bsi.

Hội thảo trực tuyến

Cập nhật những thay đổi PCI-DSS 4.0 và những việc cần chuẩn bị để đánh giá chứng nhận

29/ 06/ 2023 | 08:30 – 11:30

Ông Nguyễn Hoàng Tùng
Chuyên gia đánh giá, BSI Việt Nam

Quét mã QR để đăng ký tham dự

By Royal Charter

Payment Card Industry (PCI) Data Security Standard

Cập nhật những thay đổi PCI-DSS 4.0 và những việc cần chuẩn bị để đánh giá chứng nhận

Nguyễn Hoàng Tùng
Chuyên gia đánh giá, đào tạo tiêu chuẩn bảo mật dữ liệu thẻ PCI-DSS

By Royal Charter

bsi.

Giới thiệu về tiêu chuẩn bảo mật dữ liệu thẻ

PCI-DSS = Payment Card Industry Data Security Standard

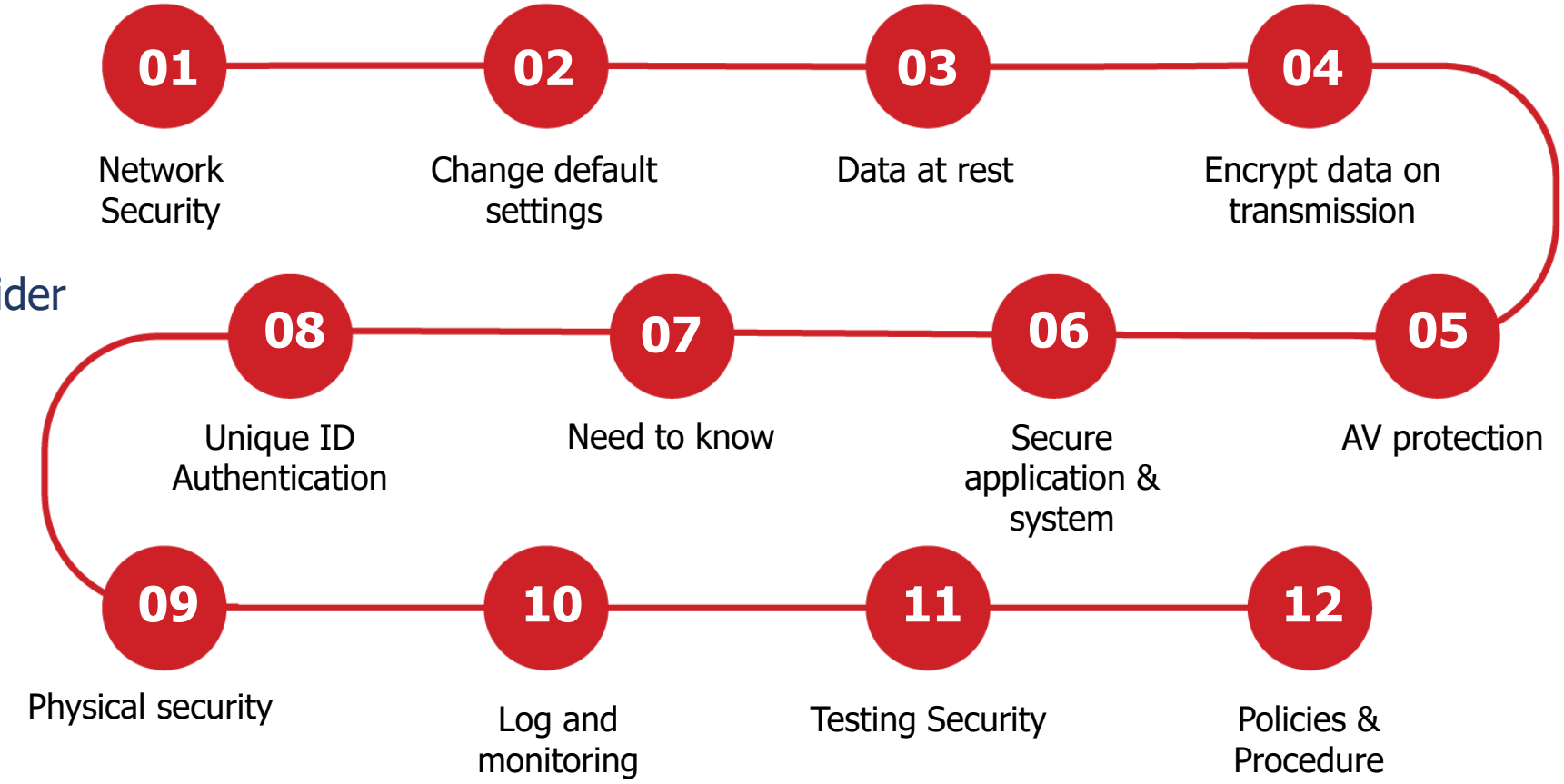
"PCI DSS áp dụng cho tất cả các tổ chức tham gia vào quá trình xử lý thẻ thanh toán — bao gồm Đơn vị chấp nhận thanh toán thẻ, ngân hàng của merchant, ngân hàng chủ thẻ và các đơn vị cung cấp dịch vụ."

