PCI Security Standards Council

# Aligning Continuous Vulnerability Management with Risk and Compliance

PCI Security Standards Council

# Randall Laudermilk

VP, Product Strategy and Strategic Partners, USA Region; CSM, CSPO

CARSON & SAINT

# Agenda

## Aligning Continuous Vulnerability Management with Risk and Compliance

- About Carson & SAINT
- Challenges of managing VA, risk and compliance
- PCI DSS v4.0 – Roadmap to alignment
- Key elements of aligning these programs
- Benefits of alignment
- Wrap Up

PCI Security Standards Council®

# About Carson & SAINT

- Headquarters in the US
- Over 25 Years in Cyber security industry
- Over 14,000 customers in 20+ countries
- Product and Services portfolio
- Partner programs


Website: https://www.carson-saint.com

Follow Us on Social Media:

https://twitter.com/Carson__SAINT

https://www.linkedin.com/company/carsonsaint

PCI Security Standards Council®

# VA, Risk and Compliance

## Challenges - Key Differences

- Vulnerability Management
  - Tactical in nature
  - Find exposures
  - Identify and prioritize remediation
- Compliance
  - Industry standard
  - Framework (what, not how-to)
- Risk Management
  - Strategic focus
  - Protect most critical assets
  - Business continuity


PCI Security Standards Council

***Business Impact + Severity/Probability = RISK***

# VA, Risk and Compliance

## Challenges - managing them separately

- Expensive
- Redundancy
- Conflicting priorities
- Inefficient
- Separate outcomes – no alignment
- No stakeholder buy-in
- Compliance is forced versus a natural outcome


PCI Security Standards Council®

# PCI DSS v4.0

## Roadmap to alignment

- Requirement 2 - Secure configurations to ALL system components
- Requirement 5: Protect ALL Systems/Networks from Malicious Software
- Requirement 6.3.1 – "…managing vulnerabilities should be integrated with other mgt processes"
- Requirement 6.4.1 – Vuln and risks to web apps
- Requirement 11.3.1.1 – Regular security testing
- Requirement 12.3 - Risks to the CDE… (TRAs)
- Requirement 12.6.3.1 – Phishing/Social Eng.
- Requirement 12.9.2 – 3rd Party Service Providers


PCI Security Standards Council

***Business Impact + Severity/Probability = RISK***

# Aligning VA, Risk and Compliance

## Include measures for all key Stakeholders

- Vulnerability Management
  - IP, MAC, hostname, CVE, CVSS, Threat
- Compliance
  - Industry (PCI)
  - Standard (DSS)
  - Control (assist in targeted risk analysis)
  - Purpose
- Risk
  - Critical Assets
  - Sensitive Data
  - Function
  - Location
  - Owner


**Critical Assets Risk**

CSV XML Page 1 of 1 10 View 1 - 5 of 5

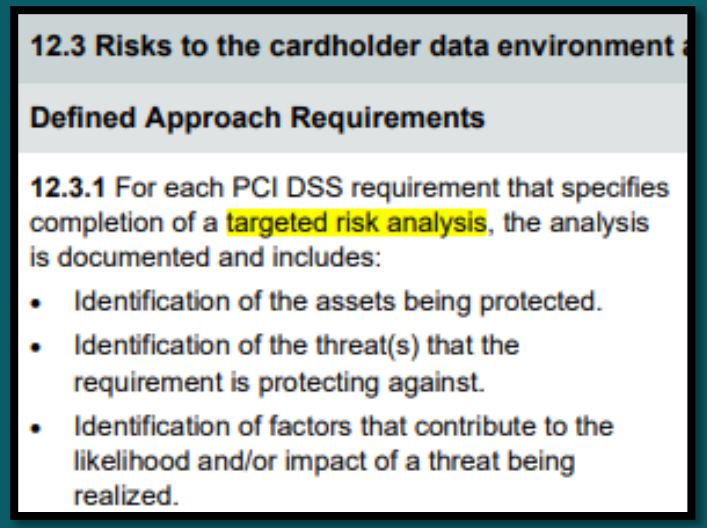
| Risk Level | Criticality | PCI - Function | Internet Facing | Sensitive Data | Location | Function | Hostname | CVSSv3 Critical | CVSSv3 High | CVSSv2 Medium | Total Vulnerabilities |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Critical | Critical | Testing | No | Yes | Denver | Testing | xpprounpatch | 18 | 104 | 51 | 345 |
| Critical | Critical | Customer DB | No | Yes | Naples | Database | ip-10-9-0-135 | 38 | 20 | 26 | 113 |
| High | Critical | eCommerce | Yes | No | Tuscany | eCommerce | ip-10-9-0-97.e | 20 | 20 | 14 | 64 |
| High | Critical | eCommerce | Yes | No | Rome | eCommerce | ip-10-9-0-214 | 7 | 2 | 2 | 23 |
| Low | Critical | Load Balancer | Yes | No | Milan | Infrastructure | ip-10-9-0-2.ec | 0 | 0 | 0 | 4 |

