RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: GRC-R03

NIST Cybersecurity Framework and PCI DSS

Troy Leach
Chief Technology Officer
PCI Security Standards Council

Emma Sutcliffe
Senior Director, Data Security Standards
PCI Security Standards Council

PCI Security Standards Council

We Help Secure Payment Data

- Global, cross-industry effort to increase payment security
- Industry-driven, flexible and effective standards and programs
- Helping businesses detect, mitigate and prevent criminal attacks and breaches

PCI Security Standards and Programs

Standards, Training and Certification Programs, Educational Resources

Payment **Equipment**

Payment **Software**

Merchant & Payment Service Provider **Environments**

Certification – Equipment, Service Providers, Assessors, Investigators

Training – Assessors, Investigators

PCI DSS and the NIST Cybersecurity Framework

- Applies wherever payment card data is stored, processed or transmitted
- Provides a baseline of technical and operational requirements
- Focused on the protection of payment card data

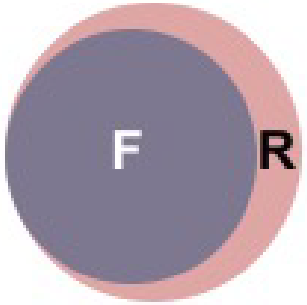
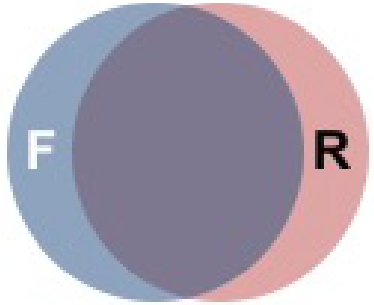
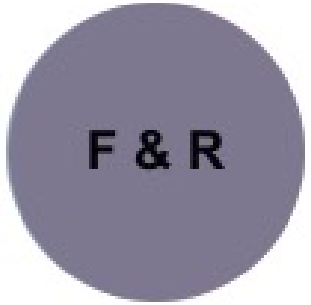
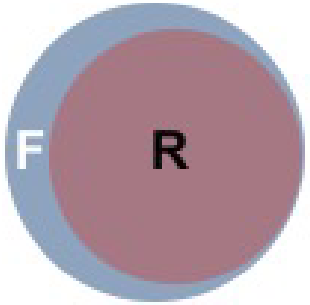
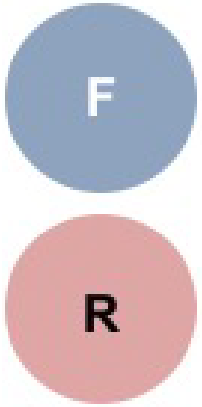
- Voluntary Framework for managing cybersecurity-related risk
- Consists of standards, guidelines, and best practices
- Promotes the protection and resilience of critical infrastructure

Standard vs. Framework

Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Mapping Relationships

Case 1	Case 2	Case 3	Case 4	Case 5
Subset of	Intersects with	Equivalent to	Superset of	Not related to
				

Observations from Mapping Exercises

- Both PCI DSS and the NIST CSF provide a comprehensive approach to security
- Mapping results are not exact matches
- Controls used to meet PCI DSS can contribute to meeting CSF, and vice versa
- Meeting either PCI DSS or the CSF does not result in the other being met

Example Mappings – Equivalence

NIST CSF (ID.AM-3)

- Organizational communication and data flows are mapped

PCI DSS (Req. 1.1)

- Network diagram that identifies all connections to/from CDE (Req. 1.1.2)
- Diagram that shows all cardholder data flows (Req. 1.1.3)

Example Mappings – Subset

NIST CSF (PR.DS-7)

- The development and testing environment(s) are separate from the production environment

PCI DSS (Req. 6.4)

- Separate development/test environments from production environments, enforce with access controls (Req. 6.4.1)
- Separation of duties between development/test and production environments (Req. 6.4.2)

Example Mappings – Intersections

NIST CSF (PR.DS-2)

- Data-in-transit is protected

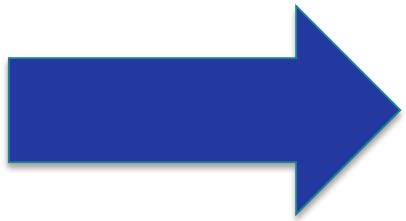
PCI DSS

- Use strong cryptography to protect cardholder data during transmission over open, public networks (Req. 4)
- Use strong cryptography to protect authentication credentials during transmission (Req. 8.2.1)

Mapping View

NIST CSF

- Integrity checking mechanisms are used to verify hardware integrity (PR.DS-8)



