BSI Webinar

เสริมเกราะป้องกันข้อมูลบัตรชำระเงินด้วยมาตรฐานสากล PCIDSS 4.0

BSI Thailand

เนื้อหา

01 What is PCI DSS and Purpose ?

02 PCI DSS Participant and Overview component

03 Overview PCIDSS requirement

04 What did v4.0 add or change ?

What is PCI DSS and Purpose ?

PCIDSS & PCISSC

The PCI Security Standards Council (PCI SSC)

is the organization that creates, maintains, and publishes the Payment Card Industry Data Security Standard (PCI DSS) as well as several related standards and programs. It consists of representatives from 6 payment brands.
Visa, MasterCard, American Express, Discover, UnionPay and JCB.

Purpose

To enhance global payment account data security by developing standards and supporting services that drive education, awareness, and effective implementation by stakeholders.

- Managing Global Payment Security Standards
- Validating and Listing Products and Solutions that Meet PCI SSC Standards and Program Requirements
- Training, Testing, and Qualifying Security Professionals and Organizations
- Providing Free Best Practices and Payment Security Resources

Cr. pcisecuritystandards.org

PCIDSS & PCISSC

The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that handle cardholder data associated with the major card brands

Visa,
MasterCard,
American Express,
Discover,
UnionPay and
JCB.

PCI DSS was developed to encourage and enhance payment card account data security and facilitate the broad adoption of consistent data security measures globally. PCI DSS provides a baseline of technical and operational requirements designed to protect payment account data.

Cr. pcisecuritystandards.org

PCIDSS & PCISSC

PCI Data Security Standard (PCI DSS)

The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that handle cardholder data associated with the major card brands

PCI DSS was developed to encourage and enhance payment card account data security and facilitate the broad adoption of consistent data security measures globally. PCI DSS provides a baseline of technical and operational requirements designed to protect payment account data.

Cr. pcisecuritystandards.org

PCI DSS Participant and Overview component

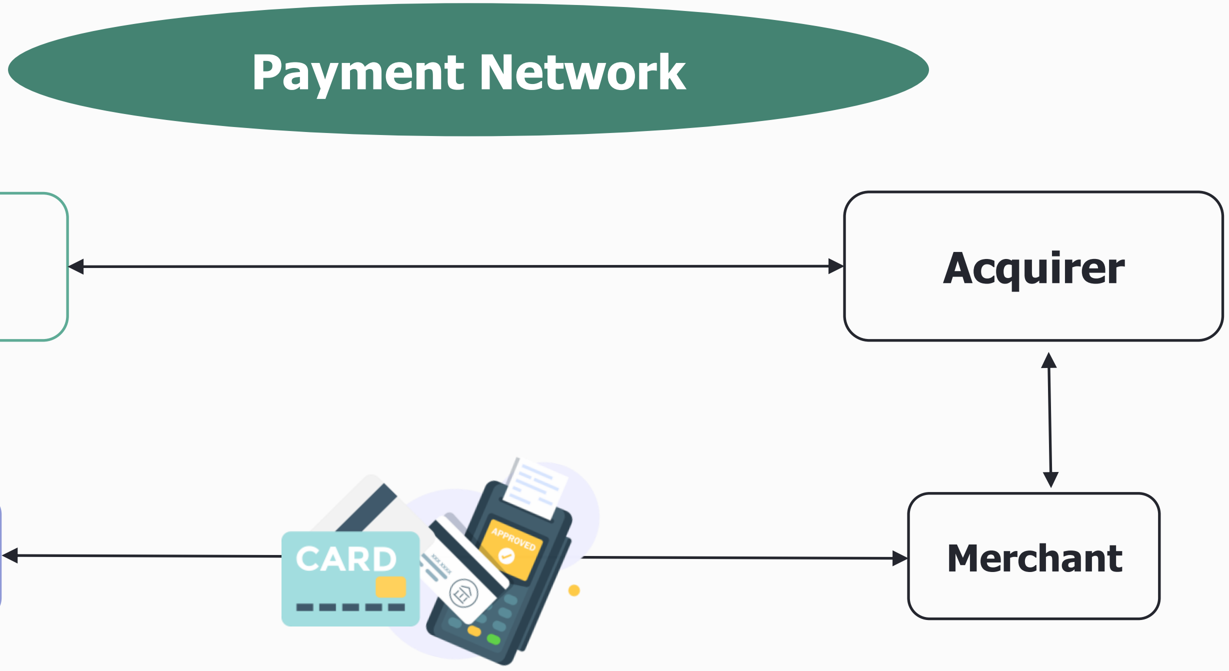
Intended Audience

Entities that store, process, or transmit cardholder data (CHD) and/or sensitive authentication data (SAD) or could impact the security of the cardholder data environment (CDE). This includes all entities involved in payment card processing – including merchants, processors, acquirers, issuers, and service providers.

- Payment brand
- Consumer
- Issuer
- Acquirer
- Merchant
- Thirty Party Service Provider
- Approved Scanning Vendors (ASV)
- Internal Security Assessors (ISA)
- Payment Card Industry Professionals (PCIP)
- PCI Forensic Investigators (PFIs)
- Qualified Security Assessor (QSA)

Cr. pcisecuritystandards.org

PCI DSS Participant and Overview component


Payment Network

Issuer

Acquirer

Consumer

Merchant

Third party Service Provider

Data Center (Hosted)
Payment Gateway
Cloud Service
Software Development
Call Center
VOIP
ASV
SOCs