Cấu trúc của tiêu chuẩn PCI-DSS

PCI-DSS có 12 yêu cầu lớn, và
3 yêu cầu bổ sung tại phụ lục

Download miễn phí tại:
https://www.pcisecuritystandards.org/document_library

A1 – Multi-tenant Service Provider
A2 – SSL/TLS cũ
A3 – Được chỉ định đặc biệt



Những thay đổi đáng kể 4.0

Tổng cộng có 64 Yêu cầu mới, trong đó:

Tham khảo thêm tại:
https://www.pcisecuritystandards.org/document_library/
Summary of Changes from PCI DSS Version 3.2.1 to 4.0

53 yêu cầu mới là áp dụng cho tất cả các tổ chức

11 yêu cầu mới là chỉ áp dụng cho các đơn vị cung cấp dịch vụ

13 yêu cầu mới là có hiệu ngay lập tức cho mọi cuộc đánh giá theo phiên bản 4.0

51 yêu cầu mới là chỉ có hiệu lực sau ngày **31/3/2025**

Chỉ có Requirement 1 và A2 là không có yêu cầu mới

Các Requirement khác (Req2-12, A1, A3) đều có các yêu cầu mới

14 yêu cầu lớn gồm Req1-12, A1, A2 (A3 ko tính)

65 mục tiêu bảo mật, 260 yêu cầu chi tiết

bsi.

Requirement 1: Install & Maintain Network Security Control

Requirement 1 không có yêu cầu mới so với PCI-DSS 3.2.1.Trong slide này, có 3 nội dung sẽ được đề cập

Thứ nhất là các yêu cầu về tài liệu được đẩy lên đầu tiên. Tư duy này được cho là hợp lý vì các hoạt động phía sau đều chỉ được thực hiện khi đã được cấp có thẩm quyền phê duyệt.

Thứ hai là các yêu cầu về Vai trò Trách nhiệm được định nghĩa. Việc này cũng được cho là hợp lý vì nó thường sẽ nằm trong các văn bản chính sách quy định quy trình

Thứ ba là khái niệm NSC hay thiết bị an ninh mạng được thay thế cho Firewall và Router. Bởi vì có các giải pháp an ninh mạng khác FW, RT truyền thống có thể thực hiện chức năng bảo vệ ở lớp mạng ví dụ Fw ảo hoá gần đây cũng được sử dụng nhiều.

Defined Approach Requirements

1.1.1 All security policies and operational procedures that are identified in Requirement 1 are:

- Documented.
- Kept up to date.
- In use.
- Known to all affected parties.

Defined Approach Requirements

1.1.2 Roles and responsibilities for performing activities in Requirement 1 are documented, assigned, and understood.

6

Requirement 2: Apply Secure Config All Components

Same to PCI-DSS 3.2.1 ngoại trừ

Yêu cầu mới		Áp dụng cho		Ngày có hiệu lực	
		Tất cả các Tổ chức	Chỉ dành cho Đơn vị cung cấp dịch vụ	Ngay lập tức cho tất cả v4.0	31 tháng 3 năm 2025
2.1.2	Vai trò và trách nhiệm thực hiện các hoạt động trong Yêu cầu 2 được lập thành văn bản, được phân công cho nhân sự hoặc phòng ban cụ thể, các nhân sự phụ trách phải hiểu rõ vai trò và trách nhiệm của mình	✓			

