PCI S3 Audit Readiness Approach & Best Practices

Suraj Gyawali

Community Meeting 2023
Europe
25-Oct-2023

Suraj GYAWALI

Introduction

12+ years leading PCI Compliance program – PCI DSS, PCI PA-DSS and PCI SSF

Led development and delivered enterprise level payment application used by biggest banks in the world including US, UK, AUS.

Trained 20+ internal product teams, transitioning from PCI PA-DSS to PCI SSF

Led 5 products to get PCI SSF (S3) validation across two large corporations

MSc Software Engineering (Security), Certified Ethical Hacker

Areas of interest are SDLC, Cryptography, Threat modelling & Security Testing

Sr. Solution Engineering Manager

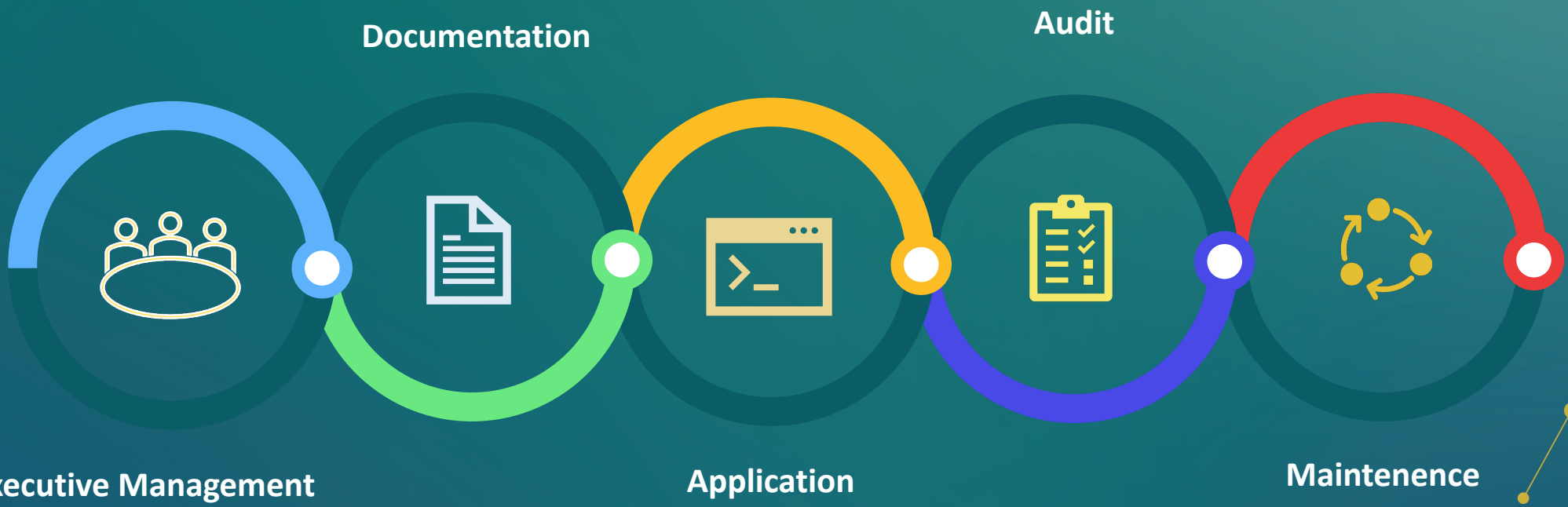
Evo Payments

PCI Security Standards Council

Agenda

PCI Security Standards Council

The Approach



PCI Security Standards Council

Executive Management

Getting management onboard

- Concept of Software Security Framework – Secure SLC & Secure Software Standard (S3)
- Agility built into the SSF framework
- Delta changes
- Project plan and resource planning
- PCI Secure SLC strategy

PCI Security Standards Council

Documentation

Crucial during transition

- Gap Analysis Document
- Critical Assets Register
- Technical Guide – Orange Book
- Software Vendor Implementation Guide

PCI Security Standards Council

Critical Assets Register (CAR)

Sensitive Data Inventory

- Sensitive Data
- Retention Period
- Data-At-rest, Data-In-flight and Data-In-Transit
- Crypto Functions
- Class & Packages
- Data Classification

PCI Security Standards Council

Orange Book

Confidential Technical Guide

- Focus on documenting control objectives specific ask
- Cryptography implementation details
- Access to sensitive data

PCI Security Standards Council

Application

Readiness of Application under test

- Entropy requirements
- Initial Vector (IV) Generation
- Crypto period monitoring
- Auditing sensitive data
- Integrity checks

PCI Security Standards Council

Audit

Learning & Doing

- Planned for several interactions with SSF Assessor
- Evolving compliance
- Learning curve for the industry, service providers, and software vendors

PCI Security Standards Council

Maintenance

Life Cycle of PCI S3 Compliance

- Build CAR and Orange Book into SDLC Process
- Change management - Impact Analysis
- Governance framework process for PCI SSLC
- Proactive to adapt applicable PCI S3 compliance modules

PCI Security Standards Council

Thank you.

If you would like to get a sample of CAR template, ask questions or comment email me on **ssuurraajj@gmail.com**

PCI Security Standards Council