Payment Card Industry (PCI) Data Security Standard

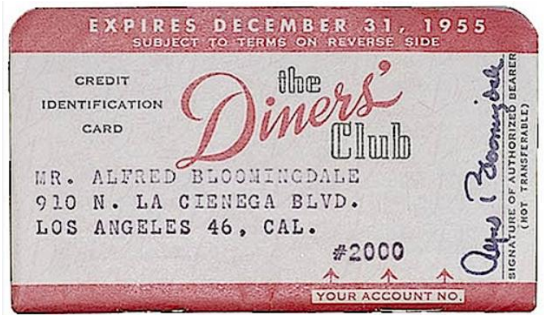
Cập nhật những thay đổi trong Tiêu chuẩn bảo mật dữ liệu thẻ thanh toán PCI-DSS 4.0 và điều kiện để được cấp giấy chứng nhận

Nguyễn Hoàng Tùng
Chuyên gia đánh giá, giảng viên của Học viện Tiêu chuẩn Anh BSI

By Royal Charter

bsi.

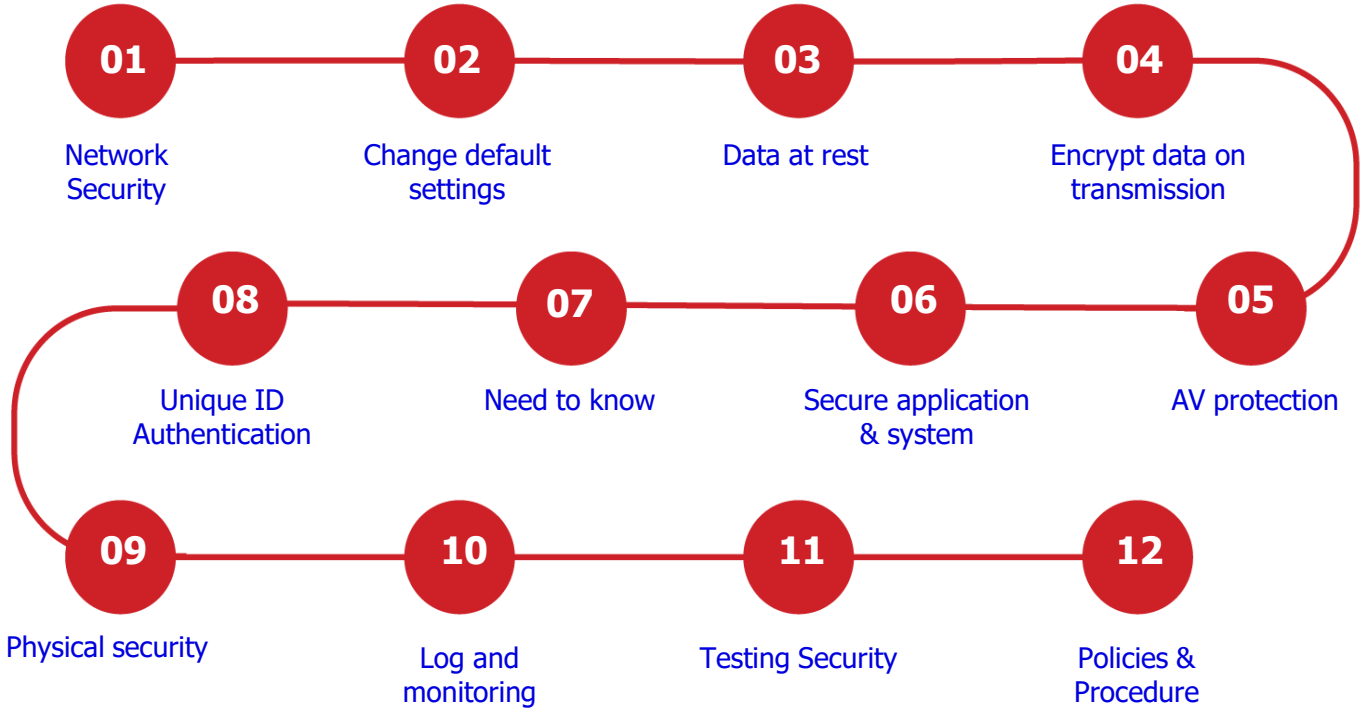
Giới thiệu về bối cảnh ra đời tiêu chuẩn PCI-DSS



PCI-DSS = Payment Card Industry Data Security Standard

Date	Version
October 2008	1.2
July 2009	1.2.1
October 2010	2.0
November 2013	3.0
April 2015	3.1
April 2016	3.2
May 2018	3.2.1
March 2022	4.0

Giới thiệu về cấu trúc tiêu chuẩn PCI-DSS



PCI-DSS = Payment Card Industry Data Security Standard

"PCI DSS là tiêu chuẩn bảo mật dữ liệu thẻ. Tiêu chuẩn áp dụng cho tất cả các tổ chức tham gia vào quá trình xử lý, lưu trữ và truyền gửi dữ liêu thẻ"

bsi.