Cr. pcisecuritystandards.org

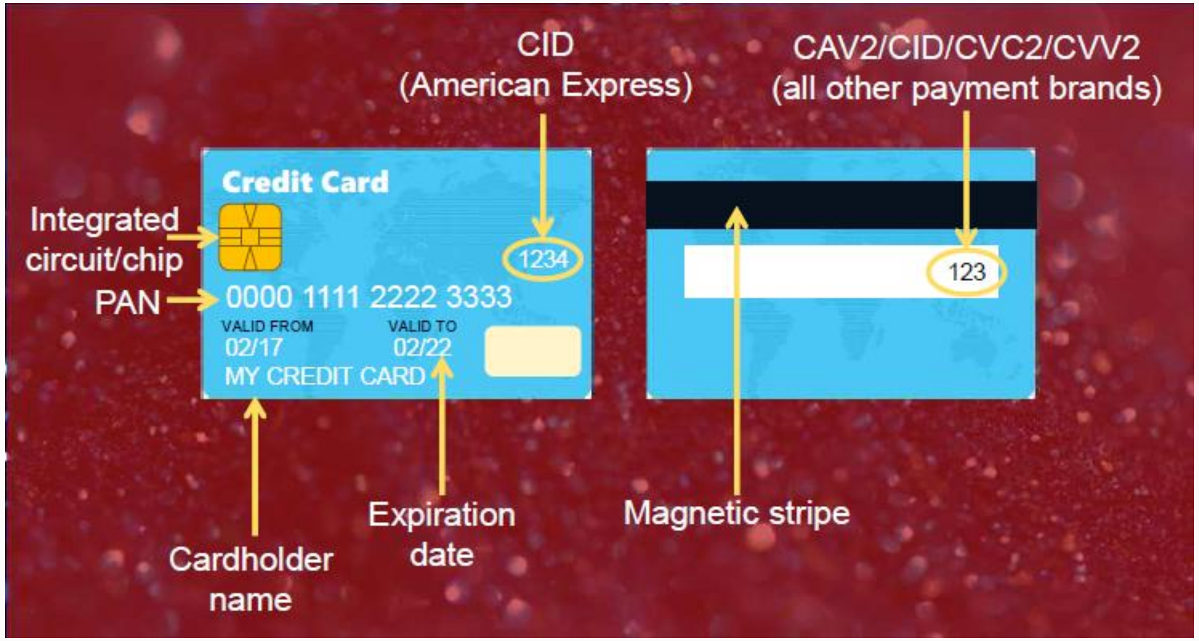
PCI DSS Participant and Overview component

Account Data
Cardholder data (CHD)

- Primary account number (PAN)
- Cardholder name
- Service code (three or four-digit number on the magnetic-stripe that specifies acceptance requirements and limitations for a magnetic-stripe read transaction)
- Expiry date

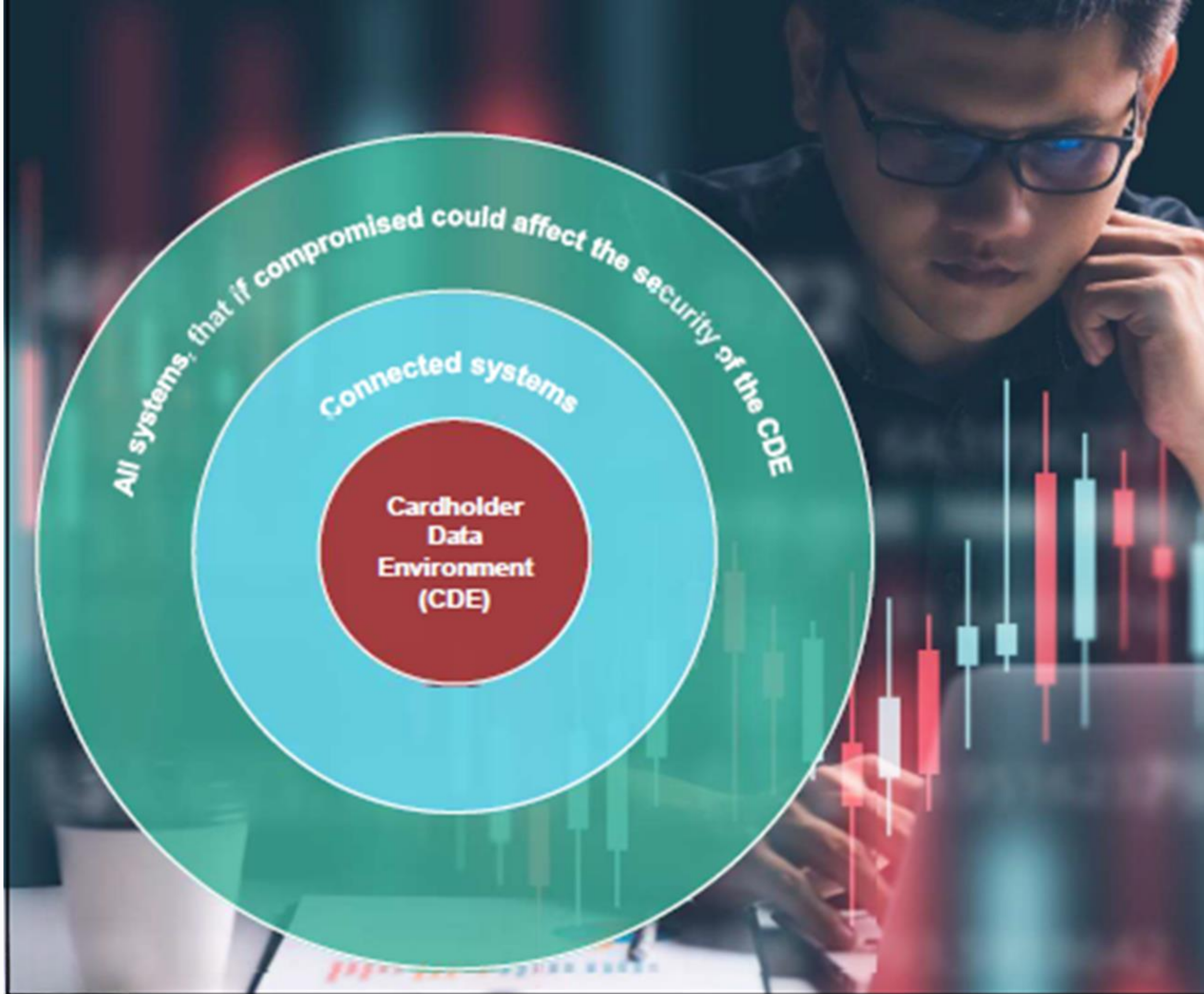
Sensitive authentication data (SAD)

