EDUCATE
EMPOWER
PROTECT

ASIA-PACIFIC
TOKYO | 14 – 15 OCTOBER

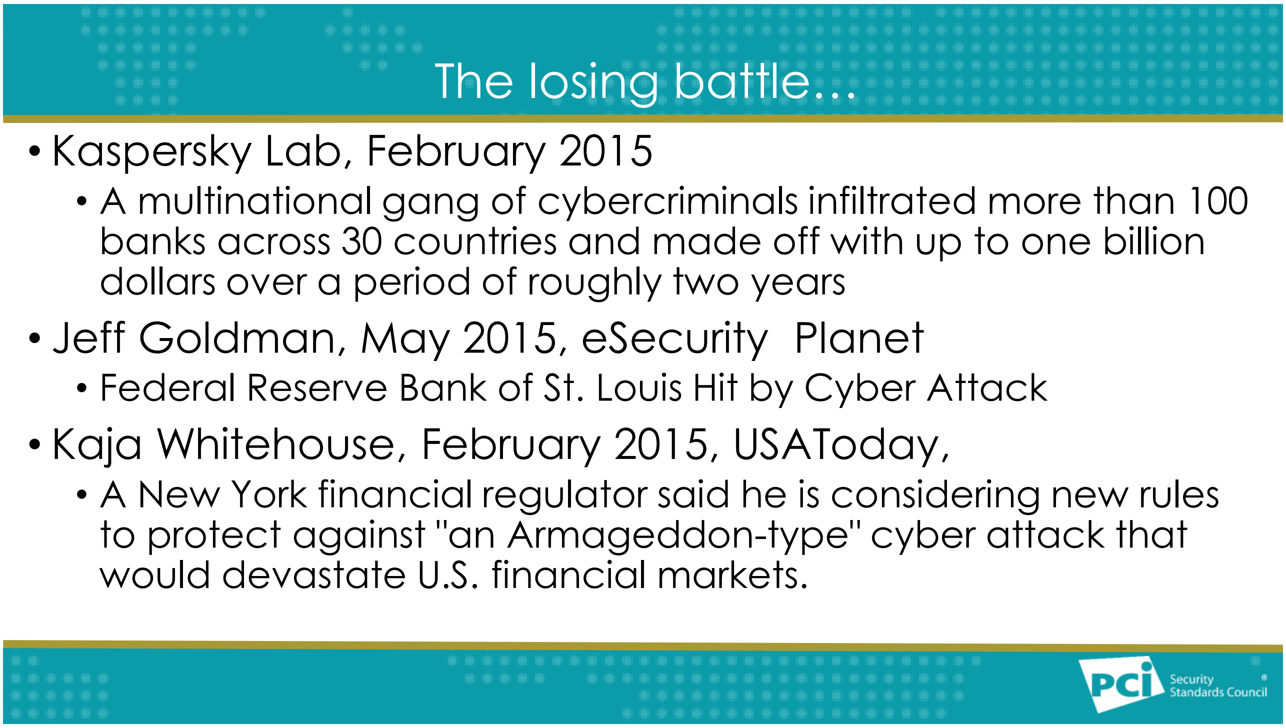
PCI Security Standards Council®

Improving Policy-based Security Specifications

Gordon McIntosh
Principal Security Consultant
atsec information security

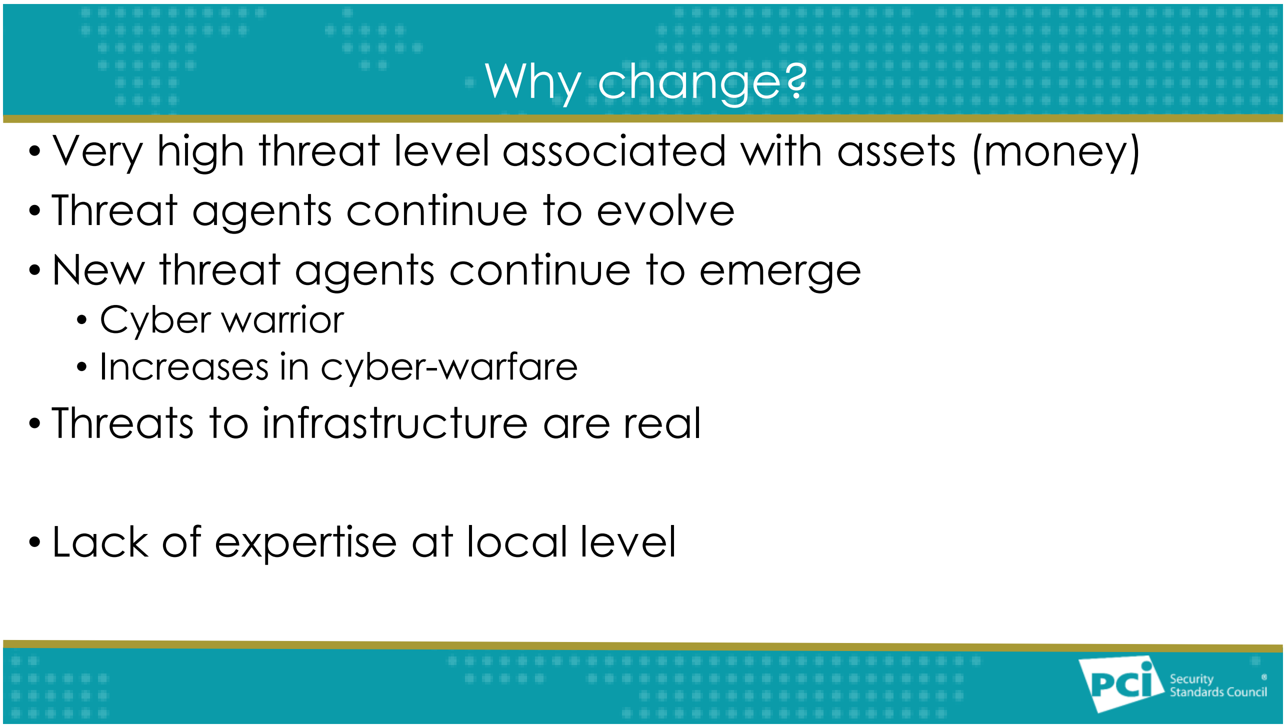
Why?

PCI Security Standards Council®



The losing battle…

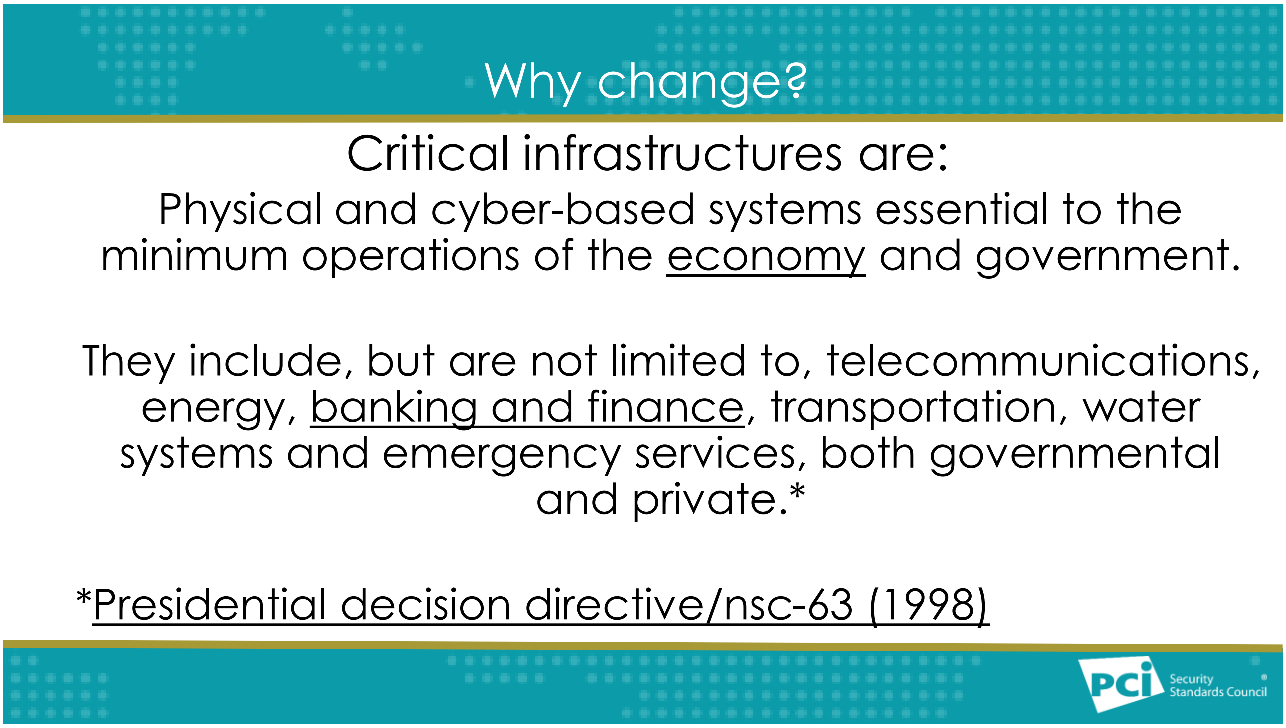
- Kaspersky Lab, February 2015
  - A multinational gang of cybercriminals infiltrated more than 100 banks across 30 countries and made off with up to one billion dollars over a period of roughly two years
- Jeff Goldman, May 2015, eSecurity Planet
  - Federal Reserve Bank of St. Louis Hit by Cyber Attack
- Kaja Whitehouse, February 2015, USAToday,
  - A New York financial regulator said he is considering new rules to protect against "an Armageddon-type" cyber attack that would devastate U.S. financial markets.



Why change?

- Very high threat level associated with assets (money)
- Threat agents continue to evolve
- New threat agents continue to emerge
  - Cyber warrior
  - Increases in cyber-warfare
- Threats to infrastructure are real

- Lack of expertise at local level



Why change?

Critical infrastructures are:

Physical and cyber-based systems essential to the minimum operations of the economy and government.