Các thông tin cần biết khi làm PCI-DSS

Các tài liệu trong Thư viện của PCI

Standard:

- PCI-DSS 4.0
- PCI DSS 4.0 Summary of change

Guidance:

- PCI Scoping and segmentation
- Connected-to service provider
- Virtualization guidelines
- Cloud guidelines
- Effective Daily Log Monitoring
- Penetration Testing Guidance
- Best Practice for Maintaining PCI-DSS
- PCI Glossary

Các Tổ chức đánh giá được cấp phép

- Qualified Security Assessor/ QSA
- Approved Security Vendor / ASV
- PCI Forensics Investigator / PFI
- PCI Professional / Chuyên gia Tư vấn

Những thay đổi của phiên bản 4.0 so với 3.2.1

Có 4 nét mới xuất hiện trong phiên bản 4.0

 # 1 – xuất hiện cách tiếp cận mới mà PCI gọi là Customized Approaches và phụ lục D,E1, E2

 # 2 – 64 yêu cầu mới, trong đó có 1 số cái là mới hoàn toàn, 1 số là điều chỉnh hoặc gộp lại từ các yêu cầu khác.

 # 3 – Hướng dẫn thực hiện được viết chi tiết hơn. Vì phần thực hiện này mà tiêu chuẩn 4.0 dài gần gấp đôi so với tiêu chuẩn 3.2.1

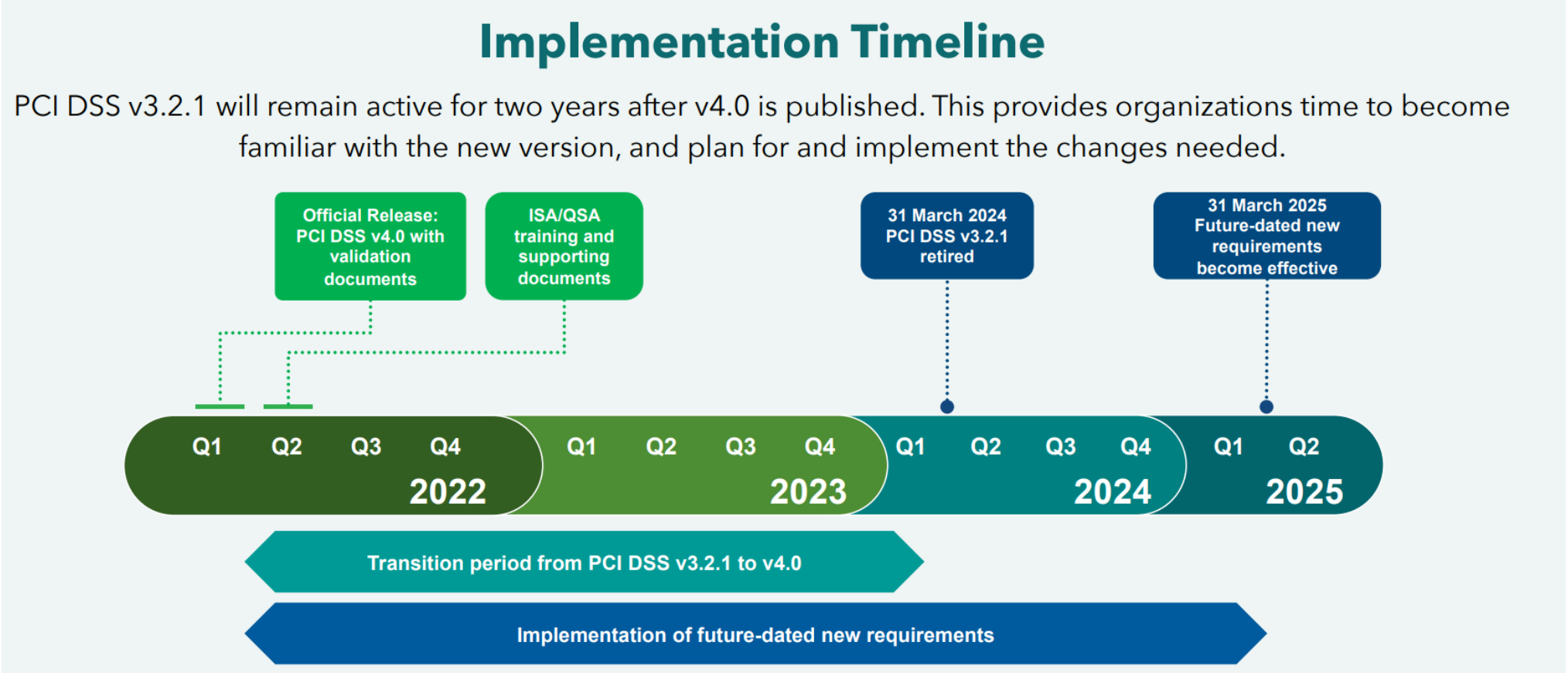
 # 4 – Báo cáo đánh giá ROC và SAQ cho phiên bản mới