- Full magnetic stripe data
- CAV2/CVC2/CVV2/CID
- PINs/PIN blocks



Cr. pcisecuritystandards.org

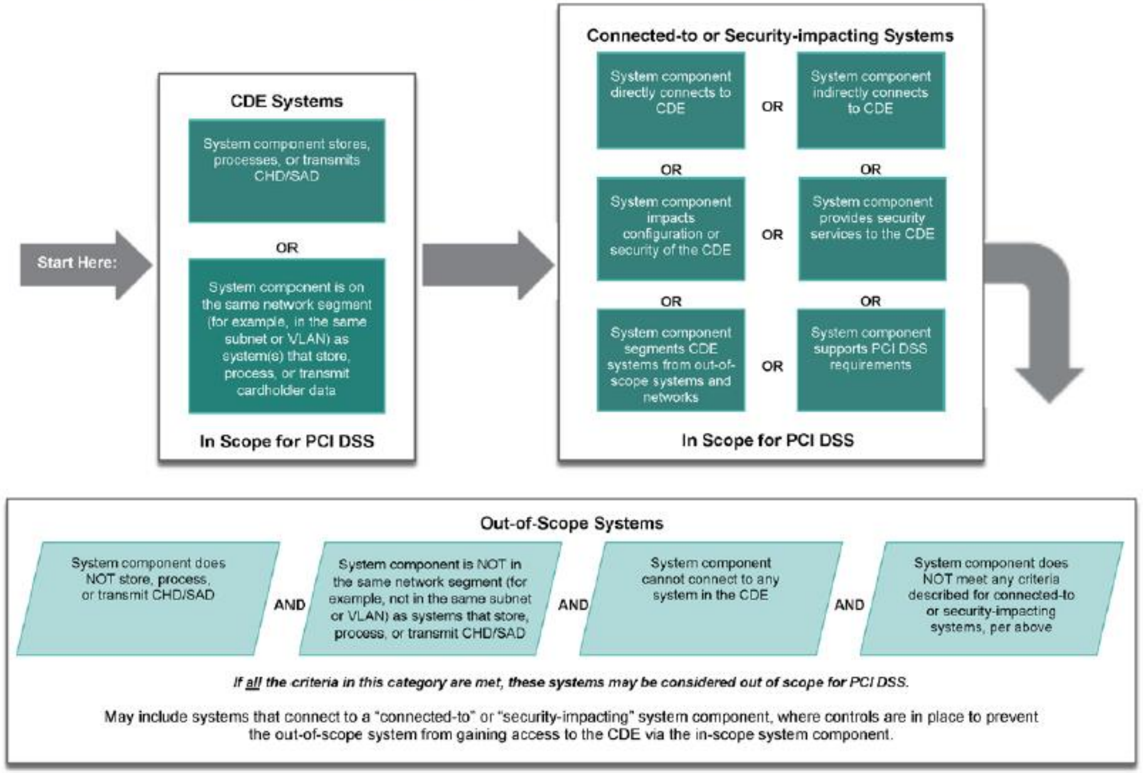
PCI DSS Participant and Overview component


All systems, that if compromised could affect the security of the CDE
Connected systems
Cardholder Data Environment (CDE)

Refer. Information Supplement: Guidance for PCI DSS Scoping and Network Segmentation

PCI DSS Participant and Overview component

FIGURE 1 – PCI DSS Scoping Categories



Start Here:

CDE Systems

System component stores, processes, or transmits CHD/SAD

OR

System component is on the same network segment (for example, in the same subnet or VLAN) as system(s) that store, process, or transmit cardholder data

In Scope for PCI DSS

Connected-to or Security-impacting Systems

System component directly connects to CDE OR System component indirectly connects to CDE

OR OR

System component impacts configuration or security of the CDE OR System component provides security services to the CDE

OR OR

System component segments CDE systems from out-of-scope systems and networks OR System component supports PCI DSS requirements