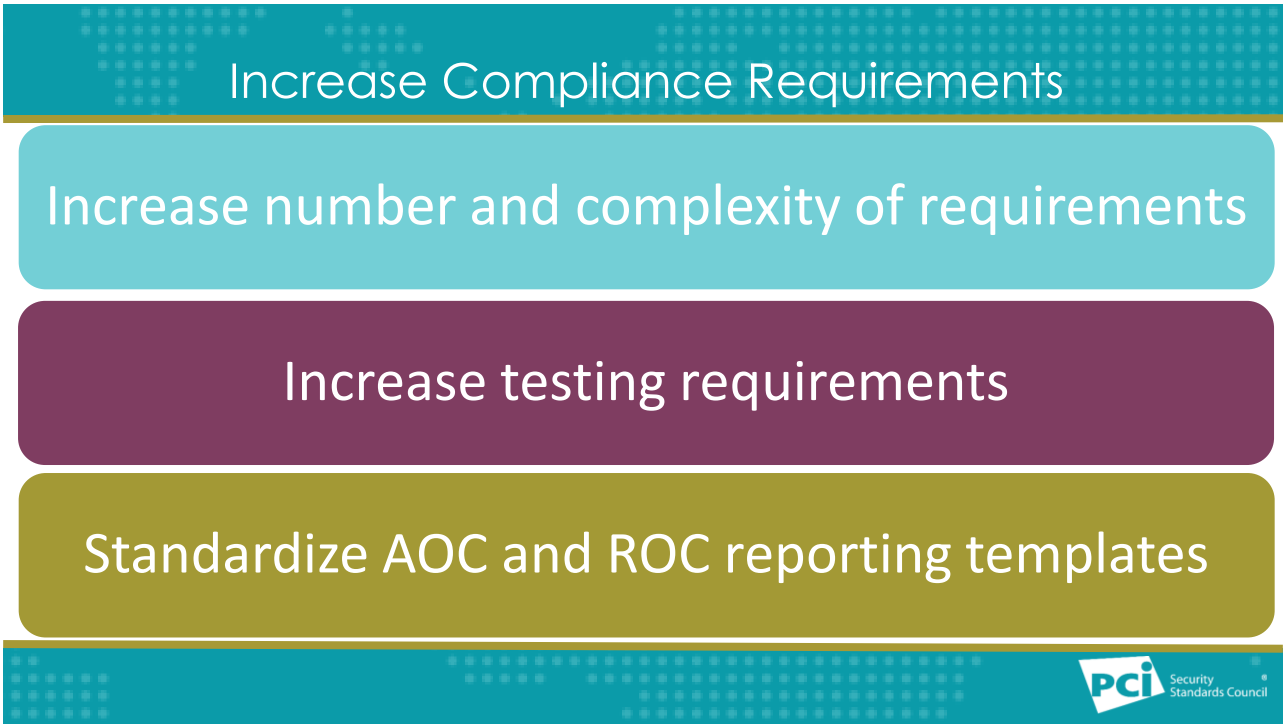
They include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private.*

*Presidential decision directive/nsc-63 (1998)

PCI Security Standards Council

The Current Solution

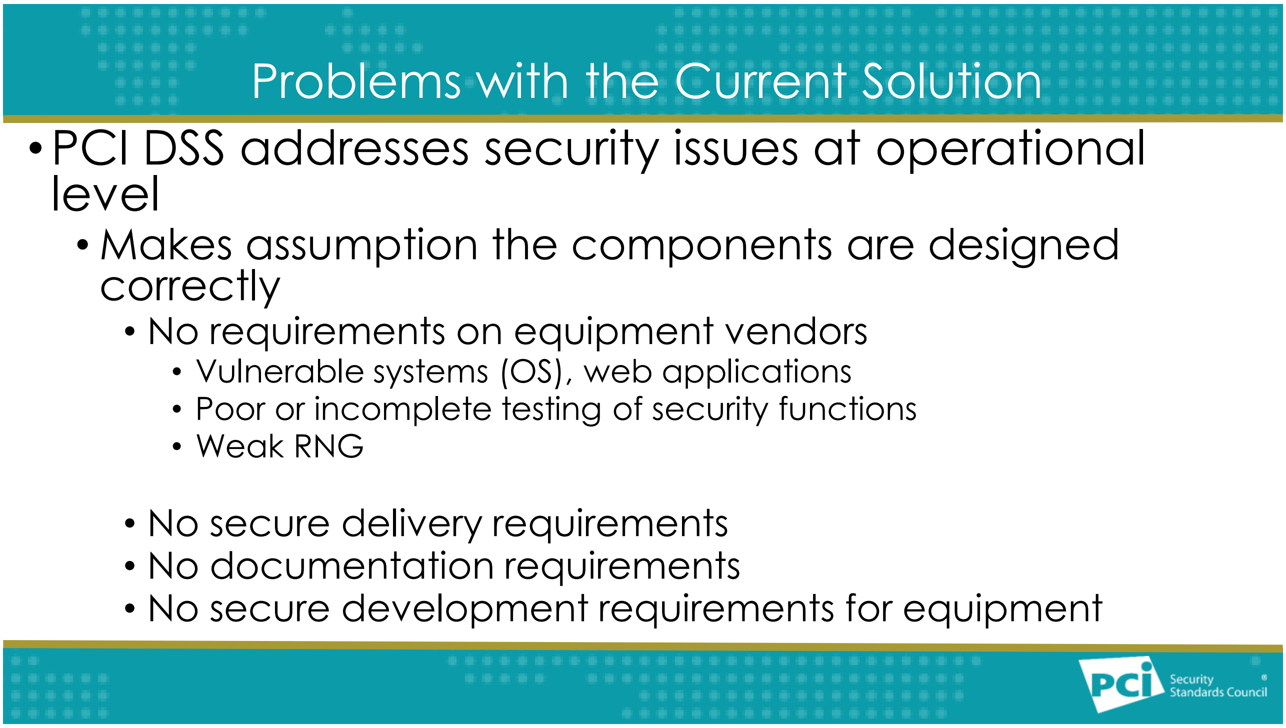
PCI Security Standards Council



Increase Compliance Requirements

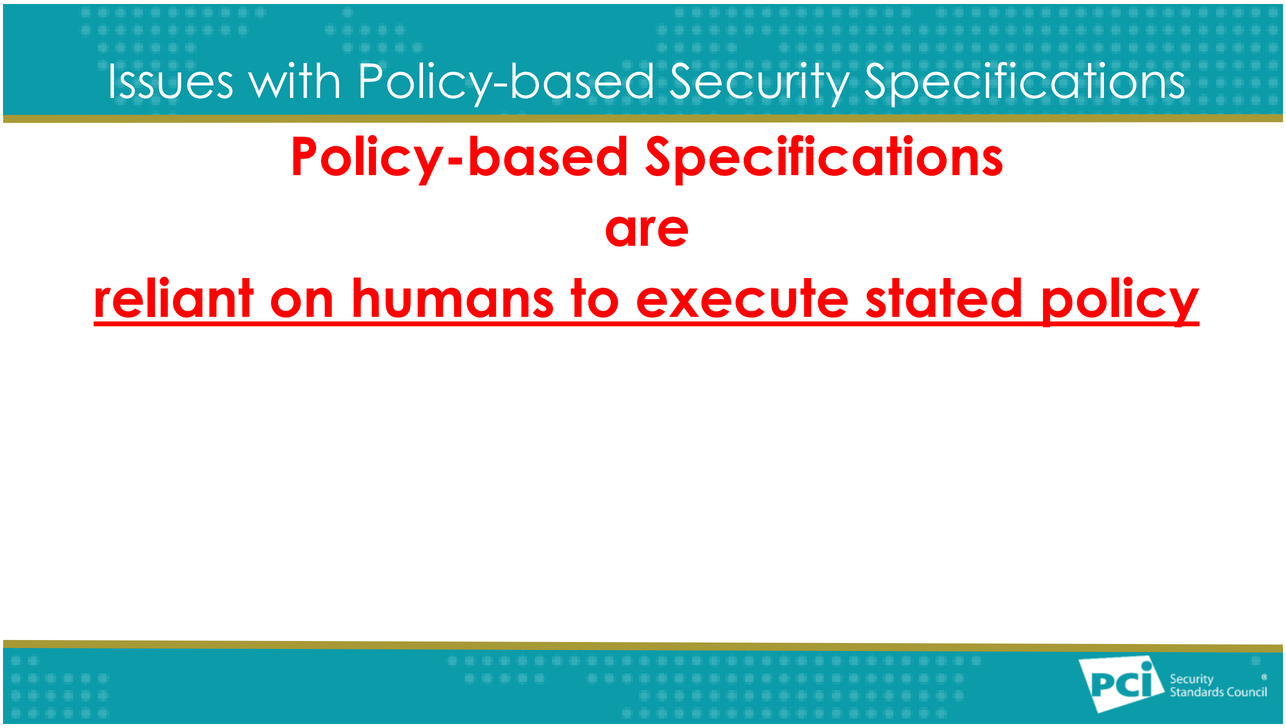
- Increase number and complexity of requirements
- Increase testing requirements
- Standardize AOC and ROC reporting templates

Problems with the Current Solution



Problems with the Current Solution

- PCI DSS addresses security issues at operational level
  - Makes assumption the components are designed correctly
    - No requirements on equipment vendors
      - Vulnerable systems (OS), web applications
      - Poor or incomplete testing of security functions
      - Weak RNG
    - No secure delivery requirements
    - No documentation requirements
    - No secure development requirements for equipment

