PCI Security Standards Council

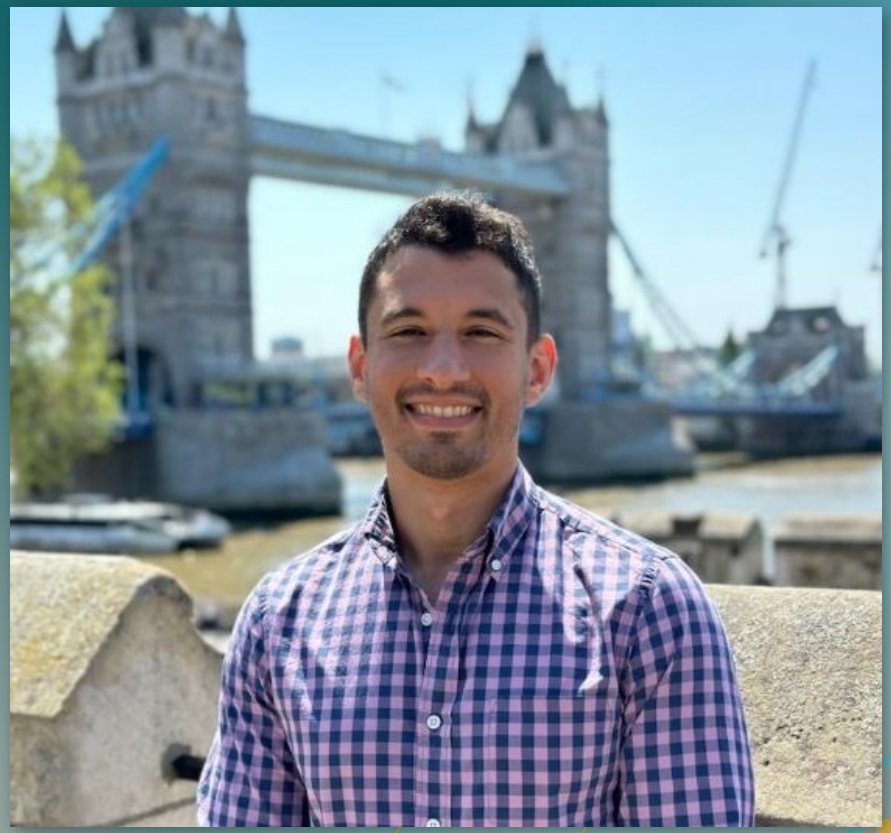
Scaling your Small Business

Building a Strong Security Framework that includes PCI DSS Compliance

Introduction

Marc Rubbinaccio, CISSP, CISA

Manager, Compliance - Secureframe



PCI Security Standards Council

Key Takeaways

Understand **common pitfalls** when meeting or maintaining PCI DSS compliance

Deep dive **actionable solutions** to establishing strong security framework

Discuss specific **services and tools** within cloud services to meet PCI DSS requirements

PCI Security Standards Council

Setting the stage

The business
is **growing fast**

PCI DSS
is now **required**

How do we get
compliant fast?

PCI Security Standards Council

Pitfalls to Acknowledge

- What is PCI DSS?
- Pitfalls
  - Subject matter knowledge
  - Budget
  - Lack of planning
  - Continuous monitoring

PCI Security Standards Council

Let's get Started!

Resources

- PCI DSS v4.0
  - Quick Reference Guide
  - Prioritized Approach
  - Summary of changes
- Guidance for PCI DSS Scoping and Segmentation v1.1
- PCI SSC Cloud Guidelines v3