7

Requirement 3: Protect Account Data

Yêu cầu mới		Áp dụng cho		Ngày có hiệu lực	
		Tất cả các Tổ chức	Chỉ dành cho Đơn vị cung cấp dịch vụ	Ngay lập tức cho tất cả v4.0	31 tháng 3 năm 2025
3.1.2	Vai trò và trách nhiệm thực hiện các hoạt động trong Yêu cầu 3 được lập thành văn bản, được phân công cho nhân sự hoặc phòng ban cụ thể, các nhân sự phụ trách phải hiểu rõ vai trò và trách nhiệm của mình	✓		✓	
3.2.1	Bất kỳ dữ liệu SAD nào được lưu trữ trước khi hoàn thành Quá trình Phê duyệt 1 giao dịch thẻ đều được giữ ở mức tối thiểu thông qua việc thực hiện các chính sách, thủ tục và quy trình lưu giữ và xử lý dữ liệu.	✓			✓
3.3.2	Dữ liệu SAD được lưu trữ dạng điện tử trước khi hoàn thành Quá trình phê duyệt 1 giao dịch thẻ phải được mã hóa bằng mật mã mạnh.	✓			✓
3.3.3	Dữ liệu SAD được lưu trữ bởi các tổ chức phát hành thẻ phải được mã hóa bằng mật mã mạnh.		✓		✓
3.4.2	Biện pháp Kiểm soát kỹ thuật để ngăn chặn việc sao chép và / hoặc di rời dữ liệu thẻ PAN khi sử dụng các công nghệ truy cập từ xa trừ khi có sự cho phép rõ ràng.	✓			✓
3.5.1.1	Các hàm băm được sử dụng để băm số PAN phải là các hàm băm có yếu tố mật mã. Khoá mật mã của hàm băm này cũng phải tuân thủ quy trình quản lý mã khoá.	✓			✓
3.5.1.2	Triển khai giải pháp mã hóa ổ đĩa hoặc mã hoá phân vùng ổ đĩa khi để biến số PAN thành dữ liệu không thể đọc được khi hiển thị.	✓			✓
3.6.1.1	Tài liệu mô tả Kiến trúc mật mã phải được lập thành văn bản bao gồm việc ngăn chặn sự sử dụng các khóa mật mã trong môi trường vận hành và môi trường thử nghiệm.		✓		✓

Requirement 4: Protect Card Data on Transmission

Same to PCI-DSS ngoại trừ

Yêu cầu mới		Áp dụng cho		Ngày có hiệu lực	
		Tất cả các Tổ chức	Chỉ dành cho Đơn vị cung cấp dịch vụ	Ngay lập tức cho tất cả v4.0	31 tháng 3 năm 2025
4.1.2	Vai trò và trách nhiệm thực hiện các hoạt động trong Yêu cầu 4 được lập thành văn bản, được phân công cho nhân sự hoặc phòng ban cụ thể, các nhân sự phụ trách phải hiểu rõ vai trò và trách nhiệm của mình	✓		✓	
4.2.1	Chứng chỉ được sử dụng để bảo vệ số PAN trong quá trình truyền qua mạng mở, mạng công cộng được xác nhận là hợp lệ và không hết hạn hoặc bị thu hồi.	✓			✓
4.2.1.1	Thiết lập và duy trì cập nhật 1 bảng kiểm kê các mã khóa và chứng chỉ đáng tin cậy.	✓			✓

Requirement 5: Protect Systems Against Malware

Same to PCI-DSS 3.2.1 ngoại trừ:

Yêu cầu mới		Áp dụng cho		Ngày có hiệu lực	
		Tất cả các Tổ chức	Chỉ dành cho Đơn vị cung cấp dịch vụ	Ngay lập tức cho tất cả v4.0	31 tháng 3 năm 2025
5.1.2	Vai trò và trách nhiệm thực hiện các hoạt động trong Yêu cầu 5 được lập thành văn bản, được phân công cho nhân sự hoặc phòng ban cụ thể, các nhân sự phụ trách phải hiểu rõ vai trò và trách nhiệm của mình	✓		✓	
5.2.3.1	Phân tích rủi ro mục tiêu để xác định tần suất đánh giá định kỳ các thành phần hệ thống được xác định là không có nguy cơ bị phần mềm độc hại.	✓			✓
5.3.2.1	Phân tích rủi ro mục tiêu để xác định tần suất dò quét phần mềm độc hại.	✓			✓
5.3.3	Dò quét phần mềm độc hại được thực hiện khi sử dụng phương tiện điện tử di động.	✓			✓
5.4.1	Các cơ chế được áp dụng để phát hiện và bảo vệ nhân viên phòng chống các nguy cơ bị tấn công lừa đảo.	✓			✓

Requirement 6:Dev & Maintain secure System Software

Same to PCI-DSS 3.2.1 ngoại trừ:

Yêu cầu mới		Áp dụng cho		Ngày có hiệu lực	
		Tất cả các Tổ chức	Chỉ dành cho Đơn vị cung cấp dịch vụ	Ngay lập tức cho tất cả v4.0	31 tháng 3 năm 2025
6.1.2	Vai trò và trách nhiệm thực hiện các hoạt động trong Yêu cầu 6 được lập thành văn bản, được phân công cho nhân sự hoặc phòng ban cụ thể, các nhân sự phụ trách phải hiểu rõ vai trò và trách nhiệm của mình	✓		✓	
6.3.2	Duy trì hàng bảng kiểm kê các phần mềm ứng dụng để tạo cơ sở cho việc quản lý lỗ hổng và bản vá.	✓			✓
6.4.2	Triển khai giải pháp kỹ thuật tự động để phát hiện và ngăn chặn các cuộc tấn công dựa trên web cho các ứng dụng web public ra ngoài	✓			✓
6.4.3	Quản lý tất cả các tập lệnh trang thanh toán được tải và thực thi trong trình duyệt của người dùng.	✓			✓

Requirement 7

Same to PCI-DSS 3.2.1 ngoại trừ:

Yêu cầu mới		Áp dụng cho		Ngày có hiệu lực	
		Tất cả các Tổ chức	Chỉ dành cho Đơn vị cung cấp dịch vụ	Ngay lập tức cho tất cả v4.0	31 tháng 3 năm 2025
7.1.2	Vai trò và trách nhiệm thực hiện các hoạt động trong Yêu cầu 7 được lập thành văn bản, được phân công cho nhân sự hoặc phòng ban cụ thể, các nhân sự phụ trách phải hiểu rõ vai trò và trách nhiệm của mình	✓		✓	
7.2.4	Rà soát tài khoản người dùng và quyền truy cập	✓			✓
7.2.5	Gán và quản lý tất cả các tài khoản ứng dụng và tài khoản hệ thống với các quyền truy cập 1 cách thích hợp	✓			✓
7.2.5.1	Rà soát tất cả quyền truy cập theo tài khoản ứng dụng và tài khoản hệ thống cũng như các đặc quyền truy cập liên quan.	✓			✓

Requirement 8:

Yêu cầu mới		Áp dụng cho		Ngày có hiệu lực	
		Tất cả các Tổ chức	Chỉ dành cho Đơn vị cung cấp dịch vụ	Ngay lập tức cho tất cả v4.0	31 tháng 3 năm 2025
8.1.2	Vai trò và trách nhiệm thực hiện các hoạt động trong Yêu cầu 8 được lập thành văn bản, được phân công cho nhân sự hoặc phòng ban cụ thể, các nhân sự phụ trách phải hiểu rõ vai trò và trách nhiệm của mình	✓		✓	
8.3.6	Mức độ phức tạp tối thiểu đối với mật khẩu khi được sử dụng làm yếu tố xác thực: 12 ký tự gồm số và chữ cái	✓			✓
8.3.10.1	Nếu mật khẩu / cụm mật khẩu là yếu tố xác thực duy nhất để xác thực người dùng, mật khẩu / cụm mật khẩu được thay đổi ít nhất 90 ngày một lần hoặc tình trạng bảo mật của tài khoản được phân tích động để xác định quyền truy cập tài nguyên theo thời gian thực.		✓		✓
8.4.2	Xác thực đa nhân tố cho tất cả quyền truy cập vào CDE.	✓			✓
8.5.1	Hệ thống xác thực đa nhân tố được triển khai đảm bảo an toàn.	✓			✓
8.6.1	Quản lý đăng nhập tương tác cho các tài khoản hệ thống hoặc tài khoản ứng dụng.	✓			✓
8.6.2	Mật khẩu / cụm mật khẩu được sử dụng để đăng nhập tương tác cho tài khoản ứng dụng và hệ thống phải được bảo vệ, không lưu trong các file cấu hình hoặc mã nguồn phần mềm.	✓			✓
8.6.3	Mật khẩu / cụm mật khẩu cho bất kỳ tài khoản ứng dụng và hệ thống nào được bảo vệ, bằng cách định kỳ thay đổi, mật khẩu phải mạnh.	✓			✓

Requirement 9:

Same to PCI-DSS 3.2.1 ngoại trừ:

Yêu cầu mới		Áp dụng cho		Ngày có hiệu lực	
		Tất cả các Tổ chức	Chỉ dành cho Đơn vị cung cấp dịch vụ	Ngay lập tức cho tất cả v4.0	31 tháng 3 năm 2025
9.1.2	Vai trò và trách nhiệm thực hiện các hoạt động trong Yêu cầu 9 được lập thành văn bản, được phân công cho nhân sự hoặc phòng ban cụ thể, các nhân sự phụ trách phải hiểu rõ vai trò và trách nhiệm của mình	✓		✓	
9.5.1.2.1	Phân tích rủi ro mục tiêu được thực hiện để xác định tần suất kiểm tra thiết bị POI định kỳ.	✓			✓

Requirement 10

Yêu cầu mới		Áp dụng cho		Ngày có hiệu lực	
		Tất cả các Tổ chức	Chỉ dành cho Đơn vị cung cấp dịch vụ	Ngay lập tức cho tất cả v4.0	31 tháng 3 năm 2025
10.1.2	Vai trò và trách nhiệm thực hiện các hoạt động trong Yêu cầu 10 được lập thành văn bản, được phân công cho nhân sự hoặc phòng ban cụ thể, các nhân sự phụ trách phải hiểu rõ vai trò và trách nhiệm của mình	✓		✓	
10.4.1.1	Áp dụng các công cụ để soát xét nhật ký 1 cách tự động (log harvesting, parsing, and alerting tools, centralized log management systems, event log analyzers, and security information and event management (SIEM) solutions)	✓			✓
10.4.2.1	Phân tích rủi ro mục tiêu được thực hiện để xác định tần suất soát xét nhật ký cho tất cả các thành phần hệ thống.	✓			✓
10.7.2	Sai lỗi của 10 hệ thống kiểm soát an ninh quan trọng được cần được phát hiện, cảnh báo và giải quyết kịp thời	✓			✓
10.7.3	7 bước Phản ứng kịp thời với sai lỗi của các hệ thống kiểm soát an ninh quan trọng	✓			✓

Requirement 11

Yêu cầu mới		Áp dụng cho		Ngày có hiệu lực	
		Tất cả các Tổ chức	Chỉ dành cho Đơn vị cung cấp dịch vụ	Ngay lập tức cho tất cả v4.0	31 tháng 3 năm 2025
10.1.2	Vai trò và trách nhiệm thực hiện các hoạt động trong Yêu cầu 10 được lập thành văn bản, được phân công cho nhân sự hoặc phòng ban cụ thể, các nhân sự phụ trách phải hiểu rõ vai trò và trách nhiệm của mình	✓		✓	
10.4.1.1	Áp dụng các công cụ để soát xét nhật ký 1 cách tự động (log harvesting, parsing, and alerting tools, centralized log management systems, event log analyzers, and security information and event management (SIEM) solutions)	✓			✓
10.4.2.1	Phân tích rủi ro mục tiêu được thực hiện để xác định tần suất soát xét nhật ký cho tất cả các thành phần hệ thống.	✓			✓
10.7.2	Sai lỗi của 10 hệ thống kiểm soát an ninh quan trọng được cần được phát hiện, cảnh báo và giải quyết kịp thời	✓			✓
10.7.3	7 bước Phản ứng kịp thời với sai lỗi của các hệ thống kiểm soát an ninh quan trọng	✓			✓
10.1.2	Vai trò và trách nhiệm thực hiện các hoạt động trong Yêu cầu 10 được lập thành văn bản, được phân công cho nhân sự hoặc phòng ban cụ thể, các nhân sự phụ trách phải hiểu rõ vai trò và trách nhiệm của mình	✓		✓	

Requirement 12

Yêu cầu mới		Áp dụng cho		Ngày có hiệu lực	
		Tất cả các Tổ chức	Chỉ dành cho Đơn vị cung cấp dịch vụ	Ngay lập tức cho tất cả v4.0	31 tháng 3 năm 2025
12.3.1	Phân tích rủi ro mục tiêu được lập thành văn bản để hỗ trợ từng yêu cầu PCI DSS cung cấp sự linh hoạt về tần suất thực hiện.	✓			✓
12.3.2	Phân tích rủi ro mục tiêu được thực hiện cho từng yêu cầu PCI DSS được đáp ứng với phương pháp tùy chỉnh.	✓		✓	
12.3.3	Các bộ mật mã và giao thức mật mã được sử dụng phải được lập thành văn bản và được xem xét hàng năm.	✓			✓
12.3.4	Công nghệ phần cứng và phần mềm được xem xét tối thiểu hàng năm.	✓			✓
12.5.2	Phạm vi PCI DSS được lập thành và cập nhật hàng năm hoặc khi có thay đổi đáng kể.	✓		✓	
12.5.2.1	Phạm vi PCI DSS được ghi lại và xác nhận ít nhất sáu tháng một lần và khi có những thay đổi đáng kể.		✓		✓
12.5.3	Những thay đổi đáng kể về cơ cấu tổ chức đối với phạm vi PCI DSS phải được lập thành văn bản và được truyền đạt cho Lãnh đạo cấp cao của tổ chức.		✓		✓
12.6.2	Chương trình nâng cao nhận thức về an toàn thông tin được xem xét ít nhất 12 tháng một lần và được cập nhật khi cần thiết.	✓			✓