In Scope for PCI DSS

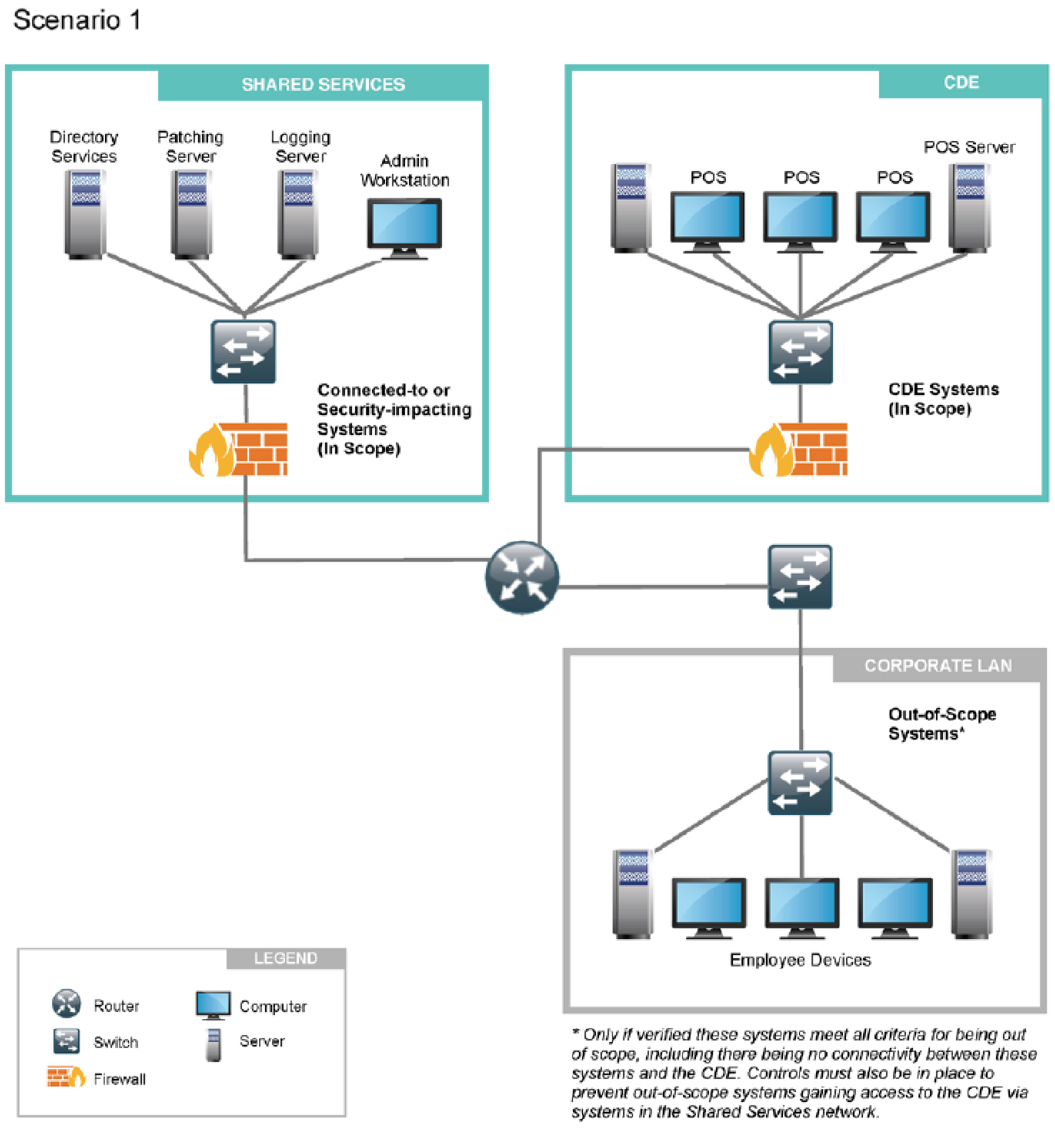
Out-of-Scope Systems

System component does NOT store, process, or transmit CHD/SAD AND System component is NOT in the same network segment (for example, not in the same subnet or VLAN) as systems that store, process, or transmit CHD/SAD AND System component cannot connect to any system in the CDE AND System component does NOT meet any criteria described for connected-to or security-impacting systems, per above

If all the criteria in this category are met, these systems may be considered out of scope for PCI DSS.

May include systems that connect to a "connected-to" or "security-impacting" system component, where controls are in place to prevent the out-of-scope system from gaining access to the CDE via the in-scope system component.

FIGURE 2 – Example Segmentation Illustration: "Connected-to" Shared Services



** Only if verified these systems meet all criteria for being out of scope, including there being no connectivity between these systems and the CDE. Controls must also be in place to prevent out-of-scope systems gaining access to the CDE via systems in the Shared Services network.*

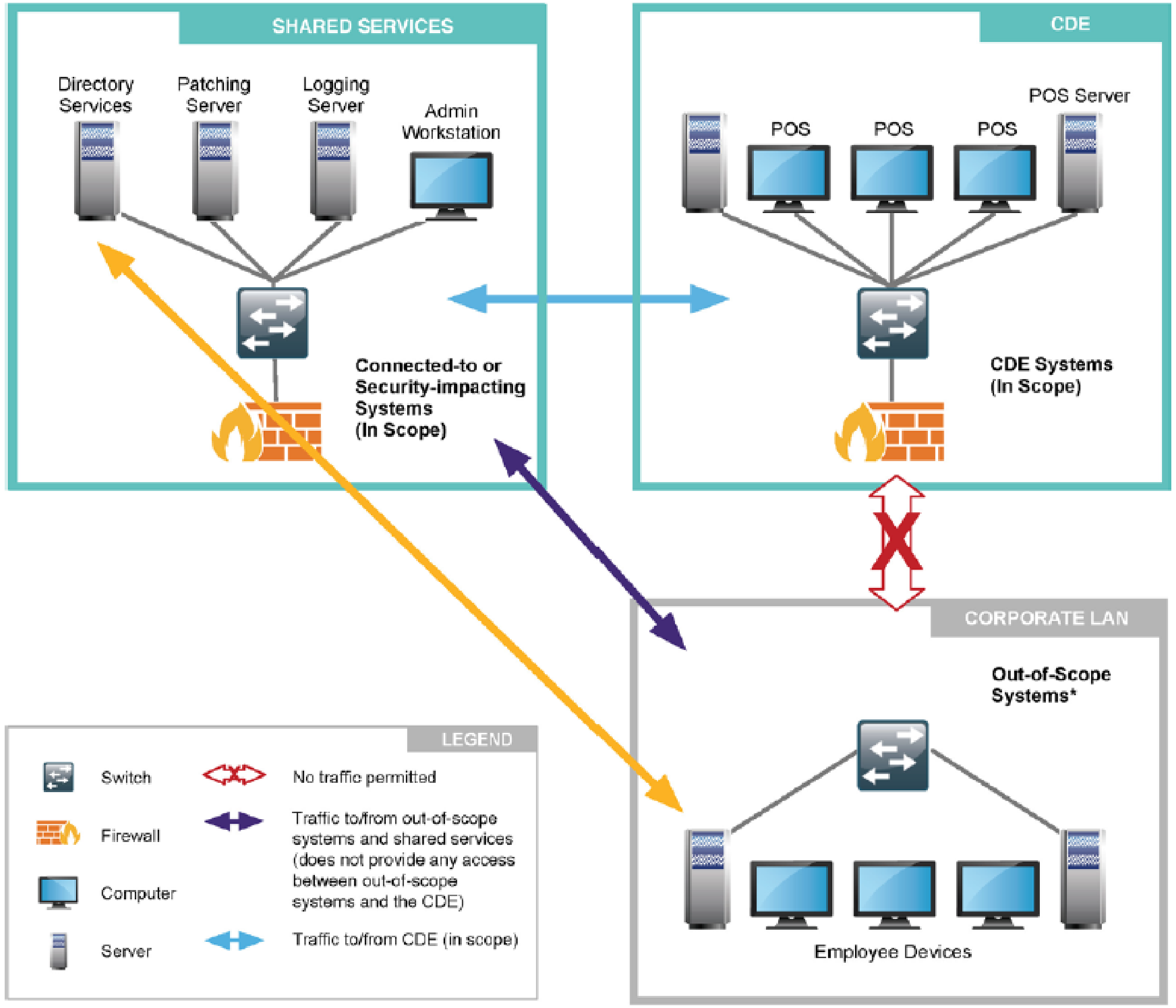
Refer. Information Supplement:
Guidance for PCI DSS Scoping and Network Segmentation

Cr. pcisecuritystandards.org

PCI DSS Participant and Overview component

Refer. Information Supplement:
Guidance for PCI DSS Scoping and Network Segmentation

Scenario 1: Logical Data Flow



Only if verified these systems meet all criteria for being out of scope, including there being no connectivity between these systems and the CDE. Controls must also be in place to prevent out-of-scope systems gaining access to the CDE via systems in the Shared Services network.