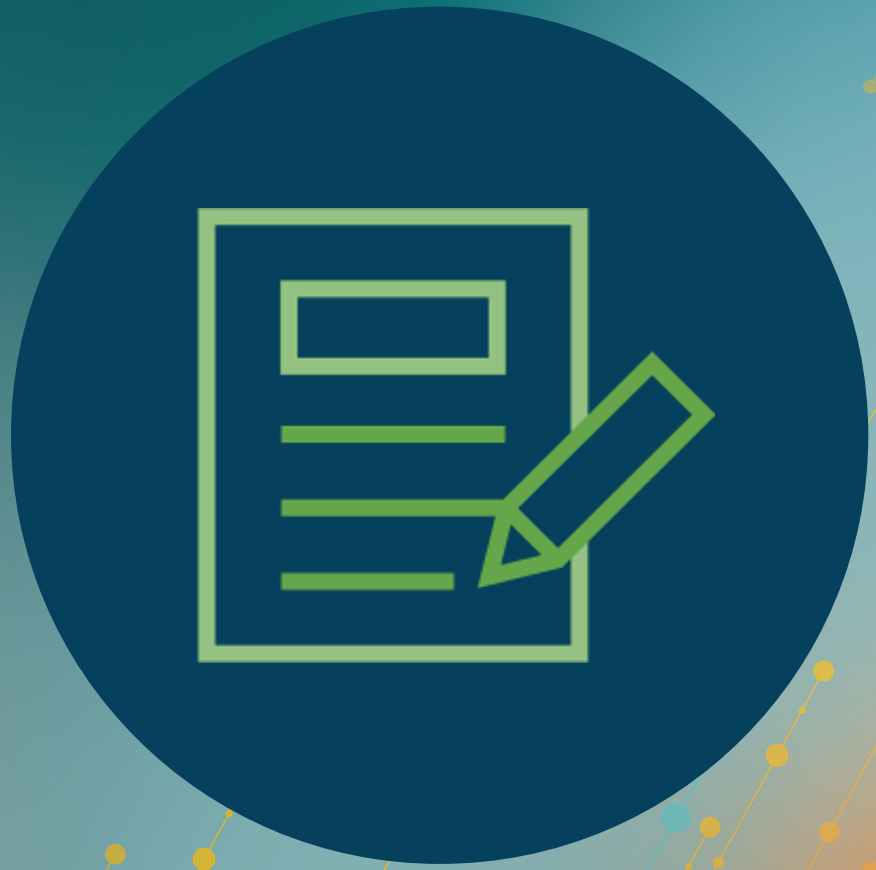
Kicking things off

- Determine your level of compliance
- Verify PCI DSS Scope
- Review controls to determine additional costs
- Perform project planning

PCI Security Standards Council

Operational Controls

- Policies and Procedures
- Onboarding and Offboarding
- Change Management
- Risk Management
- Regular Reviews



PCI Security Standards Council

Technical Controls

- **Segmentation**
- **Security Services**
  - Access management (Requirement 7,8)
    - IAM
  - Network ports, protocols, and rules (Requirement 1)
    - Security Groups

PCI Security Standards Council

Technical Controls Continued

Security Services - Continued

- Internal vulnerability scanning (Requirement 11)
  - Cloud Scanning
- Logging and monitoring (Requirement 10)
  - Centralized log monitoring and notifications
- Threat Detection (Requirement 11)
  - Intrusion detection and Inspection
- Data Loss Prevention (Nice to have)
  - DLP technology
- Encryption Key Management (Requirement 3)
  - Key Management Services
- Web Application Firewall (Requirement 6)
  - WAF

PCI Security Standards Council

What's Next?

Current State

- Reviewed and completed prioritized approach
- Implemented operational and technical controls

Next Steps

- Level 1 (or 2) - Schedule an audit with a QSA firm
- Level 3 (or 4) - Consult with a QSA

Assessment Process

- Scoping discussions
- Evidence review, interviews, observations
- Remediation and QA

PCI Security Standards Council

Maintain PCI DSS Compliance

Daily security event and log monitoring

Weekly file comparisons

Every 6 months - user access review

Every 6 months - firewall rule review

PCI DSS Scope validation

Semi-annual segmentation testing

(service provider)

Quarterly ASV scanning

Regular risk analysis

Annual security awareness trainings

Reviews and approvals on all changes

Penetration testing

Significant change management

Security incident response exercise

Vendor due diligence

Monitor third party access

Quarterly internal vulnerability scanning

PCI Security Standards Council

Thank you!

- Marc@secureframe.com
- https://www.linkedin.com/in/marcrubbinaccio/

PCI Security Standards Council