Requirement 12

Yêu cầu mới		Áp dụng cho		Ngày có hiệu lực	
		Tất cả các Tổ chức	Chỉ dành cho Đơn vị cung cấp dịch vụ	Ngay lập tức cho tất cả v4.0	31 tháng 3 năm 2025
12.6.3.1	Nội dung đào tạo nâng cao nhận thức về bảo mật bao gồm nhận thức về các mối đe dọa có thể ảnh hưởng đến an toàn của môi trường CDE và các hình thức lừa đảo mới nhắm tới nhân viên của tổ chức.	✓			✓
12.6.3.2	Đào tạo nâng cao nhận thức bảo mật bao gồm nhận thức về việc sử dụng an toàn các công nghệ mà người dùng cuối được phép sử dụng.	✓			✓
12.9.2	TPSP hỗ trợ yêu cầu của khách hàng để cung cấp trạng thái tuân thủ PCI DSS và thông tin về các yêu cầu PCI DSS thuộc trách nhiệm của TPSP.		✓	✓	
12.10.4.1	Một Phân tích rủi ro mục tiêu được thực hiện để xác định tần suất đào tạo định kỳ cho nhân sự tham gia quá trình ứng phó sự cố của tổ chức.	✓			✓
12.10.5	Kế hoạch ứng phó sự cố an toàn thông tin bao gồm các cảnh báo từ cơ chế phát hiện thay đổi và giả mạo cho các trang thanh toán.	✓			✓
12.10.7	Các quy trình ứng phó sự cố được áp dụng và bắt đầu khi phát hiện PAN.	✓			✓

Appendix A1

Same to PCI-DSS 3.2.1 ngoại trừ:

Yêu cầu mới		Áp dụng cho		Ngày có hiệu lực	
		Tất cả các Tổ chức	Chỉ dành cho Đơn vị cung cấp dịch vụ	Ngay lập tức cho tất cả v4.0	31 tháng 3 năm 2025
A1.1.1	Nhà cung cấp dịch vụ xác nhận các truy cập vào và từ môi trường khách hàng được tách biệt một cách hợp lý để ngăn chặn truy cập trái phép.		✓		✓
A1.1.4	Nhà cung cấp dịch vụ xác nhận tính hiệu lực của các biện pháp phân tách môi trường giữa các khách hàng định kỳ sáu tháng một lần thông qua kiểm thử thâm nhập.		✓		✓
A1.2.3	Nhà cung cấp dịch vụ thực hiện các quy trình hoặc cơ chế để báo cáo và giải quyết các sự cố và lỗ hổng bảo mật bị nghi ngờ hoặc đã xác nhận.		✓		✓