Tổng cộng có 64 Yêu cầu mới, trong đó:

- 53 yêu cầu mới là áp dụng cho tất cả các tổ chức (Bank, S.Provider, Merchant)
- 11 yêu cầu mới là chỉ áp dụng cho các đơn vị cung cấp dịch vụ (S.Provider)
- 13 yêu cầu mới là bắt buộc cho các cuộc đánh giá chứng nhận sau ngày **31/3/2024**
- 51 yêu cầu mới là bắt buộc cho các cuộc đánh giá chứng nhận sau ngày **31/3/2025**

bsi.

Lộ trình chuyển đổi PCI-DSS 4.0



Các khoản phạt và chi phí phải trả vì không tuân thủ

Thế giới

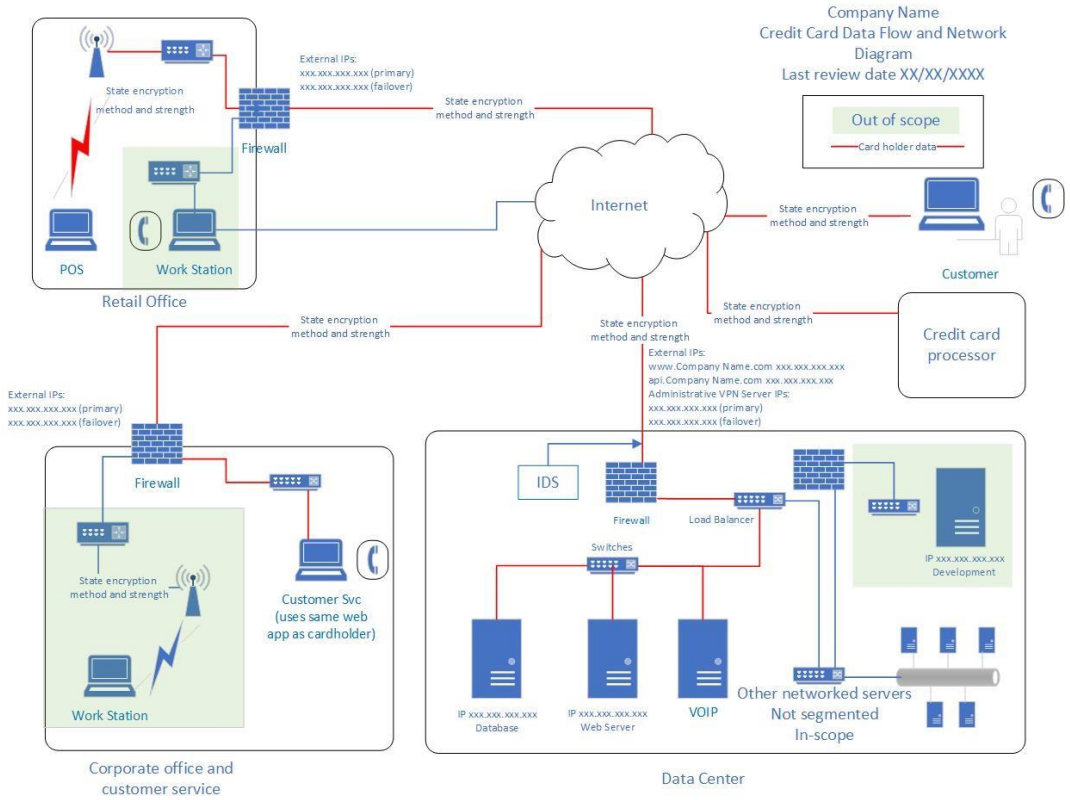
- Tiền phạt do không tuân thủ: $5,000 - $100,000 /tháng tuỳ quy mô DN và mức độ nghiêm trọng
- Tiền làm lại thẻ: $3-5/ card
- Chi phí pháp lý: bên thua sẽ phải chịu chi phí pháp lý
- Chi phí điều tra: Hãng thẻ sẽ chỉ định 1 chuyên gia pháp y máy tính PCI FPI tới điều tra. Tổ chức sẽ phải chịu chi phí này.
- Chi phí cho các giải pháp đắt tiền: để phòng tránh các sự vụ vi phạm tương tự lặp lại, các hãng thẻ có thể sẽ yêu cầu tổ chức đầu tư nhiều giải pháp tiến tiên kèm theo giá bán đắt đỏ.

