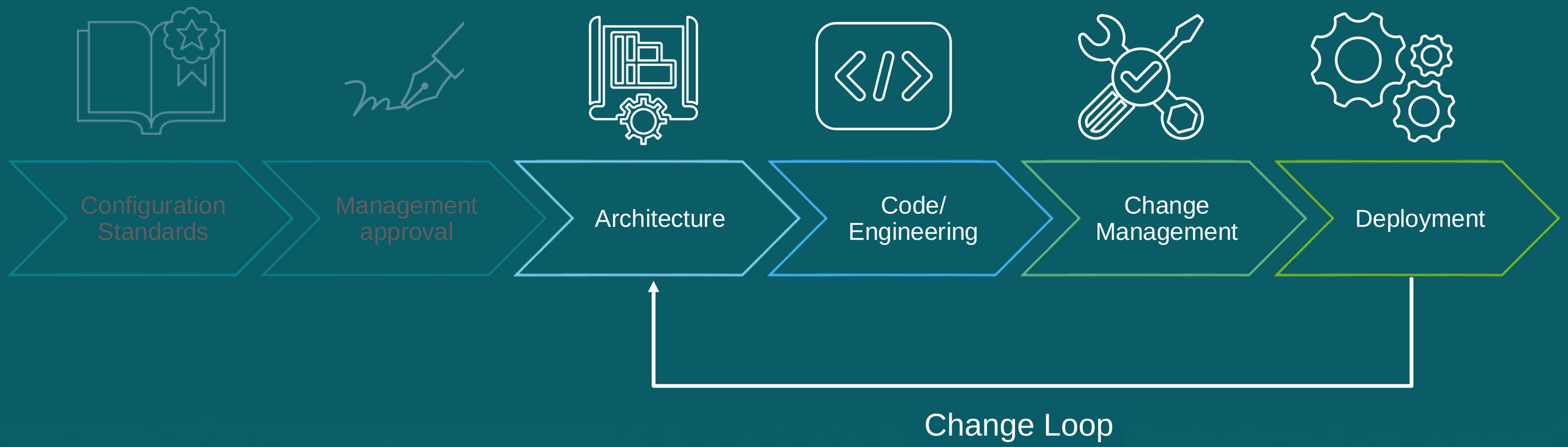
Steps to Infrastructure as Code



PCI Security Standards Council®

blackfoot cybersecurity

Steps to Infrastructure as Code



PCI Security Standards Council®

blackfoot cybersecurity

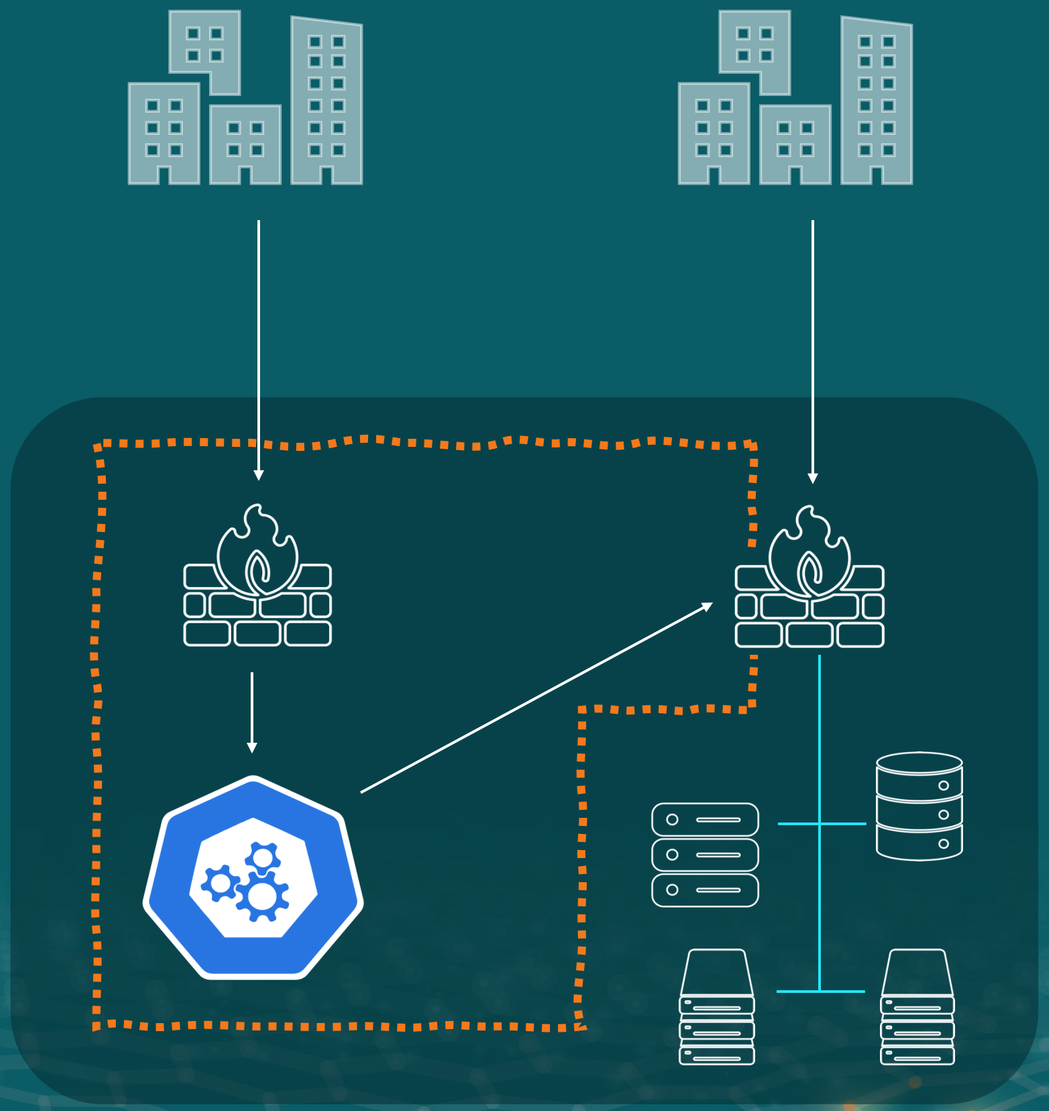
Pop Quiz | Ask a QSA

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



PCI Security Standards Council®

blackfoot cybersecurity

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

PCI Security Standards Council®

blackfoot cybersecurity

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

PCI Security Standards Council®

blackfoot cybersecurity

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

PCI Security Standards Council®

blackfoot cybersecurity

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