PCI DSS (Req. 9.9)

- Devices that capture payment card data are protected from tampering and substitution

Reverse View

NIST CSF

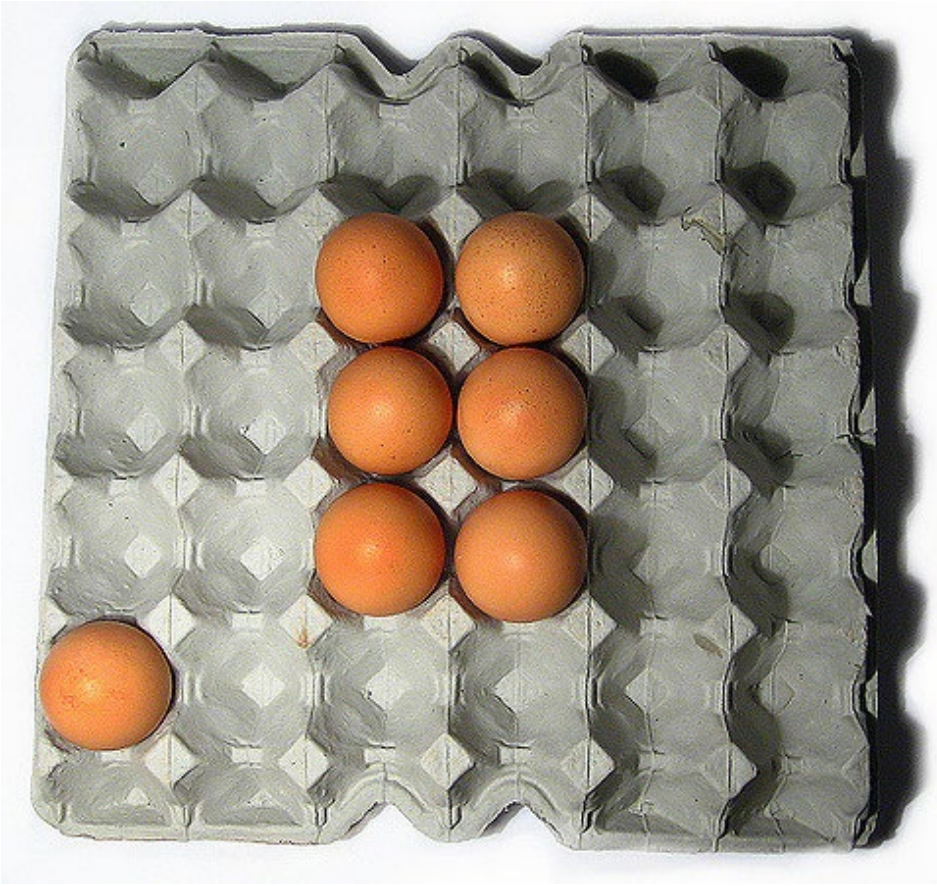
- Integrity checking mechanisms are used to verify hardware integrity (PR.DS-8)
- Physical devices and systems within the organization are inventoried (ID.AM-1)
- All users are informed and trained (PR.AT-1)

PCI DSS (Req. 9.9)

- Devices that capture payment card data are protected from tampering and substitution

Example Mappings – Not Related

- CSF Subcategories
  - Availability
    - Adequate capacity to ensure availability is maintained (PR.DS-4)
    - Systems operate in pre-defined functional states to achieve availability (PR.PT-5)
  - Recovery communications
    - Public relations are managed (RC.CO-1)
    - Reputation after an event is repaired (RC.CO-2)