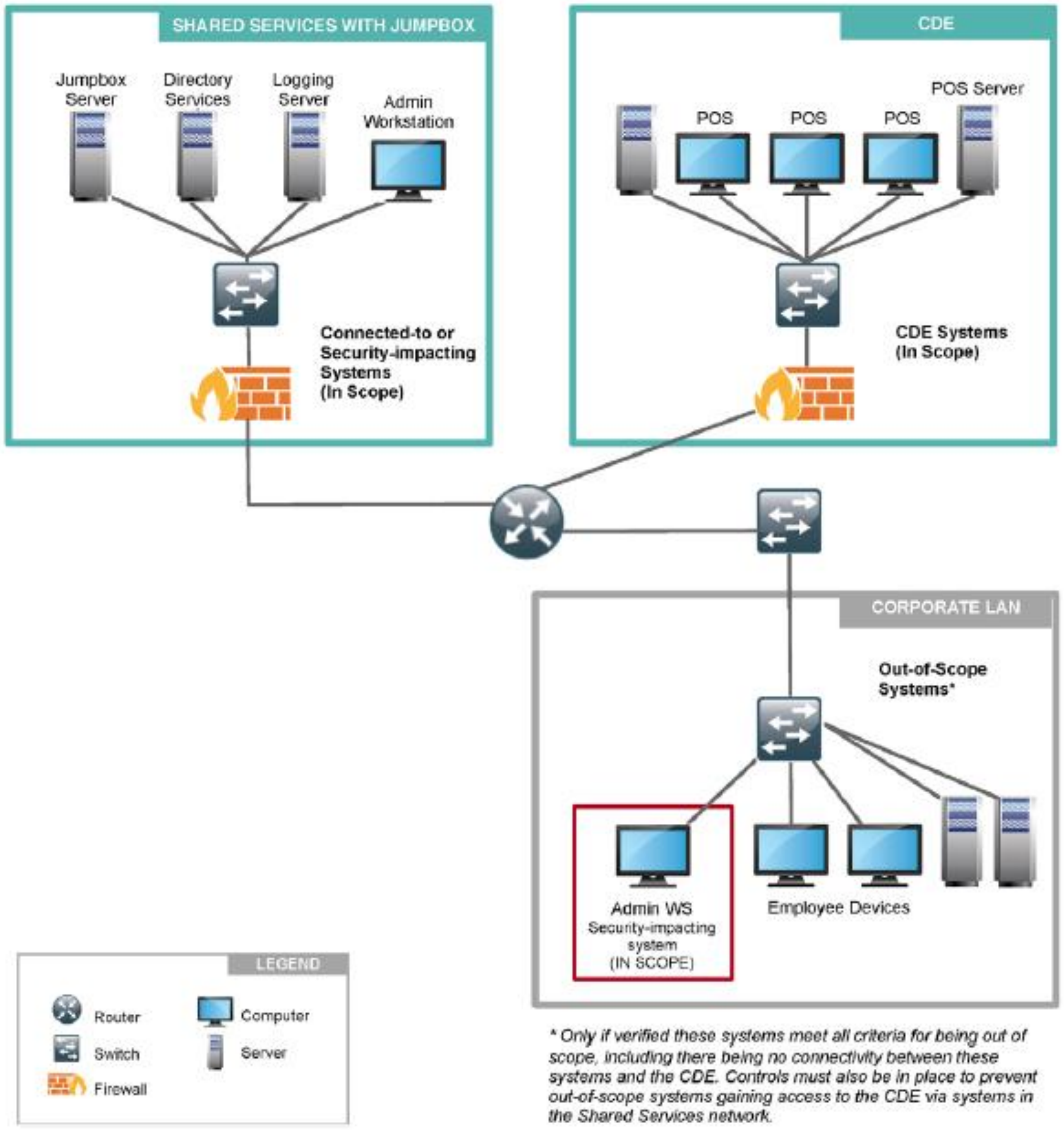
Cr. pcisecuritystandards.org

PCI DSS Participant and Overview component

Refer. Information Supplement:
Guidance for PCI DSS Scoping and Network Segmentation

FIGURE 4 – Example Segmentation Illustration: Administration of CDE Systems from a Security-Impacting System in the Corporate LAN