PCI Security Standards Council®

blackfoot cybersecurity

Ongoing Considerations

PCI Security Standards Council®

blackfoot cybersecurity

Ongoing Considerations

PCI DSS SCOPE

SIGNIFICANT CHANGE

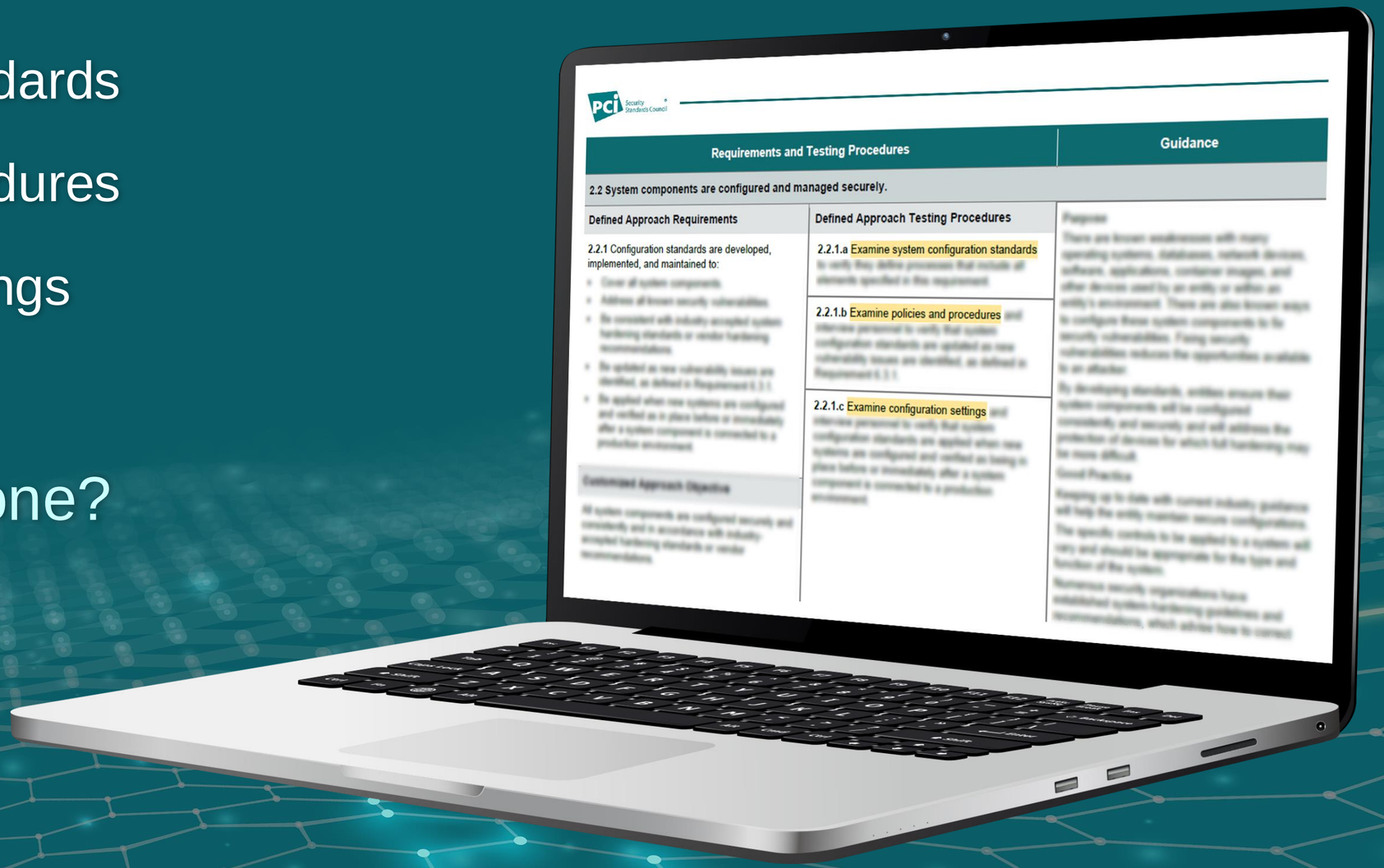
PCI Security Standards Council®

blackfoot cybersecurity

IaC (Relationship) with PCI DSS Requirements

- Configuration Standards
- Policies and Procedures
- Configuration Settings

Where has IaC gone?



PCI Security Standards Council

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)

PCI Security Standards Council®

blackfoot cybersecurity

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)

PCI Security Standards Council®

blackfoot cybersecurity

Infrastructure as Code – Considerations for PCI DSS

PCI Security Standards Council®

blackfoot cybersecurity

Infrastructure as Code – Considerations for PCI DSS

PCI Security Standards Council®

blackfoot cybersecurity

Infrastructure as Code – Considerations for PCI DSS

PCI Security Standards Council®

blackfoot cybersecurity

Key Takeaways

Requirements
6.5 & 12.5

Assessment Time

Direct Component
Review

PCI Security Standards Council

blackfoot cybersecurity

Key Takeaways

Requirements
6.5 & 12.5

Assessment Time

Direct Component
Review

PCI Security Standards Council

blackfoot cybersecurity

John Bloomfield

Manager, Data Security Standards
PCI Security Standards Council

PCI Security Standards Council®

Peter O’Sullivan

QSA, Principal Information Security Consultant
Blackfoot Cybersecurity

blackfoot cybersecurity

blackfoot cybersecurity

PCI Security Standards Council®

Security Standards Council®