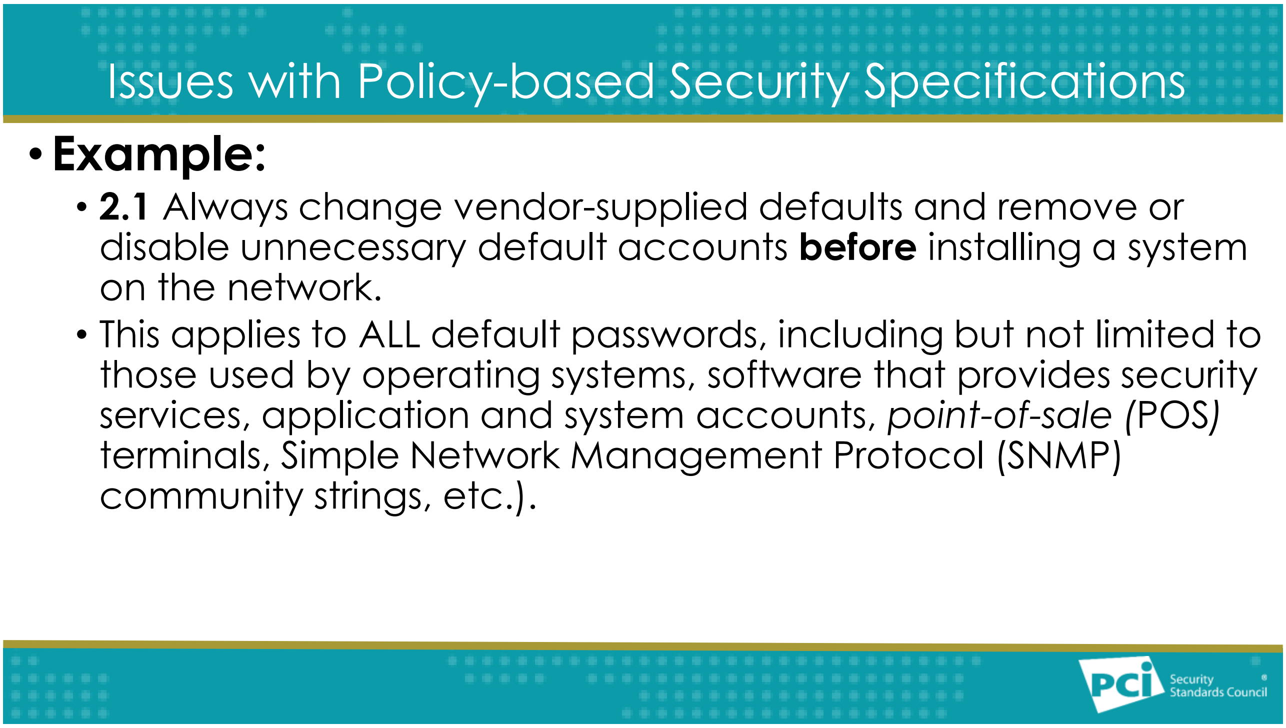


Issues with Policy-based Security Specifications

Policy-based Specifications

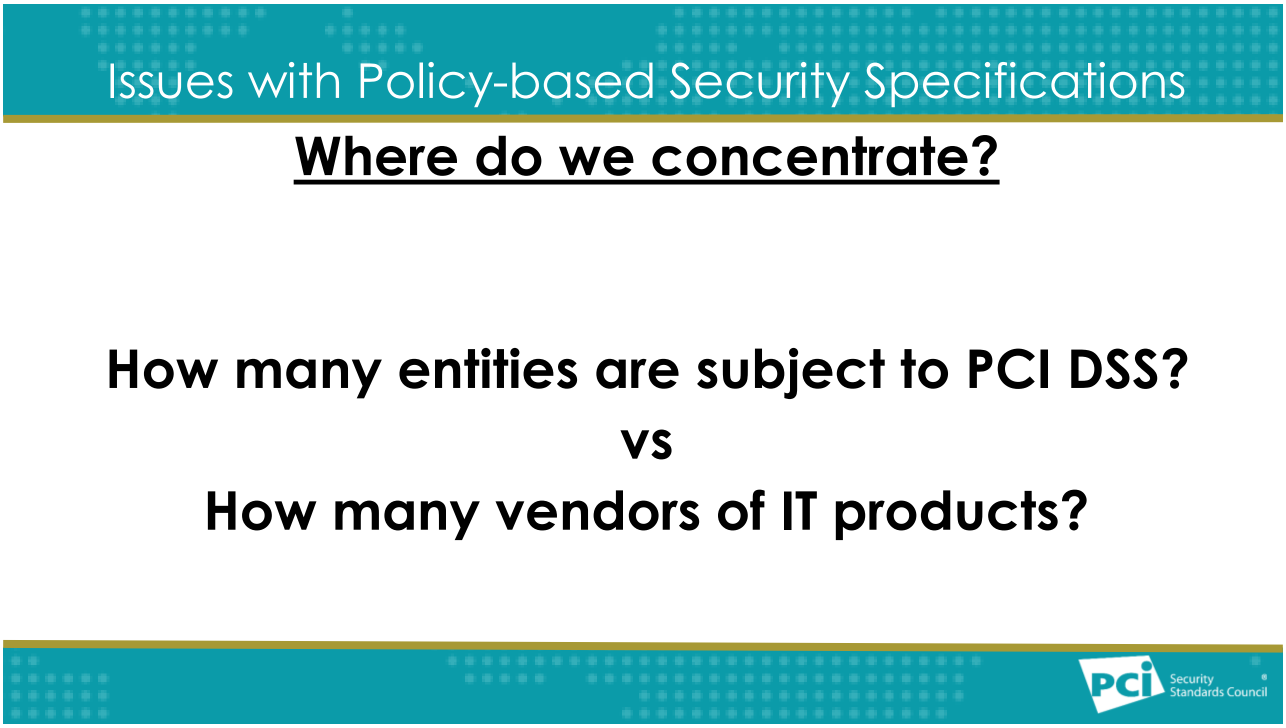
are

reliant on humans to execute stated policy



Issues with Policy-based Security Specifications

- **Example:**
  - **2.1** Always change vendor-supplied defaults and remove or disable unnecessary default accounts **before** installing a system on the network.
  - This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, *point-of-sale* (POS) terminals, Simple Network Management Protocol (SNMP) community strings, etc.).



Issues with Policy-based Security Specifications

Where do we concentrate?

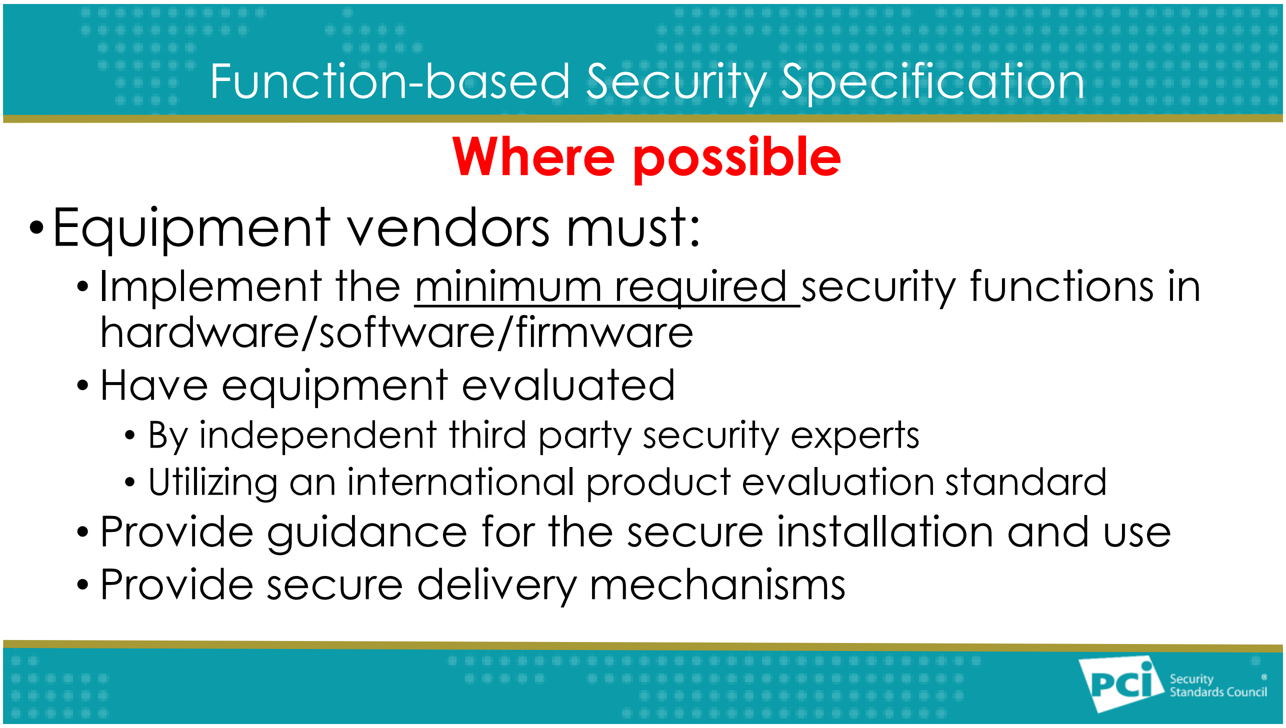
How many entities are subject to PCI DSS?

vs

How many vendors of IT products?