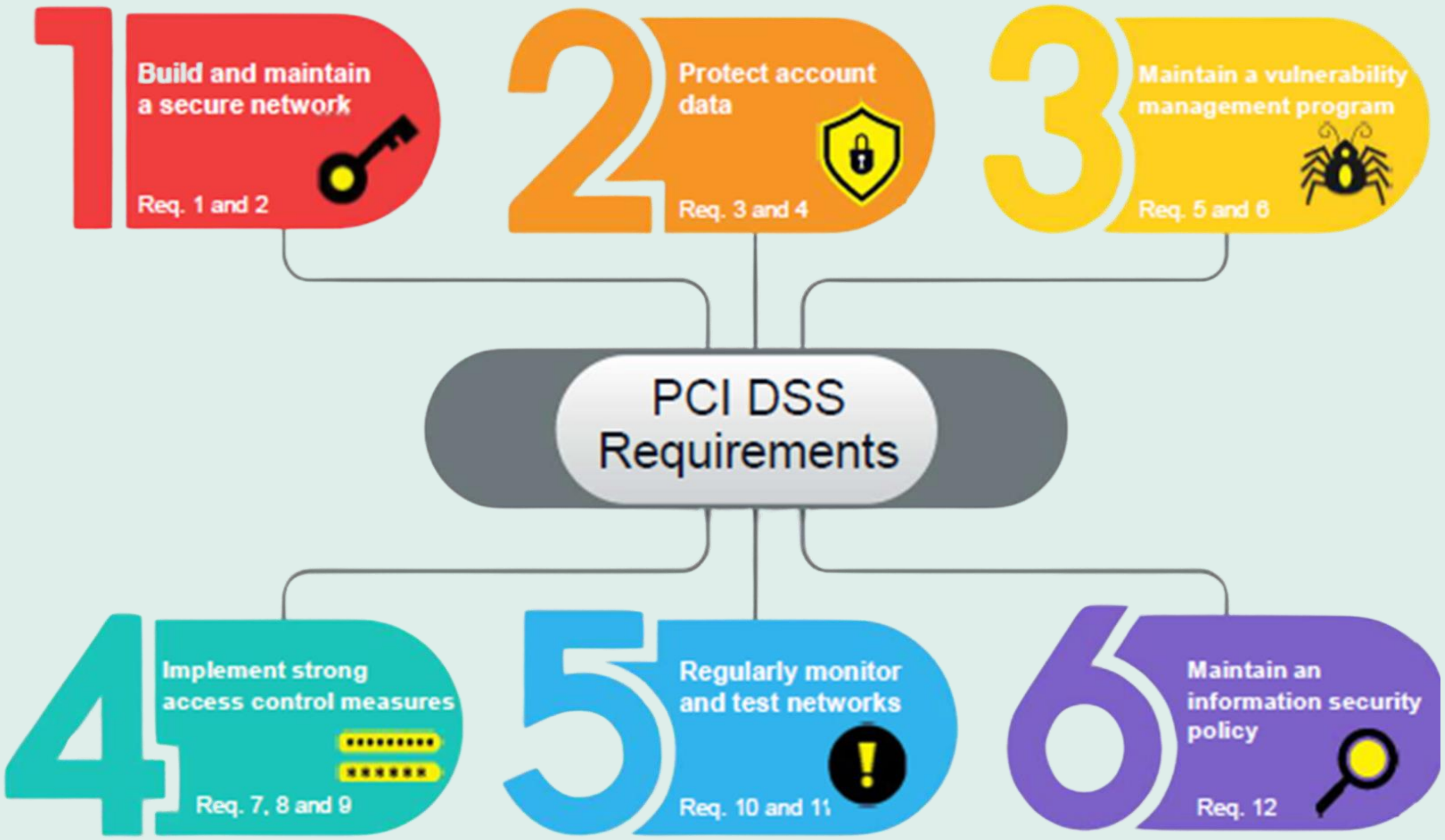
Scenario 2



* *Only if verified these systems meet all criteria for being out of scope, including there being no connectivity between these systems and the CDE. Controls must also be in place to prevent out-of-scope systems gaining access to the CDE via systems in the Shared Services network.*

Cr. pcisecuritystandards.org

Overview PCIDSS requirement



PCI DSS Requirements

1 Build and maintain a secure network

Req. 1 and 2

2 Protect account data

Req. 3 and 4

3 Maintain a vulnerability management program

Req. 5 and 6

4 Implement strong access control measures

Req. 7, 8 and 9

5 Regularly monitor and test networks

Req. 10 and 11

6 Maintain an information security policy

Req. 12

Overview PCIDSS requirement

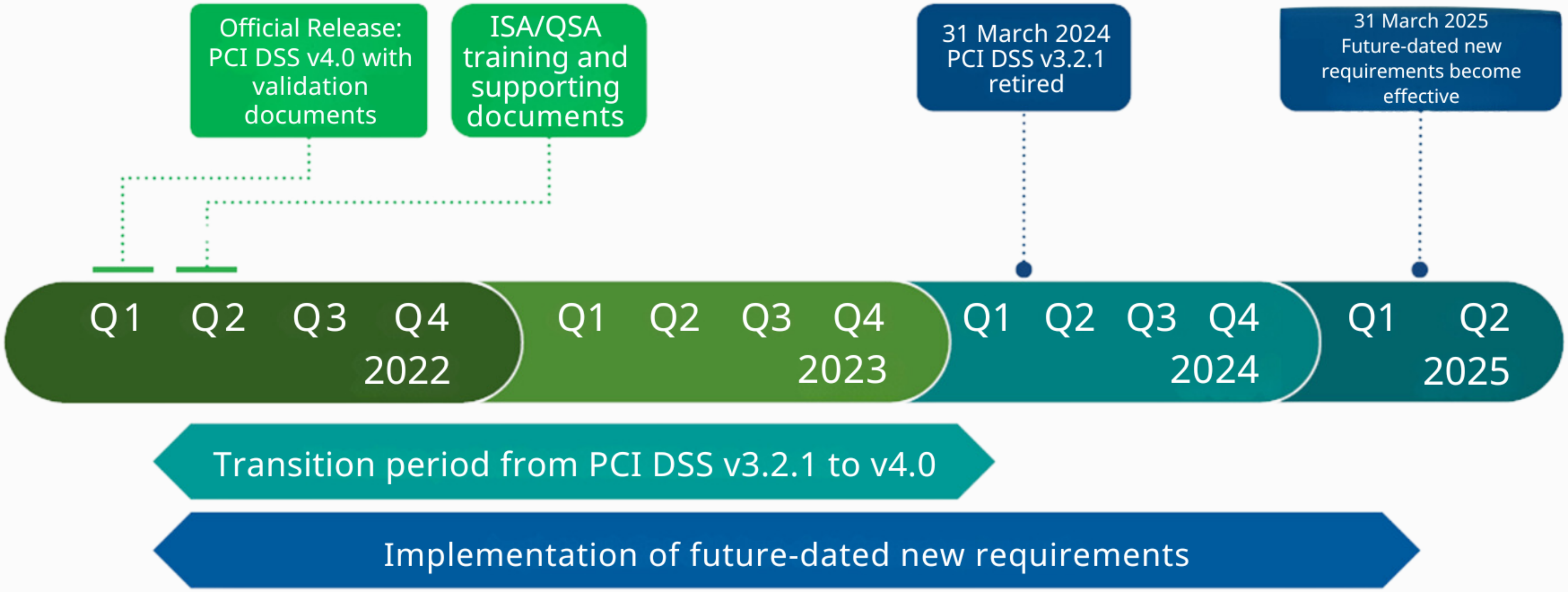
Requirement	Description
1	Install and Maintain Network Security Controls
2	Apply Secure Configurations to All System Components
3	Protect Stored Account Data
4	Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public
5	Protect All Systems and Networks from Malicious Software
6	Develop and Maintain Secure Systems and Software
7	Restrict Access to System Components and Cardholder Data by Business Need to Know
8	Identify Users and Authenticate Access to System Components
9	Restrict Physical Access to Cardholder Data
10	Log and Monitor All Access to System Components and Cardholder Data
11	Test Security of Systems and Networks Regularly
12	Support Information Security with Organizational Policies and Programs

Cr. pcisecuritystandards.org

What did v4.0 add or change ?