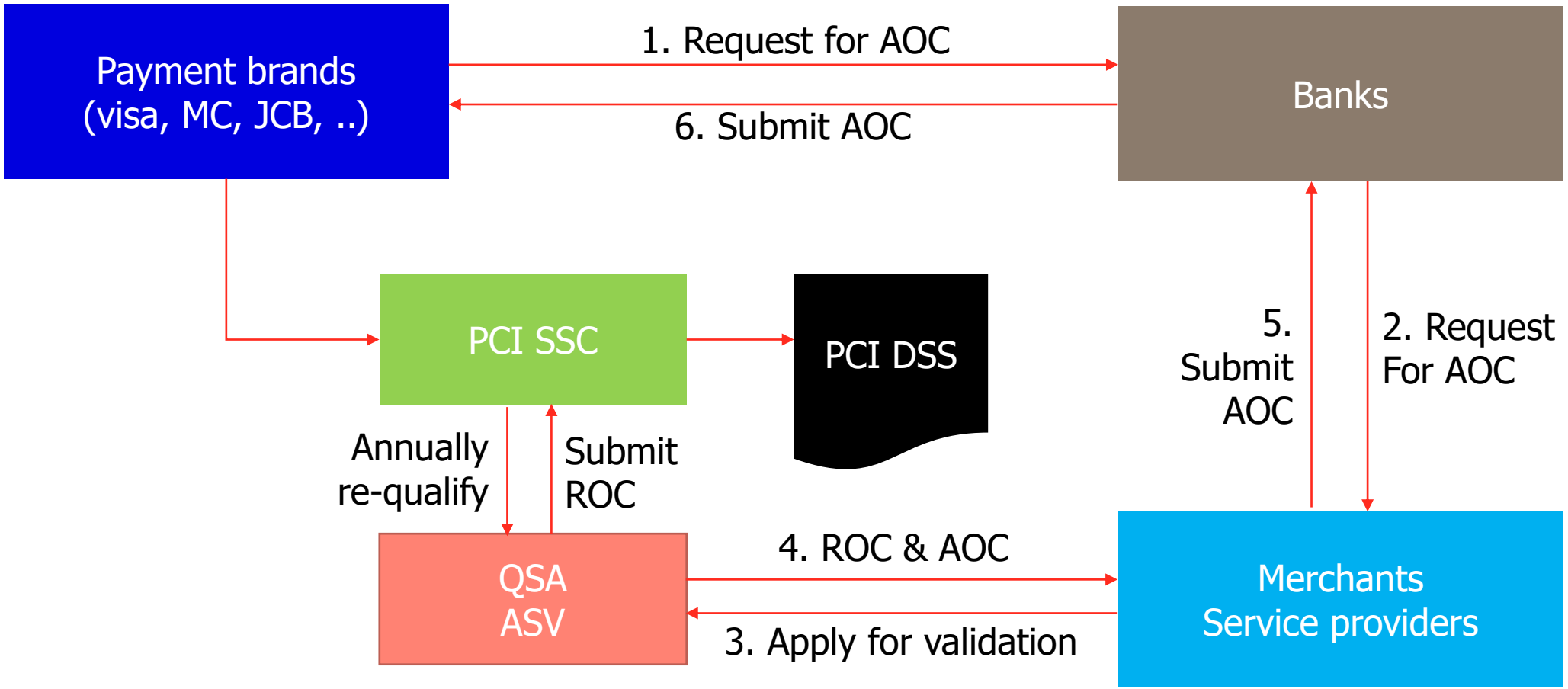
Appendix A3

Same to PCI-DSS 3.2.1 ngoại trừ:

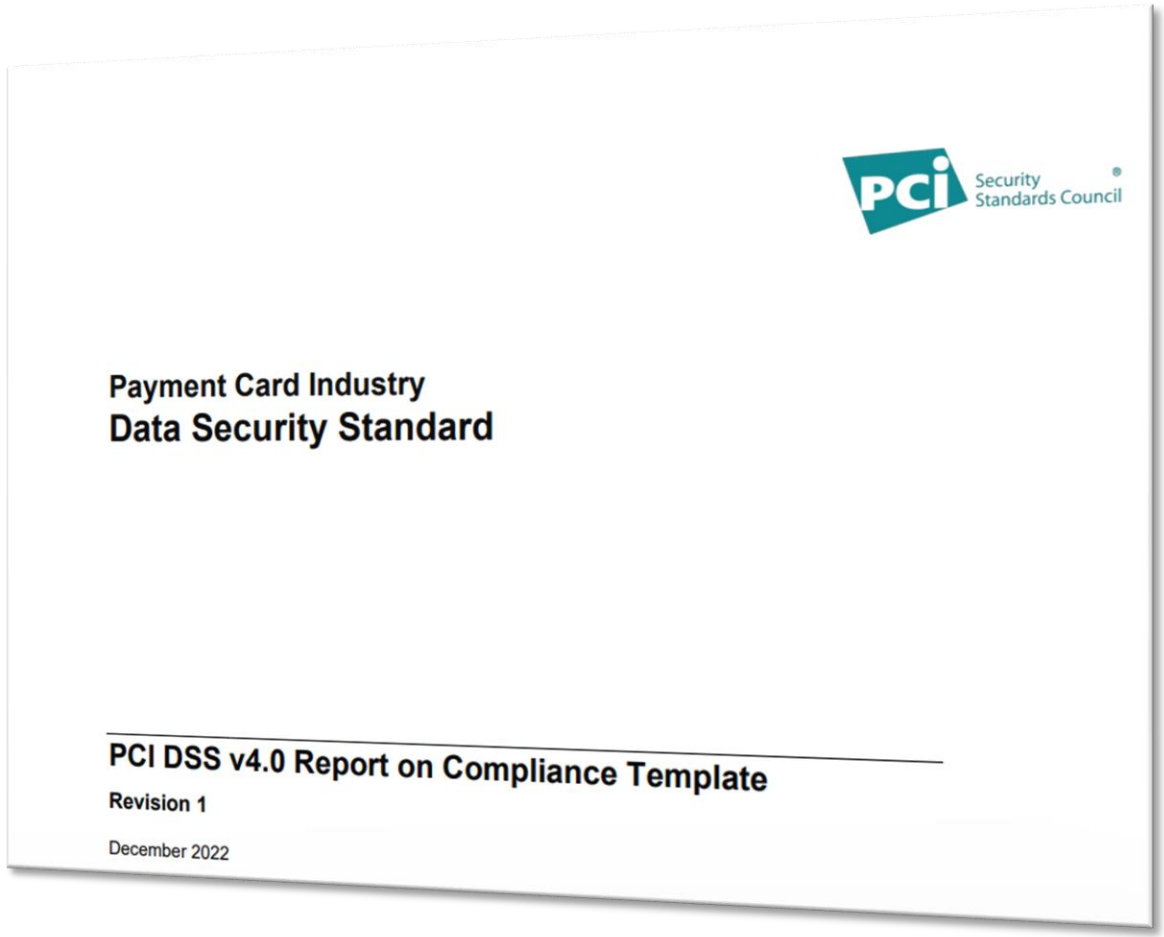
Yêu cầu mới		Áp dụng cho		Ngày có hiệu lực	
		Tất cả các Tổ chức	Chỉ dành cho Đơn vị cung cấp dịch vụ	Ngay lập tức cho tất cả v4.0	31 tháng 3 năm 2025
A3.3.1	Sai lỗi của 10 hệ thống kiểm soát an ninh được phát hiện, cảnh báo và báo cáo kịp thời	✓			✓