An Alternate Solution

PCI Security Standards Council

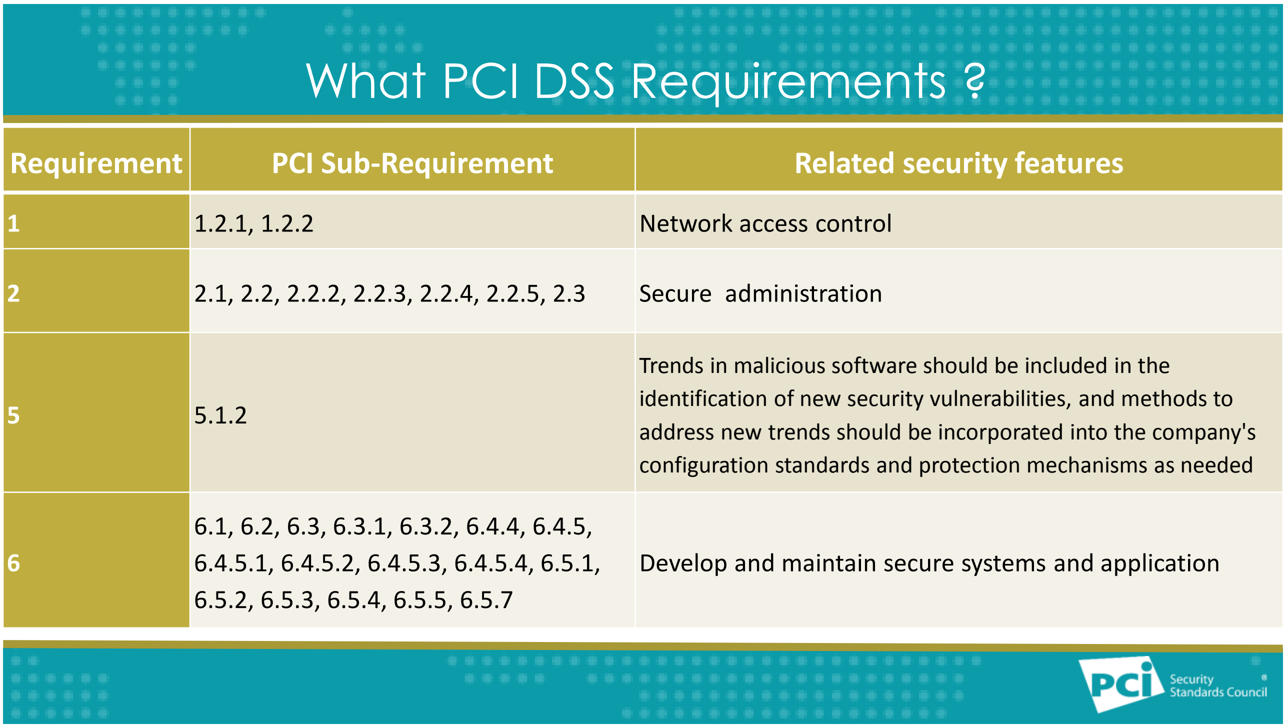


Function-based Security Specification

Where possible

- Equipment vendors must:
  - Implement the minimum required security functions in hardware/software/firmware
  - Have equipment evaluated
    - By independent third party security experts
    - Utilizing an international product evaluation standard
  - Provide guidance for the secure installation and use
  - Provide secure delivery mechanisms

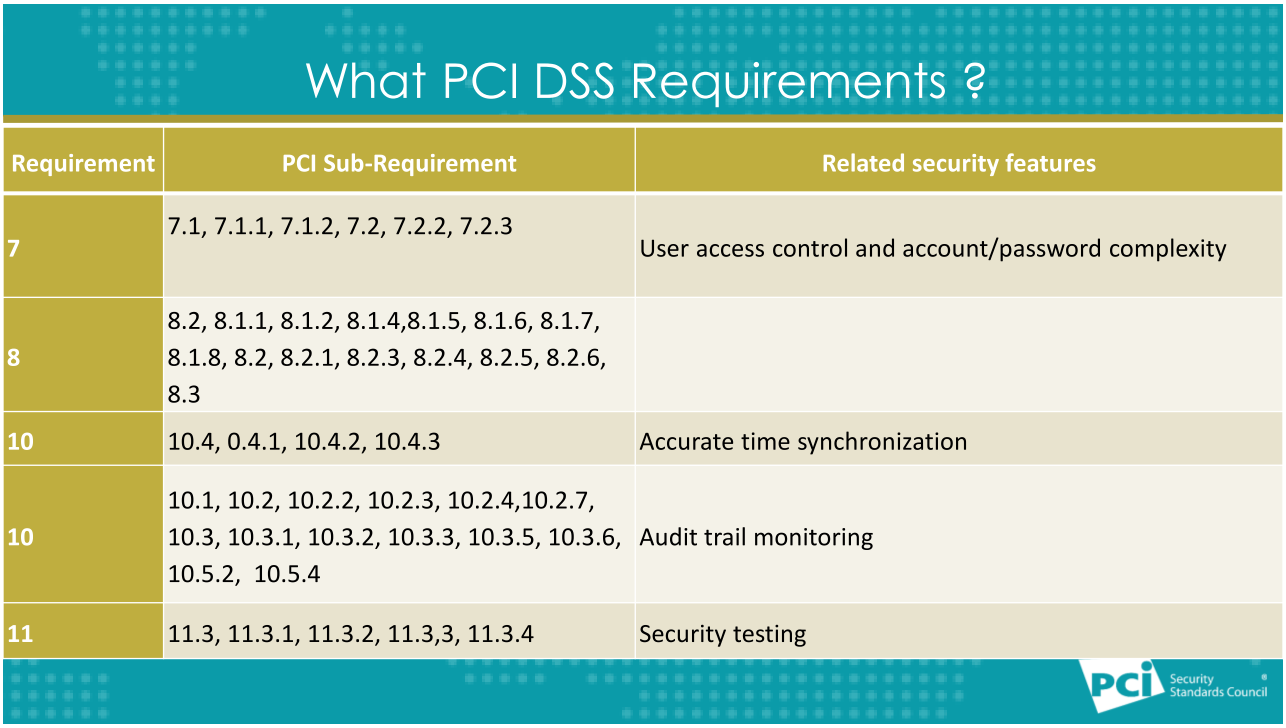
PCI Security Standards Council



What PCI DSS Requirements ?

Requirement	PCI Sub-Requirement	Related security features
1	1.2.1, 1.2.2	Network access control
2	2.1, 2.2, 2.2.2, 2.2.3, 2.2.4, 2.2.5, 2.3	Secure administration
5	5.1.2	Trends in malicious software should be included in the identification of new security vulnerabilities, and methods to address new trends should be incorporated into the company's configuration standards and protection mechanisms as needed
6	6.1, 6.2, 6.3, 6.3.1, 6.3.2, 6.4.4, 6.4.5, 6.4.5.1, 6.4.5.2, 6.4.5.3, 6.4.5.4, 6.5.1, 6.5.2, 6.5.3, 6.5.4, 6.5.5, 6.5.7	Develop and maintain secure systems and application

PCI Security Standards Council



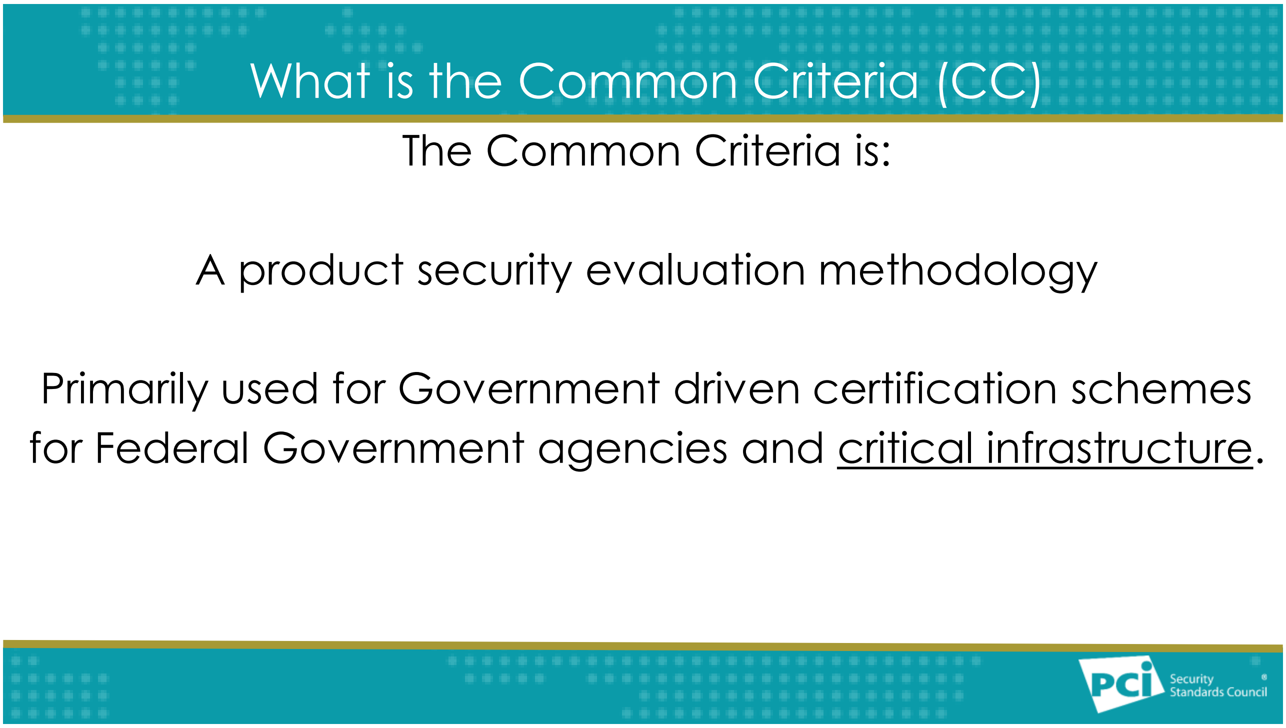
What PCI DSS Requirements ?