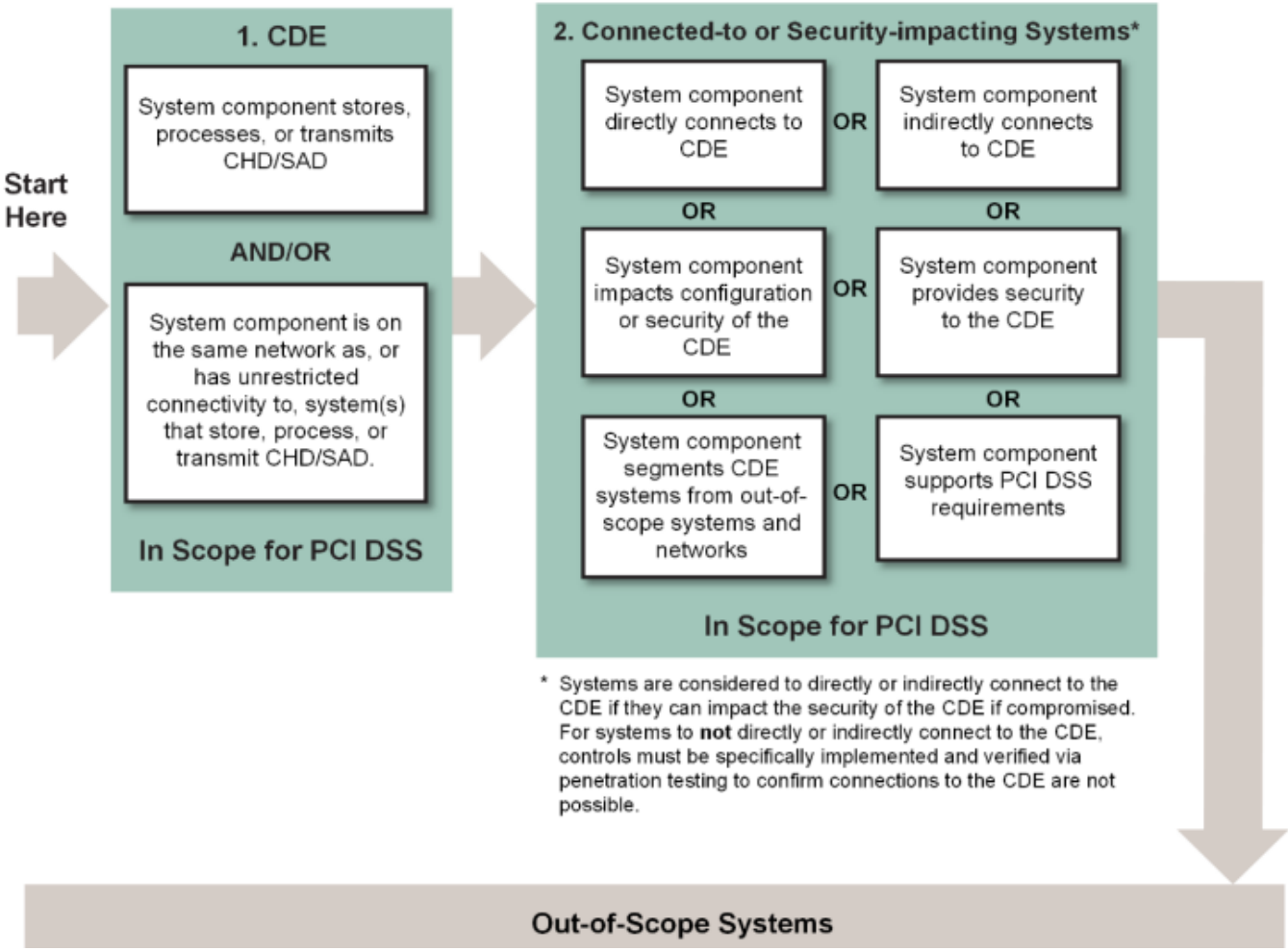
Trong nước

- Hiện chưa có thông tin chính thức công bố 1 cách công khai v/v xử lý vi phạm dữ liệu thẻ.
- Tuy nhiên tương lai gần khi quy định pháp luật Việt Nam về xử lý các vụ việc vi phạm dữ liệu cá nhân được thông qua, thì cũng sẽ áp dụng cho phạm vi sự cố vi phạm dữ liệu thẻ. Do dữ liệu thẻ được tính là 1 loại dữ liệu cá nhân nhạy cảm.
- Tại châu Âu mức phạt có thể lên tới 20 triệu Euro hoặc 4% tổng doanh thu toàn cầu của tổ chức.
- PCI DSS là 1 Framework tốt, có thể dùng để tiếp cận bài toán bảo mật cho các dữ liệu cá nhân khác ngoài dữ liệu thẻ.

bsi.

Xác nhận phạm vi PCI hàng năm, trước đánh giá chứng nhận





Lên kế hoạch đánh giá thử

Mapping yêu cầu PCI với các loại tài sản

- ❑ Thiết bị mạng
- ❑ Hệ thống
- ❑ Ứng dụng, CSDL
- ❑ Nhân sự phụ trách
- ❑ Địa điểm

Table 2: Applicability of PCI DSS Requirements to Assets Type

	PCI DSS Requirements											
	Req. 1	Req. 2	Req. 3	Req. 4	Req. 5	Req. 6	Req. 7	Req. 8	Req. 9	Req. 10	Req. 11	Req. 12
NETWORK EQUIPMENT												
Network Firewall	SP1	SP1				X		SP1		X		X
Network Routers	X	X				X		X		X	X	X
Layer 3 Switch												
Layer 2 Switch												
SDN Switch												
Load Balancer												
IPS/IDS												
WAF												

	PCI DSS Requirements											
	Req. 1	Req. 2	Req. 3	Req. 4	Req. 5	Req. 6	Req. 7	Req. 8	Req. 9	Req. 10	Req. 11	Req. 12
SYSTEMS AND APPLICATIONS												
Applications												
Operating Systems												