Implementation Timeline

PCI DSS v3.2.1 will remain active for two years after v4.0 is published. This provides organizations time to become familiar with the new version, and plan for and implement the changes needed.



Official Release: PCI DSS v4.0 with validation documents

ISA/QSA training and supporting documents

31 March 2024 PCI DSS v3.2.1 retired

31 March 2025 Future-dated new requirements become effective

Transition period from PCI DSS v3.2.1 to v4.0

Implementation of future-dated new requirements

Cr. pcisecuritystandards.org

What did v4.0 add or change ?

Change Type	Definition
Evolving requirement	Changes to ensure that the standard is up to date with emerging threats and technologies, and changes in the payment industry. Examples include new or modified requirements or testing procedures, or the removal of a requirement.
Clarification or guidance	Updates to wording, explanation, definition, additional guidance, and/or instruction to increase understanding or provide further information or guidance on a particular topic.
Structure or format	Reorganization of content, including combining, separating, and renumbering of requirements to align content.

Cr. pcisecuritystandards.org

What did v4.0 add or change ?

Continue to meet the security needs of the payments industry.

Why it is important: Security practices must evolve as threats change.

Examples:

- Expanded multi-factor authentication requirements.
- Updated password requirements.
- New e-commerce and phishing requirements to address ongoing threats.

Promote security as a continuous process.

Why it is important: Criminals never sleep. Ongoing security is crucial to protect payment data.

Examples:

- Clearly assigned roles and responsibilities for each requirement.
- Added guidance to help people better understand how to implement and maintain security.

Cr. pcisecuritystandards.org

What did v4.0 add or change ?

Increase flexibility for organizations using different methods to achieve security objectives.

Why it is important: Increased flexibility allows more options to achieve a requirement's objective and supports payment technology innovation.

Examples:

- Allowance of group, shared, and generic accounts.
- Targeted risk analyses empower organizations to establish frequencies for performing certain activities.
- Customized approach, a new method to implement and validate PCI DSS requirements, provides another option for organizations using innovative methods to achieve security objectives.

Enhance validation methods and procedures.

Why it is important: Clear validation and reporting options support transparency and granularity.

Example:

- Increased alignment between information reported in a Report on Compliance or Self-Assessment Questionnaire and information summarized in an Attestation of Compliance.

Cr. pcisecuritystandards.org

What did v4.0 add or change ?

Requirement	Defined Approach
Requirement 1 and General in each requirement	1.1.2 Roles and responsibilities for performing activities in Requirement 1 are documented, assigned, and understood.
Requirement 2	2.2.2 Clarified that the intent is to understand whether vendor default accounts are in use and to manage them accordingly. *(default password is changed, not be used, the account is removed or disabled.)*
	2.2.5 If any insecure services, protocols, or daemons are present:. *Business justification is documented. Additional security features are documented and implemented that reduce the risk of using insecure services, protocols, or daemons.*
	2.3.1 For wireless environments connected to the CDE or transmitting account data, all wireless vendor defaults are changed at installation or are confirmed to be secure, *encryption keys, SNMP defaults., Passwords*
Requirement 3	3.2.1 New requirement bullet to address SAD stored prior to completion of authorization through implementation of data retention and disposal policies, procedures, and processes. This bullet is a best practice until 31 March 2025.
	3.3.2 New requirement *SAD* that is stored electronically *prior to completion of authorization is encrypted* using strong cryptography. This requirement is a best practice until 31 March 2025.
	3.4.2 New requirement When using remote-access technologies, technical controls *prevent copy and/or relocation of PAN* for all personnel, except for those with documented, explicit authorization and a legitimate, defined business need.
	3.5.1 PAN is rendered unreadable anywhere it is stored by using any of the following approaches: *One-way hashes Truncation Index tokens or Strong cryptography*

Cr. pcisecuritystandards.org

What did v4.0 add or change ?

Requirement	Defined Approach
Requirement 4	4.2.1 New requirement bullet Certificates used to safeguard PAN during transmission over open, public networks are confirmed as valid and are not expired or revoked.
Requirement 4	4.2.1.1 New requirement bullet An inventory of the entity’s trusted keys and certificates used to protect PAN during transmission is maintained.
Requirement 5	5.2.3.1 New requirement The frequency of periodic evaluations of system components identified as not at risk for malware is defined in the entity’s targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1.
	5.3.2.1 If periodic malware scans are performed to meet Requirement 5.3.2, the frequency of scans is defined in the entity’s targeted risk analysis,
Requirement 6	6.3.2 New requirement An inventory of bespoke and custom software, and third-party software components incorporated into bespoke and custom software is maintained to facilitate vulnerability and patch management.
	6.4.2 New requirement For public-facing web applications, an automated technical solution is deployed that continually detects and prevents web-based attacks
Requirement 7	7.2.4 New requirement All user accounts and related access privileges, including third-party/vendor accounts, are reviewed as follows *At least once every six months, appropriate based on job function etc.*
	7.2.5 New requirement All application and system accounts and related access privileges are assigned and managed as follows: *Based on the least privileges necessary, Access is limited*

Cr. pcisecuritystandards.org

What did v4.0 add or change ?