Requirement	PCI Sub-Requirement	Related security features
7	7.1, 7.1.1, 7.1.2, 7.2, 7.2.2, 7.2.3	User access control and account/password complexity
8	8.2, 8.1.1, 8.1.2, 8.1.4,8.1.5, 8.1.6, 8.1.7, 8.1.8, 8.2, 8.2.1, 8.2.3, 8.2.4, 8.2.5, 8.2.6, 8.3	
10	10.4, 0.4.1, 10.4.2, 10.4.3	Accurate time synchronization
10	10.1, 10.2, 10.2.2, 10.2.3, 10.2.4,10.2.7, 10.3, 10.3.1, 10.3.2, 10.3.3, 10.3.5, 10.3.6, 10.5.2, 10.5.4	Audit trail monitoring
11	11.3, 11.3.1, 11.3.2, 11.3,3, 11.3.4	Security testing

PCI Security Standards Council

International Security Standards for Product Evaluation

Common Criteria

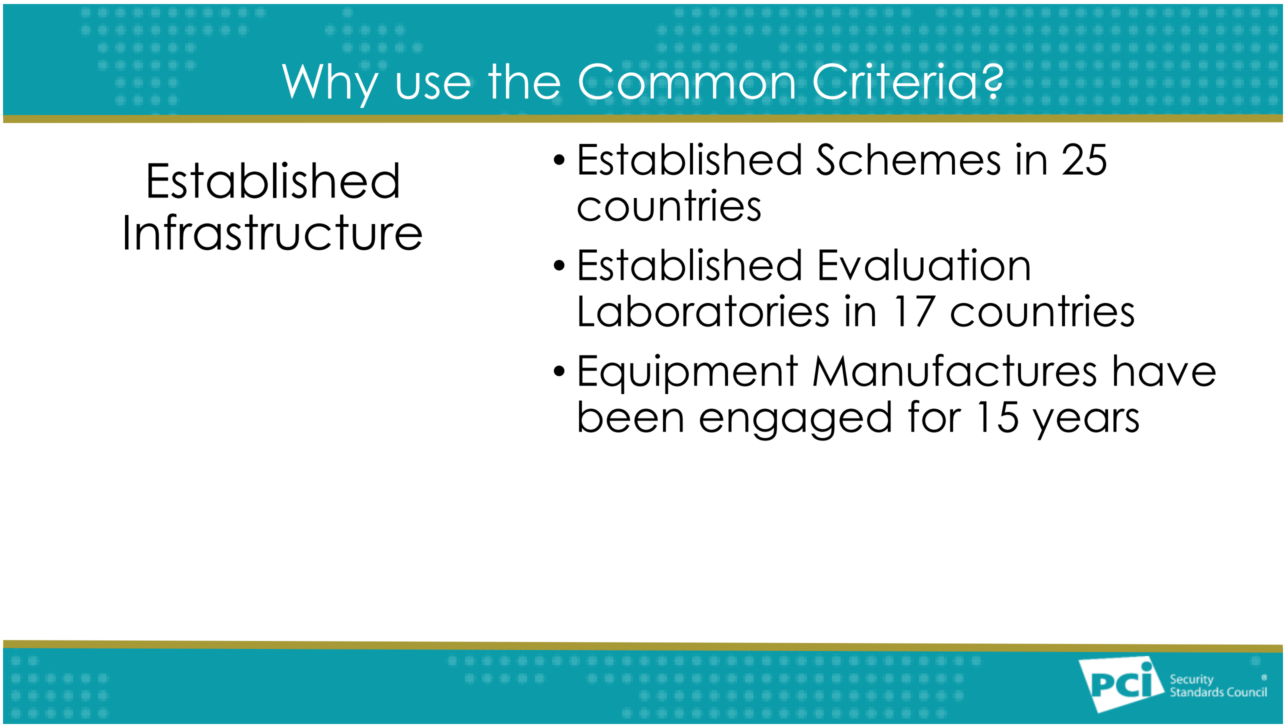


What is the Common Criteria (CC)

The Common Criteria is:

A product security evaluation methodology

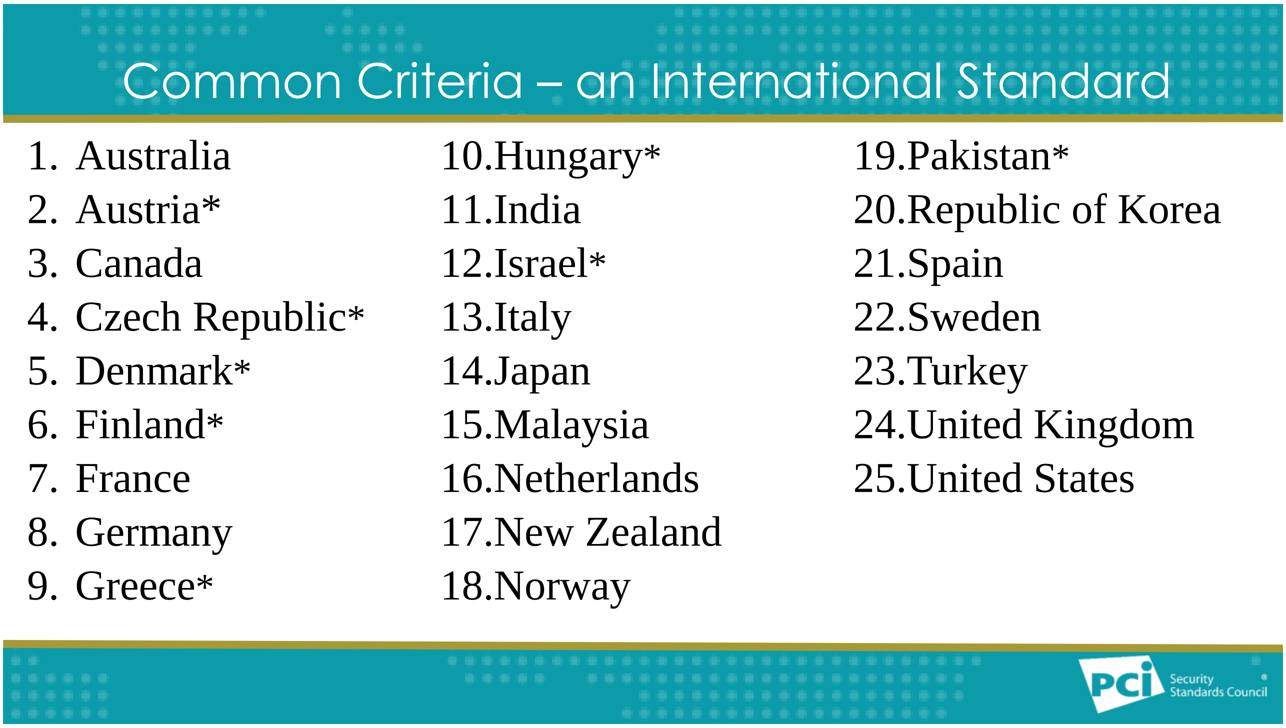
Primarily used for Government driven certification schemes for Federal Government agencies and critical infrastructure.



Why use the Common Criteria?

Established Infrastructure

- Established Schemes in 25 countries
- Established Evaluation Laboratories in 17 countries
- Equipment Manufactures have been engaged for 15 years



Common Criteria – an International Standard

1. Australia
2. Austria*
3. Canada
4. Czech Republic*
5. Denmark*
6. Finland*
7. France
8. Germany
9. Greece*
10. Hungary*
11. India
12. Israel*
13. Italy
14. Japan
15. Malaysia
16. Netherlands
17. New Zealand
18. Norway
19. Pakistan*
20. Republic of Korea
21. Spain
22. Sweden
23. Turkey
24. United Kingdom
25. United States

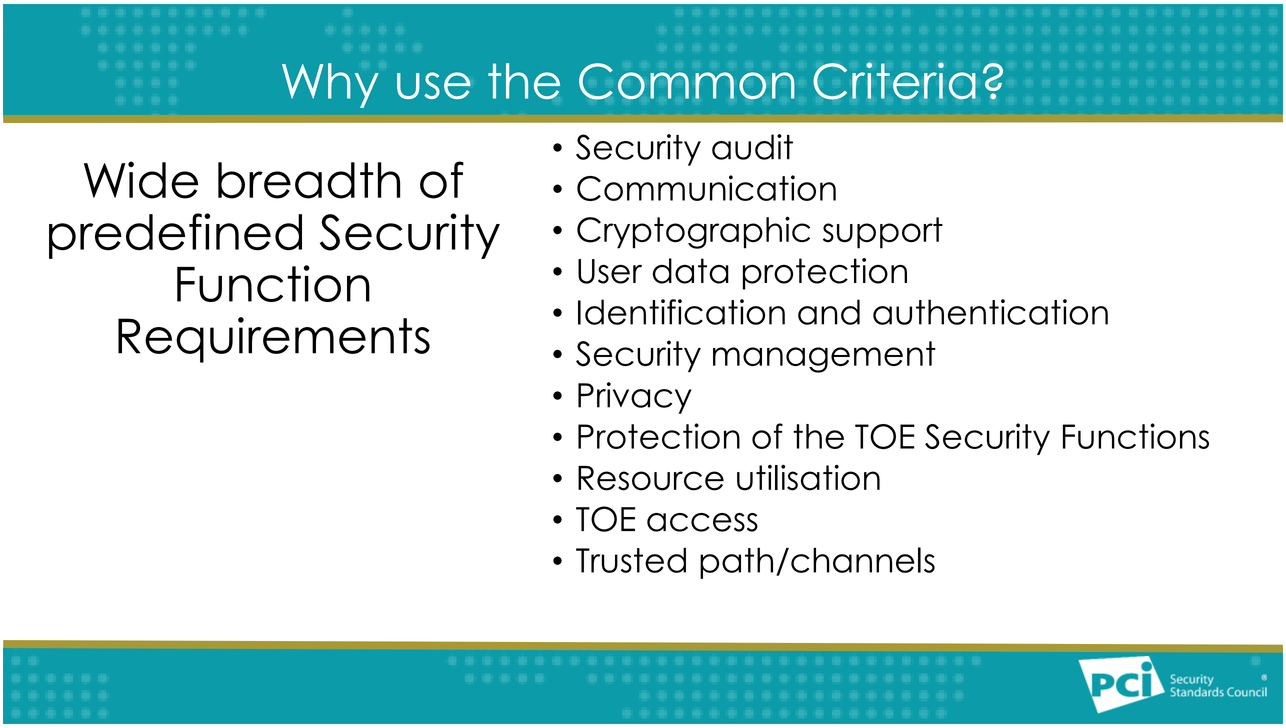
Why use the Common Criteria?

Manufacturers participation

- Over 2700 Products have been certified
- Over 475 Manufacturers have certified products

Why use the Common Criteria?