Databases												
Antivirus												
Vulnerability Management												
PERSONNEL												
Network Administrator												
System Administrator												
Software Development												
HR												
Legal												
PHYSICAL LOCATIONS												
Head office												
Datacenter												

bsi.

Tham khảo: https://www.pcisecuritystandards.org/document_library/
Best Practices for Maintaining PCI DSS Compliance

Lên kế hoạch Đánh giá thử

PCI có đặc điểm là có nhiều hoạt động được yêu cầu thực hiện Theo định kỳ

Timeframes in PCI DSS Requirements	Descriptions and Examples
Daily	Every day of the year (not only on business days).
Weekly	At least once every seven days.
Monthly	At least once every 30 to 31 days, or on the n^{th} day of the month.
Every three months ("quarterly")	At least once every 90 to 92 days, or on the n^{th} day of each third month.
Every six months	At least once every 180 to 184 days, or on the n^{th} day of each sixth month.
Every 12 months ("annually")	At least once every 365 (or 366 for leap years) days or on the same date every year.
Periodically	Frequency of occurrence is at the entity's discretion and is documented and supported by the entity's risk analysis. The entity must demonstrate that the frequency is appropriate for the activity to be effective and to meet the intent of the requirement.
Immediately	Without delay. In real time or near real time.
Promptly	As soon as reasonably possible.