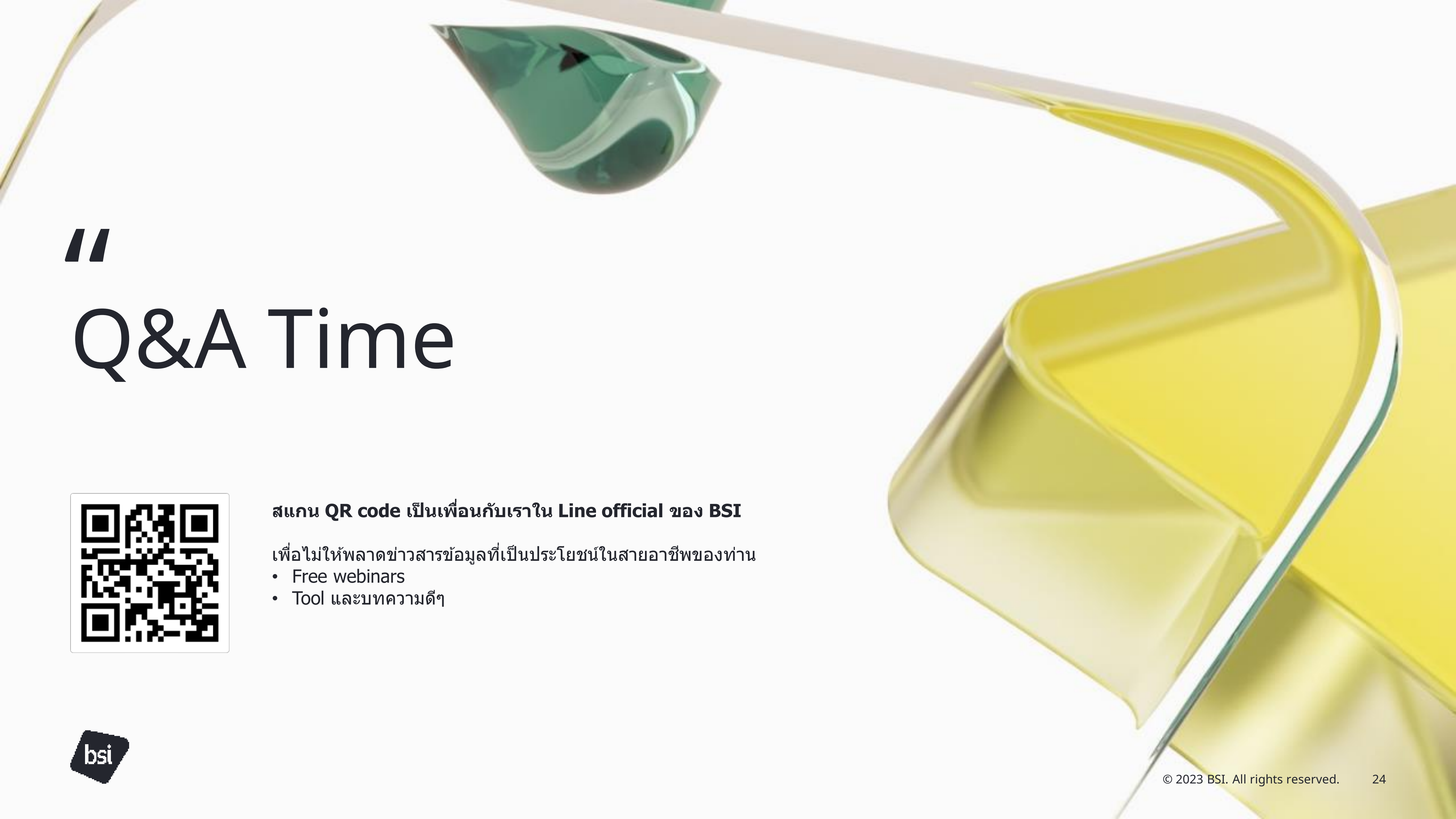
Requirement	Defined Approach
Requirement 8	8.3.6 New requirement bullet If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they meet the following minimum level of complexity: - A minimum length of 12 characters (or IF the system does not support 12 characters, a minimum length of eight characters). - Contain both numeric and alphabetic characters.
	8.4.2 New requirement bullet ***MFA*** is implemented for all access into the CDE.
Requirement 9	9.5.1.2.1 New requirement bullet The frequency of periodic POI device inspections and the type of inspections performed is defined in the entity’s targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1.
Requirement 10	10.4.1.1 New requirement for the use of automated mechanisms to perform audit log reviews.
	10.7.2 New requirement for all entities to detect, alert, and promptly address failures of critical security control systems. Network security controls, Anti-malware solutions, Logical access controls and Audit log review mechanisms etc.
Requirement 11	11.3.1.1 New requirement to manage all other applicable vulnerabilities (those not ranked as high-risk or critical) found during internal vulnerability scans.
	11.3.1.2 New requirement to perform internal vulnerability scans via authenticated scanning.

Cr. pcisecuritystandards.org

What did v4.0 add or change ?

Requirement	Defined Approach
Requirement 12	12.3.1 New requirement to perform a targeted risk analysis for any PCI DSS requirement that provides flexibility for how frequently it is performed.
	12.3.2 New requirement for *entities using a Customized Approach* to perform a targeted risk analysis for each PCI DSS requirement that the entity meets with the customized approach.
	12.3.3 New requirement to document and review cryptographic cipher suites and protocols in use at least once every 12 months.
	12.5.2 New requirement to document and confirm PCI DSS scope at least every 12 months and upon significant change to the in-scope environment.
	12.5.2.1 New requirement **for service providers** service providers confirm PCI DSS scope at least once every six months and upon significant change to the in-scope environment.
	12.6.3.1 New requirement New requirement for security awareness training to include awareness of threats and vulnerabilities that could impact the security of the CDE. **(include phishing and related attacks and social engineering.)**
	12.10.7 New requirement for incident response procedures to be in place and initiated upon detection of stored PAN anywhere it is not expected.

Cr. pcisecuritystandards.org



"

Q&A Time

สแกน QR code เป็นเพื่อนกับเราใน Line official ของ BSI

เพื่อไม่ให้พลาดข่าวสารข้อมูลที่เป็นประโยชน์ในสายอาชีพของท่าน
- Free webinars
- Tool และบทความดีๆ