Product Category	# Certified Products
ICs, Smart Cards and Smart Card-Related Devices and Systems	852
Other Devices and Systems	284
Network and Network-Related Devices and Systems	218
Multi-Function Devices	129
Boundary Protection Devices and Systems	110
Operating Systems	104
Products for Digital Signatures	85
Access Control Devices and Systems	73
Data Protection	65
Databases	30
Key Management Systems	30
Detection Devices and Systems	21
Trusted Computing	6
Biometric Systems and Devices	3

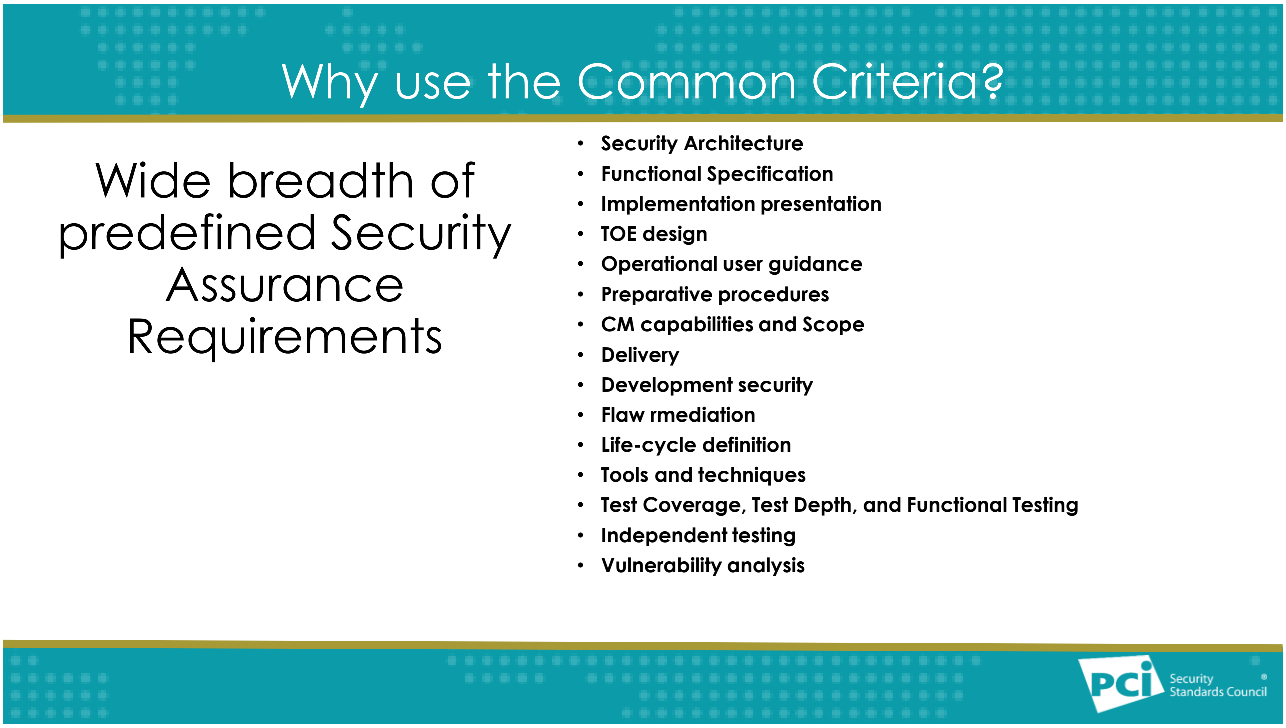


Why use the Common Criteria?

Wide breadth of predefined Security Function Requirements

- Security audit
- Communication
- Cryptographic support
- User data protection
- Identification and authentication
- Security management
- Privacy
- Protection of the TOE Security Functions
- Resource utilisation
- TOE access
- Trusted path/channels

PCI Security Standards Council



Why use the Common Criteria?

Wide breadth of predefined Security Assurance Requirements

- **Security Architecture**
- **Functional Specification**
- **Implementation presentation**
- **TOE design**
- **Operational user guidance**
- **Preparative procedures**
- **CM capabilities and Scope**
- **Delivery**
- **Development security**
- **Flaw rmediation**
- **Life-cycle definition**
- **Tools and techniques**
- **Test Coverage, Test Depth, and Functional Testing**
- **Independent testing**
- **Vulnerability analysis**

PCI Security Standards Council

CC Strengths

- International Standard
- Wide acceptance at National level
- Long history w/ large body of experts
- Wide applicability to IT products of different technologies
- Very wide breadth
- Depth and rigor adjustable for different environments

CC Weaknesses

- Evaluation inconsistencies
  - Differences between scheme capabilities
  - Differences between laboratory capabilities
- Evaluation process takes too long
- Product vendors often say the evaluation costs are too high.
  - Laboratory costs (1X)
  - Internal costs (4X – 5X)

CC Changes

- Substantial CC changes have been proposed to:
  - Better target specific technologies
  - Better represent industry groups and consumers
  - Reduce time in evaluation
  - Reduce cost

CC Changes

- Elimination of EALs (Evaluation Assurance Levels)
- Requiring PP's (Protection Profiles)for all evaluations
- Assurance requirements detailed in the PP's vs. in the Common Criteria Part 3

CC Changes

- Movement to a collaborative Protection Profile (cPP)
  - Improved targeting to specific technologies
  - Developed by International Technical Communities
    - iTCs are composed of but not limited to:
      - Scheme experts
      - Product vendors
      - Consultants and Evaluators
      - Government end-users

Security specification using Common Criteria

- Part 2 - Security Function Requirements (SFRs)
  - Extensive catalog of standard security function requirements
  - Constrained language
  - The catalog is extensible

- Part 3 - Security Assurance Requirements (SARs)
  - Extensive catalog of standard security assurance requirements
  - Constrained language
  - The catalog is extensible

Security specification using Common Criteria

- Protection Profile
  - Template specifying the minimum security characteristics of a product
  - There are PPs written for each class of product

- Protection Profiles have constrained formats and contain:
  a) PP *introduction* (narrative description)
  b) *Conformance claim,*
  c) *Security problem definition*
  d) *Security objectives,*
  e) *Extended components definition,*
  f) *Security requirements*

Security specification using Common Criteria

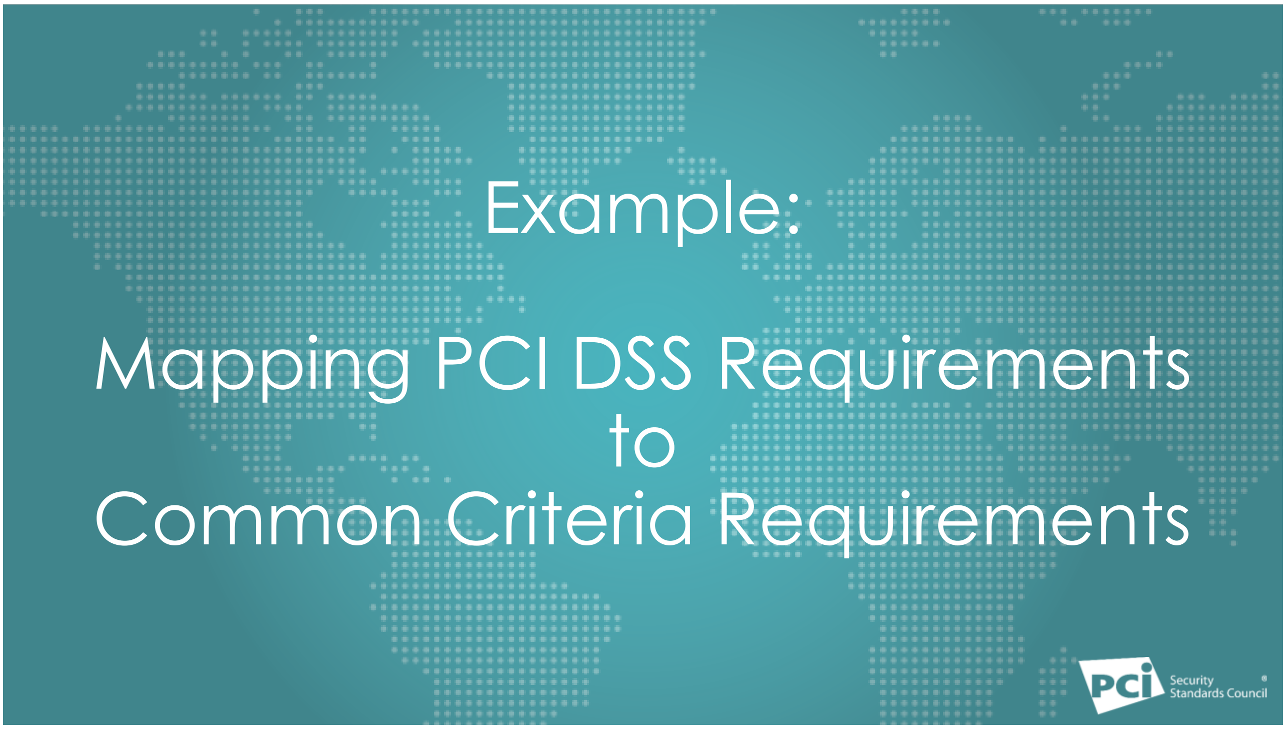
Security Targets contain:

a) ST *introduction* (narrative description at 3 levels of detail)
b) *Conformance claim,*
c) *Security problem definition*
d) *Security objectives,*
e) *Extended components definition,*
f) *Security requirements*
g) TOE summary specification;