ID	PCI DSS Requirement	Title	Additional Guidance	Owner[22]	Status	Due Date	Comment
DAILY FREQUENCY							
D-01	10.6.x	Daily security monitoring	Conduct review of security events for: • All security events, • Logs of all system components that store, process or transmit cardholder data (CHD), • Logs of all critical components, and • Logs of all servers & systems that perform security functions (e.g., firewalls, IDS, authentication servers, e-commerce redirection servers).		OK		
D-02	8.1.3	Disable terminated user accounts	Immediately revoke access for any terminated users relating to the CDE.		OK		
D-03	BAU	IT operational checks	Status of **daily** operational checks for systems within the CDE.		OK		
WEEKLY FREQUENCY							
W-01	6.1	Review vulnerability advisories	Weekly review of notifications received from vulnerability alerting and monitoring systems.		OK		
W-02	5.2.c	Review anti-malware operation	Weekly review to confirm that anti-malware signatures are current and periodic scans have completed.		OK		
W-03	10.6.x	Security monitoring	Review logs of all other systems within the CDE not already covered by the daily log monitoring activity (e.g., logs from key security systems outside of CDE).		OK		
W-04	6.6	Review WAF operation	Weekly review to confirm that WAF configuration and signatures are current.		OK		

ID	PCI DSS Requirement	Title	Additional Guidance	Owner[22]	Status	Due Date	Comment
M-05	11.2	Review authorized IP addresses for external and internal scanning	Process to check IP addresses to confirm: • IP addresses match those in the asset inventory for the CDE, and • Presence of unknown IPs identified by the scan.		OK		
M-06	5.2	Monthly anti-virus status review	Review the status of the service from an operational and updates perspective. Where any issues arise, resolve accordingly.		OK		
M-07	8.1.4	Monthly review for inactive user accounts	Run tools/scripts for local user accounts and directory service user accounts to identify accounts that have not been used to login to CDE systems for more than 60 days.		OK		
M-08	10.8	Critical systems failures review	Review, risk analysis and lessons learnt for any critical failures identified by Service and Security Monitoring.		OK		
M-09	BAU	IT operational checks	Status of **monthly** operational checks for systems within the CDE.		OK		
QUARTERLY FREQUENCY							
Q-01	2.4	Review and update asset inventory	Ensure that the data within the asset inventory for the CDE and the actual deployed architecture is consistent—make any changes to the relevant artifacts/assets as necessary.		OK		
Q-02	2.2	Review and update (if needed) configuration standards	Review configuration standards for all system components, ensuring updates as new vulnerability issues are identified.		OK		
Q-03	9.9.1	Review and update payment terminal inventory	Ensure that the inventory for payment terminals is up to date and accurate.		OK		
Q-04	3.1	Secure deletion process review	Review and confirm that CHD that has exceeded its retention period has been securely deleted.		OK		

Tham khảo: https://www.pcisecuritystandards.org/document_library/
Best Practices for Maintaining PCI DSS Compliance

Lựa chọn Cơ quan chứng nhận QSA

- Giấy phép hoạt động của Cty QSA phải còn hiệu lực; chứng chỉ của chuyên gia QSA cũng phải còn hiệu lực.
- Ngoài ra, a/c nên lựa chọn QSA theo kinh nghiệm đánh giá các tổ chức khác trong lĩnh vực kinh doanh của tổ chức.
- QSA cũng nên có cùng văn hóa, địa lý và ngôn ngữ với tổ chức. Vì thường thì các QSA có thể hỗ trợ ngoài đánh giá, giúp tổ chức hiểu cách đạt được và duy trì sự tuân thủ trên cơ sở liên tục.
- Nhiều QSA cũng có thể cung cấp các dịch vụ bổ sung liên quan Rà quét lỗ hổng, kiểm thử xâm nhập, SOC.
- Danh sách các QSA có sẵn tại https://listings.pcisecuritystandards.org/assessors_and_solutions/qualified_security_assessors

Tham khảo: https://listings.pcisecuritystandards.org/assessors_and_solutions/qualified_security_assessors

Đầu ra của đánh giá chứng nhận

Thảo luận về Customized Approach

- Customized Approach là sản phẩm sau đợt xin ý kiến lần thứ 2 của PCI-SSC với cộng đồng. Trước đó, tại lần xem xét thứ nhất thì không có khái niệm này.
- Mục đích của nó là để tổ chức thoải mái mới trong cách lựa chọn công nghệ miễn sao đạt đc mục tiêu mà nó kì vọng.
- Các yêu cầu trong các phiên bản trước mà PCI đưa ra thì bây giờ gọi là "Defined Approach", nó chỉ rõ ra hành động cần thực hiện;
- Còn tại phiên bản mới thì khái niệm customized approach này ko yêu cầu hành động cụ thể, hành động nào cũng được, miễn sao đạt được mục đích.
- Ví dụ Req 5.3.1. Câu trả lời có thể là: thông qua phân tích hành vi mà phần mềm AV có thể phát hiện đc mã độc mới mà không phải thông qua cập nhật.