The Mapping Process

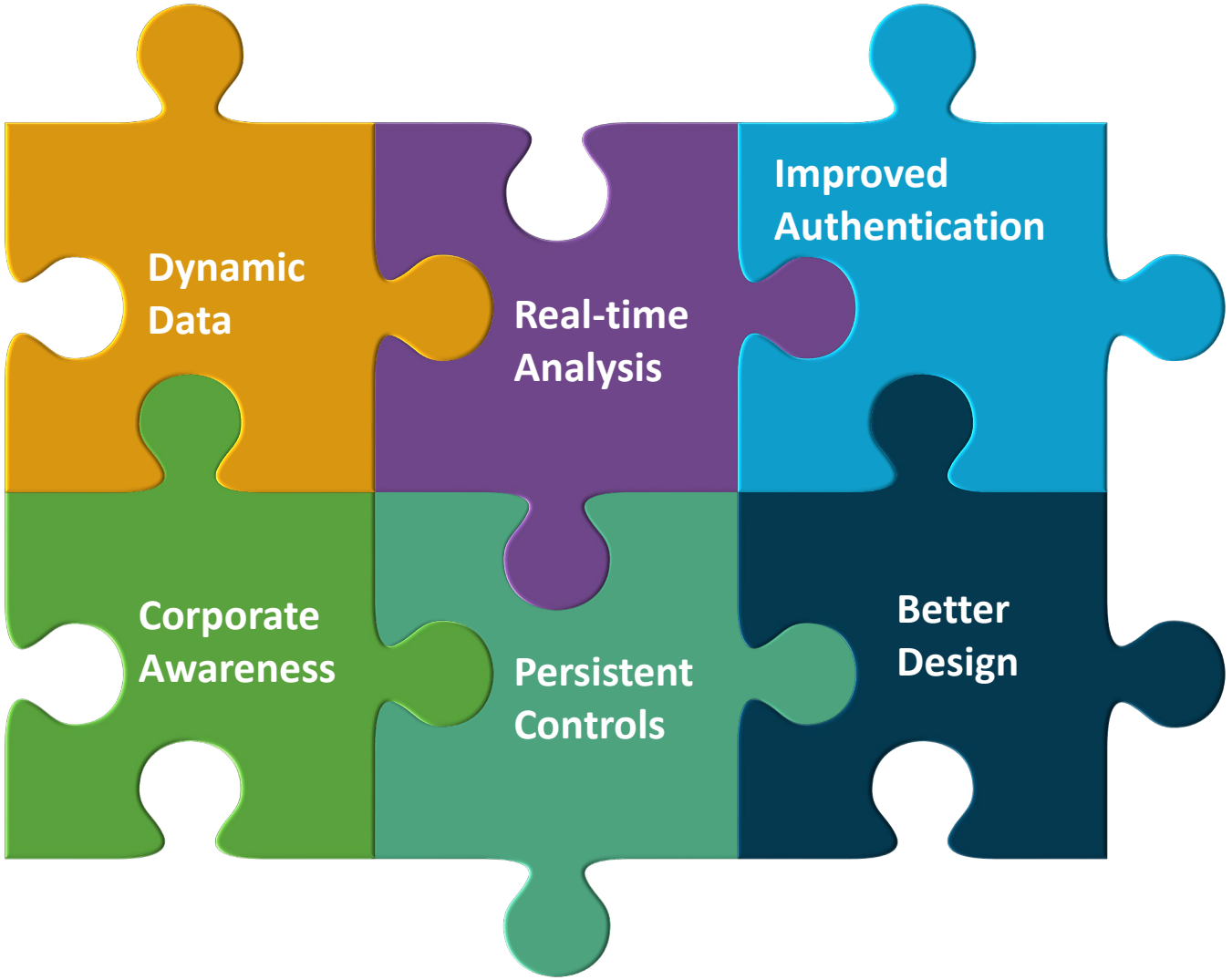
- PCI SSC is the first organization to work with NIST to undertake an exhaustive study on the extent to which another standard fulfills CSF elements
- Process requires a thoughtful approach to mapping

Lessons Learned

- PCI DSS and NIST CSF both offer comprehensive security coverage
- Complementary approaches; one does not supersede need for the other
- NIST mapping shows one-way relationship from the Reference to the CSF
- Achieving CSF outcomes may not result in payment data being protected

RSAConference2019

And PCI is Evolving…..


Dynamic Data
Real-time Analysis
Improved Authentication
Corporate Awareness
Persistent Controls
Better Design

DSS Revision and Future Updates

2018 Revision

Next major release

What We've Heard During Open Feedback Period

Objective Based Requirements

BENEFITS

Suited to organizations with mature risk management programs and robust governance structures

Supports adoption of cutting-edge technologies – organizations finding new ways to meet their security needs