Integrating the CC into PCI DSS

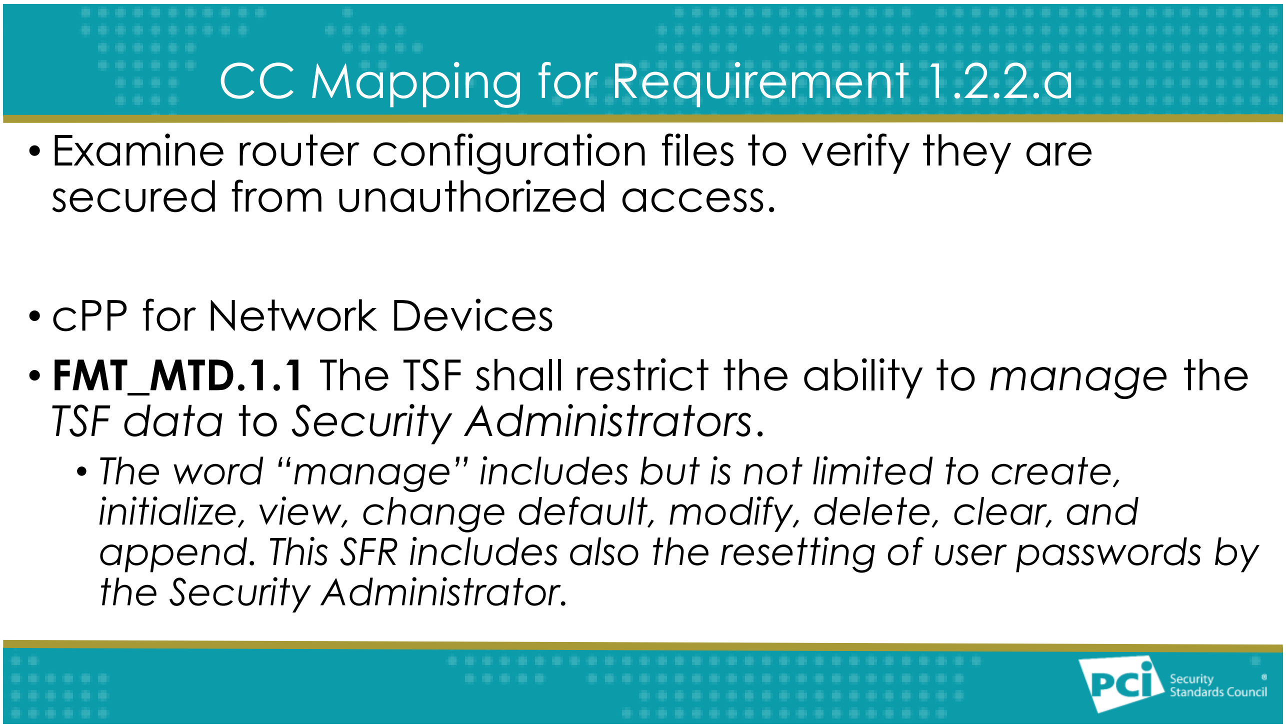
Integrating the CC into PCI DSS

1. Develop appropriate cPPs specific to PCI DSS
   - Base each on existing cPPs
     - Save development time, effort and money
   - Network Device cPP
     - Firewall
     - Switches
     - Routers
   - OS cPP
   - Virtualization cPP
   - Application Software cPP
   - …
2. Mapping PCI DSS Requirements to Common Criteria Requirements



Example:

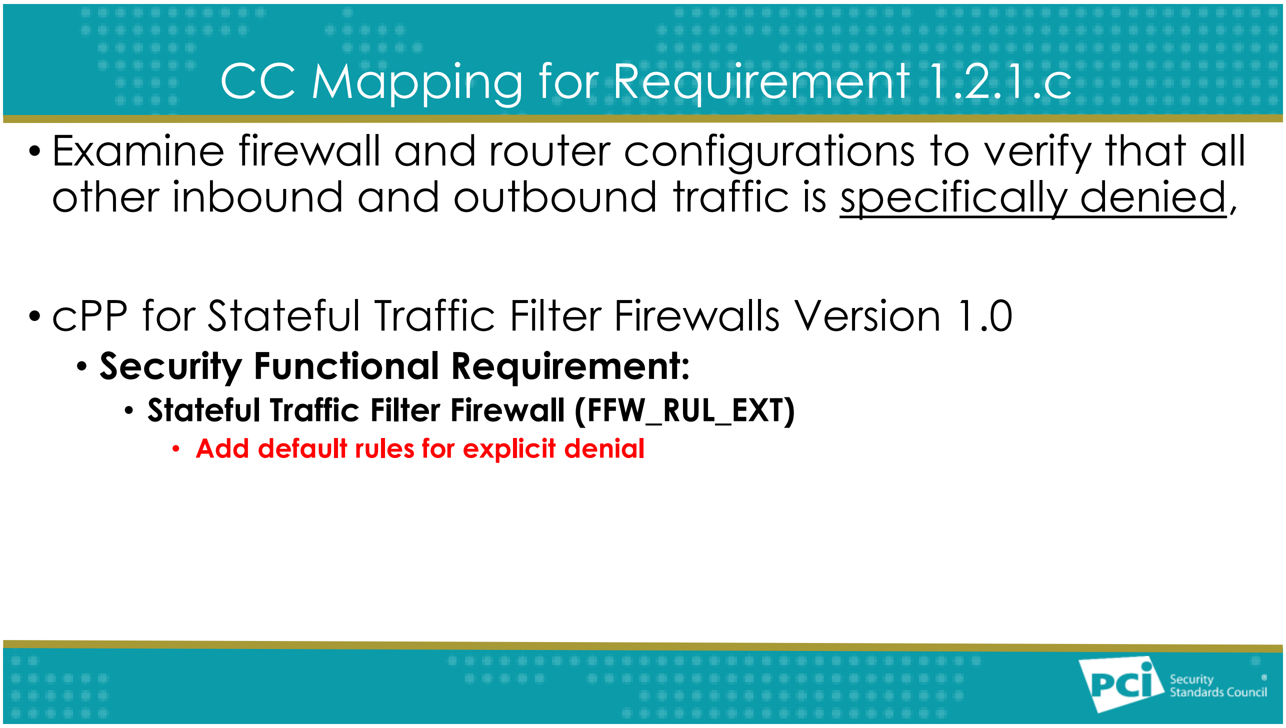
Mapping PCI DSS Requirements to Common Criteria Requirements



CC Mapping for Requirement 1.2.2.a

- Examine router configuration files to verify they are secured from unauthorized access.

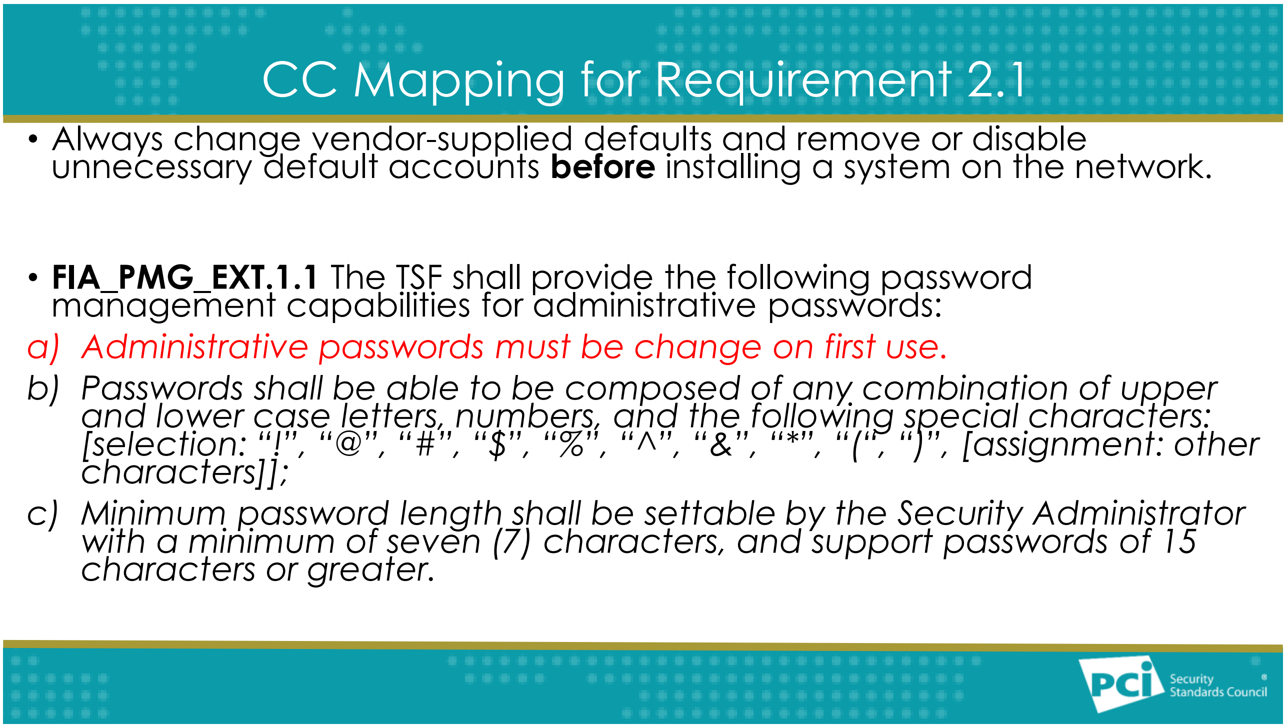
- cPP for Network Devices
- **FMT_MTD.1.1** The TSF shall restrict the ability to *manage* the *TSF data* to *Security Administrators*.
  - *The word "manage" includes but is not limited to create, initialize, view, change default, modify, delete, clear, and append. This SFR includes also the resetting of user passwords by the Security Administrator.*



CC Mapping for Requirement 1.2.1.c

- Examine firewall and router configurations to verify that all other inbound and outbound traffic is specifically denied,

- cPP for Stateful Traffic Filter Firewalls Version 1.0
  - **Security Functional Requirement:**
    - **Stateful Traffic Filter Firewall (FFW_RUL_EXT)**
      - **Add default rules for explicit denial**