Defined Approach Requirements
5.3.1 The anti-malware solution(s) is kept current via automatic updates.

Customized Approach Objective
Anti-malware mechanisms can detect and address the latest malware threats.

bsi.

Thảo luận về Compensating Controls

Compensating controls hay Biện pháp kiểm soát bù, là biện pháp tạm thời được QSA chấp nhận sử dụng để hạn chế rủi ro gây ra do hạn chế của công nghệ hoặc hạn chế về kinh doanh của tổ chức

- Ví dụ như 1 hệ thống Legacy sử dụng hệ điều hành AIX/ AS400 không có chức năng mã hoá dữ liệu
- Hay 1 thiết bị appliance không thể cập nhật bản vá HĐH mới.

Việc thiết kế Compensating controls có 3 đặc điểm:

1 – Phải giải quyết được Rủi ro của yêu cầu tương ứng.

2 – có thể sử dụng 1 yêu cầu khác nhưng phải áp dụng 1 cách nghiêm ngặt hơn.

3 – có thể kết hợp nhiều biện pháp khác nhau

Customize Approach hay Compensating Controls

Mục đích là như nhau bởi vì bản chất đều là Biện pháp kiểm soát rủi ro nhưng khác nhau ở bối cảnh sử dụng.

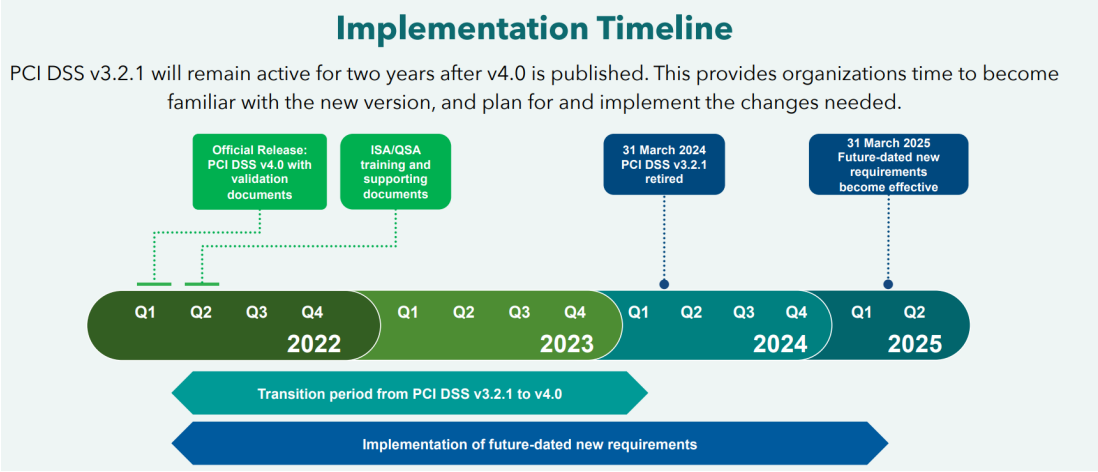
Customized Approach thường sẽ dùng cho các tổ chức mới áp dụng và triển khai PCI DSS, nơi mà tổ chức có điều kiện áp dụng các công nghệ mới hơn ví dụ thay vì giải pháp chống mã độc truyền thống thì có thể áp dụng giải pháp phòng chống mã độc dựa trên phân tích của AI.