PCI Security Standards Council

# Aligning VA, Risk and Compliance

Aligned measures contribute to the TRA

1. Identify critical assets; align to the business.
2. Map assets to CDE to support TRA.
3. Identify Stakeholders and their role(s).
4. Identify 3rd party vendors and supply chain that connect to critical systems.
5. Implement VA and Pentesting to assess and verify exposures.
6. Verify state of malware tools
7. Phishing testing as well as prevention.
8. Measure outcomes by risk – not just severity.
9. Focus resources and response on business risk and TRA.
10. Outcomes feed TRA



**12.3 Risks to the cardholder data environment**

**Defined Approach Requirements**

**12.3.1** For each PCI DSS requirement that specifies completion of a targeted risk analysis, the analysis is documented and includes:

- Identification of the assets being protected.
- Identification of the threat(s) that the requirement is protecting against.
- Identification of factors that contribute to the likelihood and/or impact of a threat being realized.

PCI Security Standards Council

# Aligning VA, Risk and Compliance

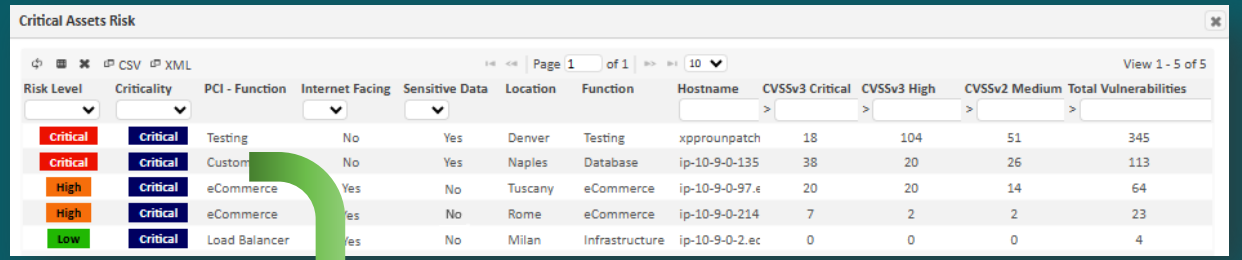
## Use common language to implement controls

**12.3 Risks to the cardholder data environment**

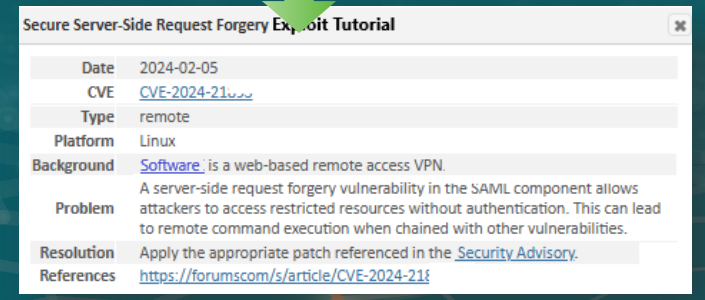
**Defined Approach Requirements**

**12.3.1** For each PCI DSS requirement that specifies completion of a targeted risk analysis, the analysis is documented and includes:

- Identification of the assets being protected.
- Identification of the threat(s) that the requirement is protecting against.
- Identification of factors that contribute to the likelihood and/or impact of a threat being realized.








PCI Security Standards Council®

# Benefits of Aligning VA, Risk and Compliance

1. Cost reduction
2. Risk-based VA aligns to TRA
3. Eliminate redundancy
4. Better communication, decision making and response.
5. Increase stakeholder confidence
6. Encourages continuous improvement through feedback between programs and stakeholders.

# Key Takeaways

1. PCI DSS v4.0 emphasized continuous security.
   - The DSS is not only a standard. It is a framework.
2. Vulnerability Management programs must evolve to vulnerability risk management.
3. Human Weaknesses cannot be overlooked.
4. 3rd Party Vendor/Supply Chain risks pose unique exposures.
5. Alignment feeds Targeted Risk Analysis
   - Protecting the CDE and reducing costs of TRAs


PCI Security Standards Council

# Questions

Thanks for joining us today

Visit us at Booth 39


PCI Security Standards Council