CC Mapping for Requirement 2.1

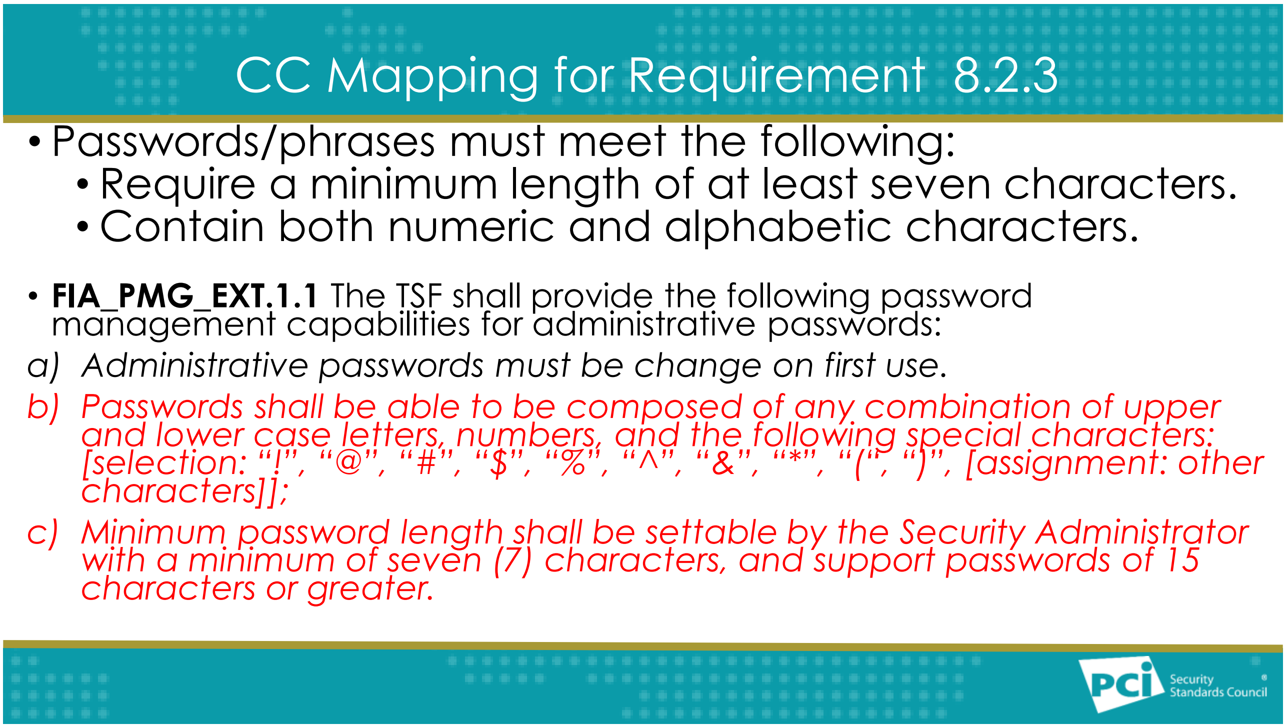
- Always change vendor-supplied defaults and remove or disable unnecessary default accounts **before** installing a system on the network.

- **FIA_PMG_EXT.1.1** The TSF shall provide the following password management capabilities for administrative passwords:

a) *Administrative passwords must be change on first use.*

b) *Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: [selection: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”, [assignment: other characters]];*

c) *Minimum password length shall be settable by the Security Administrator with a minimum of seven (7) characters, and support passwords of 15 characters or greater.*



CC Mapping for Requirement 8.2.3

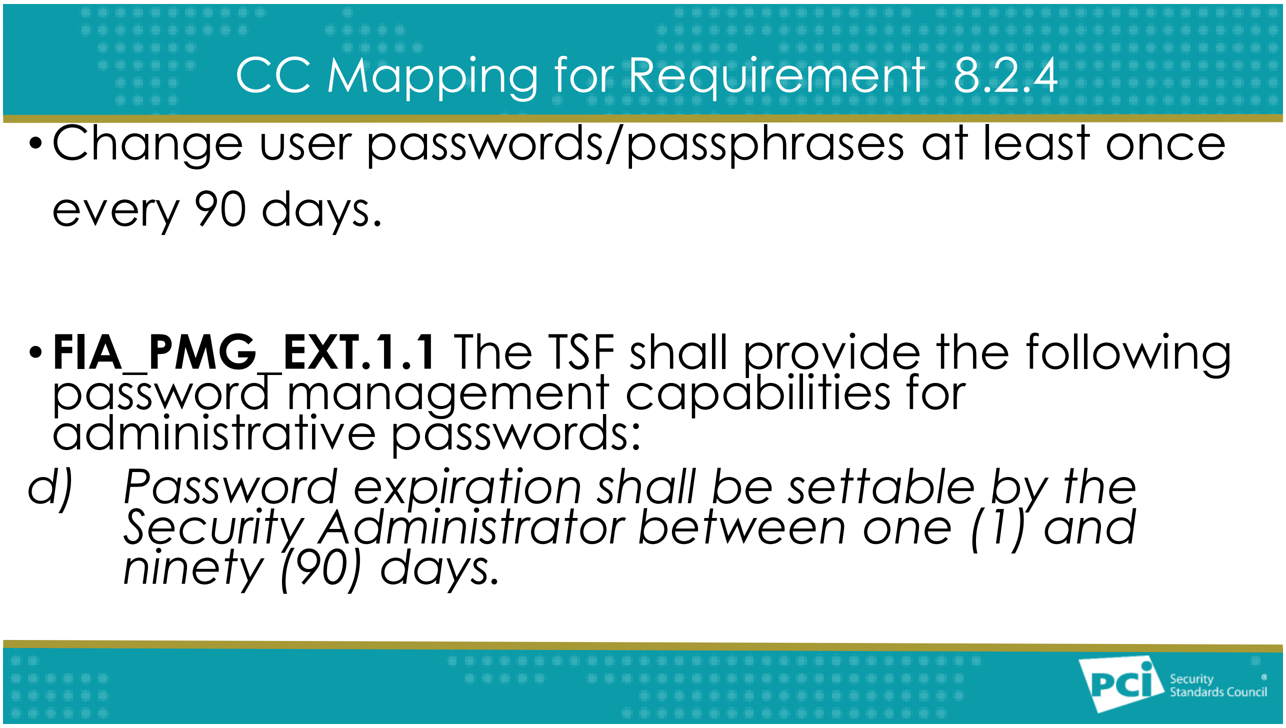
- Passwords/phrases must meet the following:
  - Require a minimum length of at least seven characters.
  - Contain both numeric and alphabetic characters.

- **FIA_PMG_EXT.1.1** The TSF shall provide the following password management capabilities for administrative passwords:

a) *Administrative passwords must be change on first use.*

b) *Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: [selection: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”, [assignment: other characters]];*

c) *Minimum password length shall be settable by the Security Administrator with a minimum of seven (7) characters, and support passwords of 15 characters or greater.*

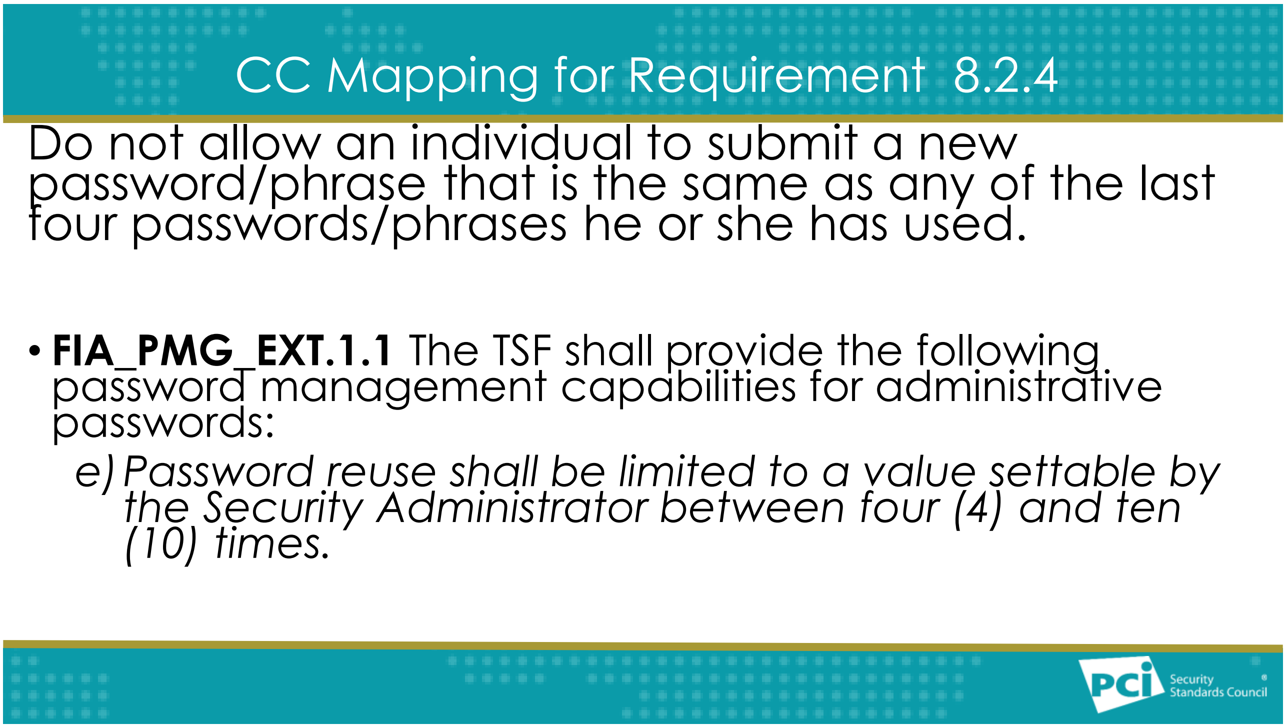


CC Mapping for Requirement 8.2.4

- Change user passwords/passphrases at least once every 90 days.

- **FIA_PMG_EXT.1.1** The TSF shall provide the following password management capabilities for administrative passwords:

d) *Password expiration shall be settable by the Security Administrator between one (1) and ninety (90) days.*



CC Mapping for Requirement 8.2.4

Do not allow an individual to submit a new password/phrase that is the same as any of the last four passwords/phrases he or she has used.

- **FIA_PMG_EXT.1.1** The TSF shall provide the following password management capabilities for administrative passwords:
  - *e) Password reuse shall be limited to a value settable by the Security Administrator between four (4) and ten (10) times.*

End !

Thank You