CHALLENGES

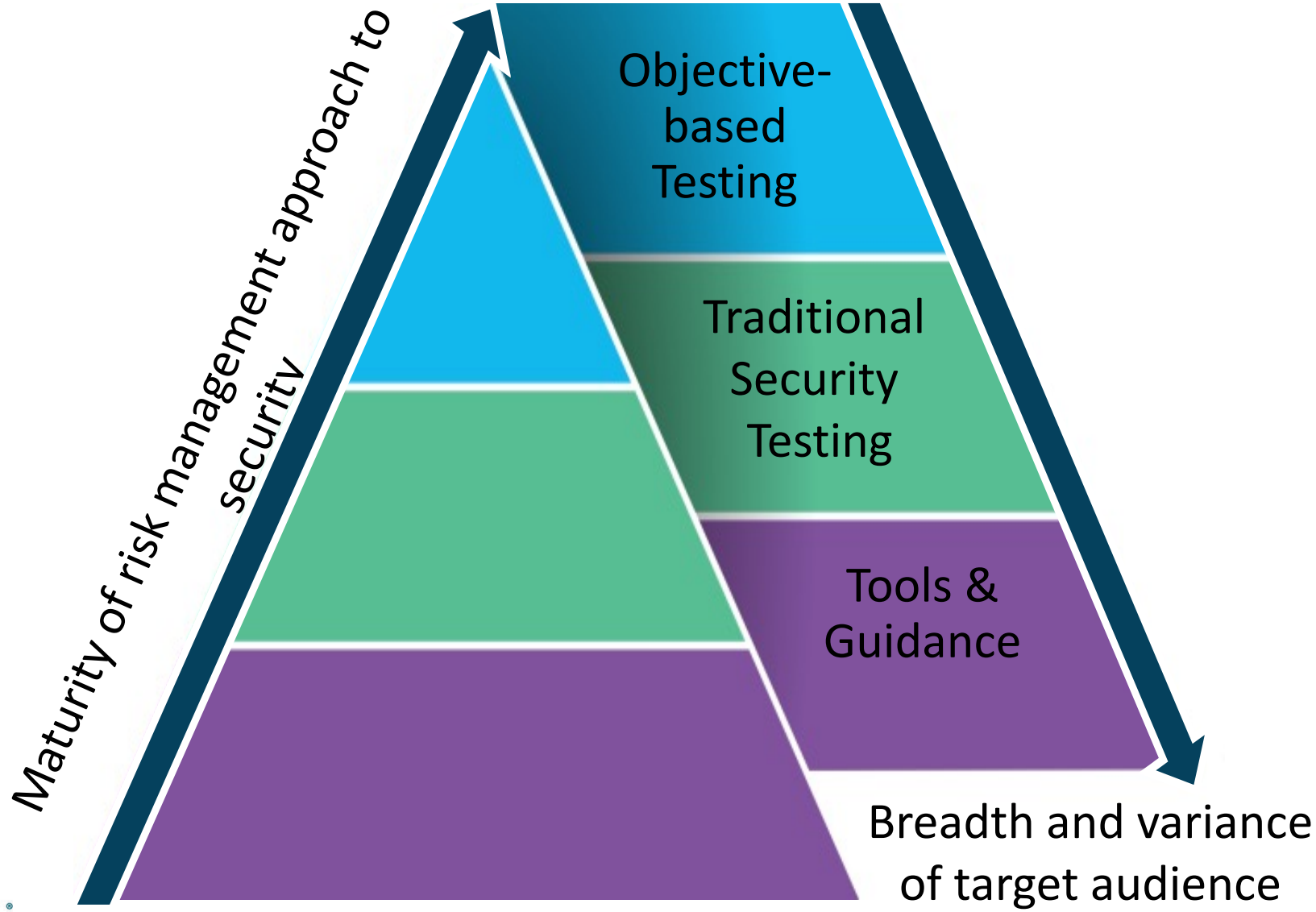
Broader variance between implementations: Greater effort required to validate if security requirements are met

More open to subjective interpretation when evaluating level of security assurance

DSS Potential Goals

- Design security requirements to include objective/outcome-based assessment
- Establish culture for on-going security practices
- Enhance the validation methodology

Security Approach for Different Audiences



TIMELINE FOR DSS V4.0 ENGAGEMENT

Expected 2020 Publication with additional RFCs starting in Fall 2019

Opportunity to Provide Feedback on DSS

<u>New RFC Process for 2019:</u>

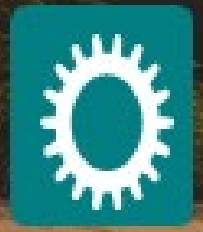
Consistency in approach

Transparency in changes

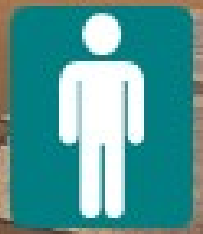
RFC Logistics

Ways to Reduce Footprint

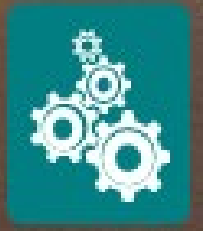
Reduce the need or ability to store or transmit cardholder data



Business process



Outsource



Simplify

Render Unreadable

Apply what you have learned

- Evaluate existing critical assets and properly label their priority to your organization
- Evaluate industry mappings to reduce duplicity of internal assessment
- Stay connected and informed as these frameworks constantly change to reflect new risk

RSAConference2019

Thank You!