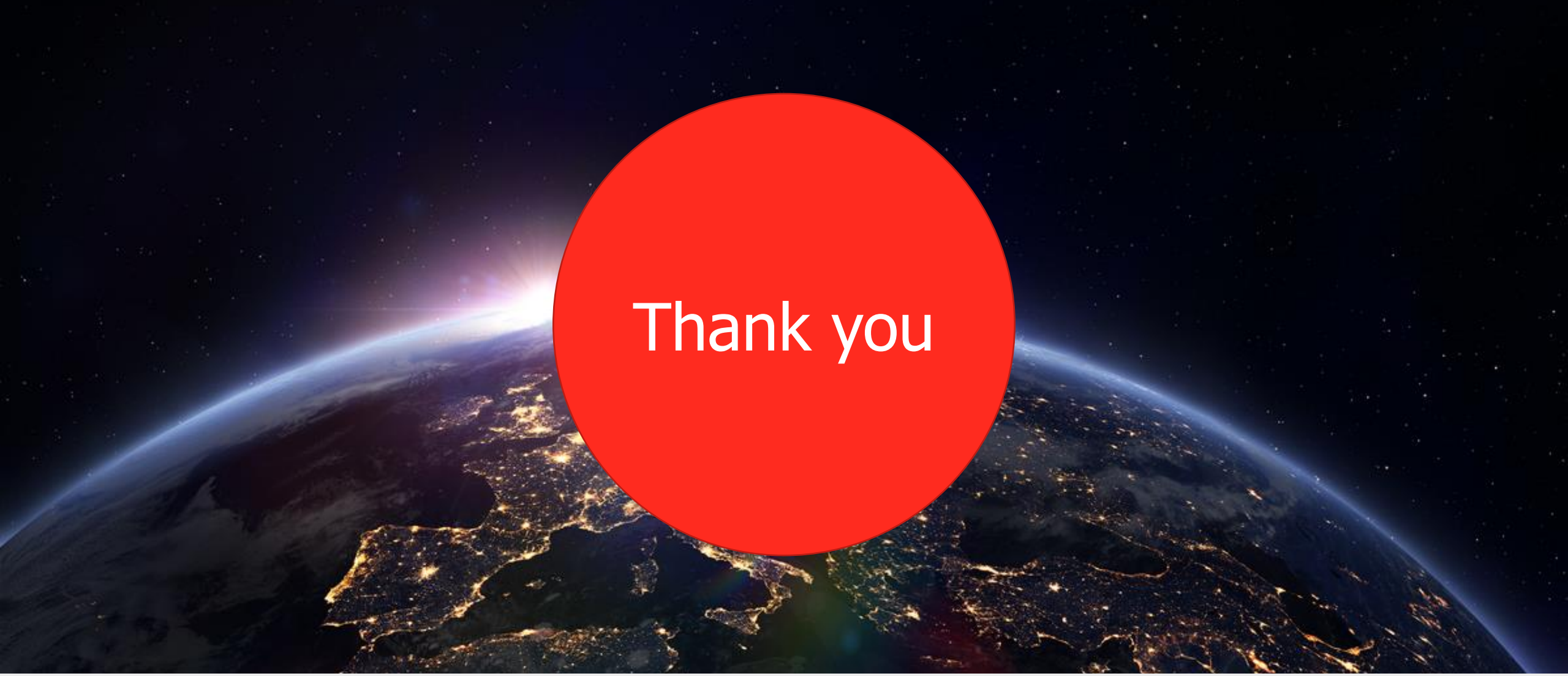
Compensating controls thường được dùng trong bối cảnh tổ chức đã triển khai PCI.

Tiêu chuẩn PCI-DSS đã phát triển được 20 năm, và hiện khá ổn định. Vì vậy, tổ chức nên cân nhắc hơn việc triển khai theo yêu cầu của PCI.

13 Các kiểm soát cần được ưu tiên triển khai trước

- 31 Tháng 3, 2022 → Công bố PCI-DSS 4.0
- 31 Tháng 3, 2024 → Ngày hết hiệu lực PCI-DSS 3.2.1; Mọi cuộc đánh giá chứng nhận phải thực hiện theo tiêu chuẩn PCI-DSS 4.0. Trong đó có 1 số yêu cầu mới chỉ là khuyến nghị, chưa bắt buộc phải tuân thủ.
- 31 Tháng 3, 2025 → Mọi cuộc đánh giá chứng nhận phải theo tiêu chuẩn PCI-DSS 4.0, mọi yêu cầu phải được tuân thủ.





Nếu anh chị có câu hỏi cụ thể hơn liên quan tới công việc triển khai PCI-DSS

Vui lòng liên hệ với BSI. Chúng tôi rất vui nếu có thể giải đáp thắc mắc cho anh chị.

By Royal Charter

bsi.