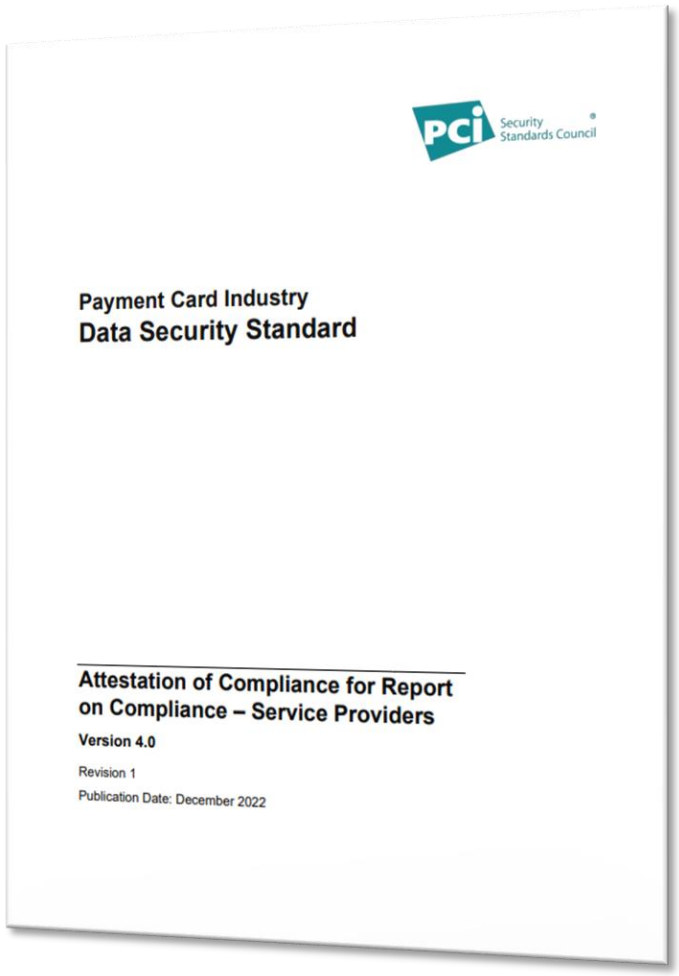
Các công việc cần chuẩn bị cho đánh giá chứng nhận

Cơ chế chứng nhận



Đầu ra của đánh giá tuân thủ





Lựa chọn Cơ quan Chứng nhận QSA

- QSA mà bạn chọn phải có hiểu biết về lĩnh vực hoạt động của tổ chức. Vì các đánh giá sẽ luôn xoay quanh các nghiệp vụ liên quan đến thẻ. Ngoài ra QSA cũng phải có kinh nghiệm trong việc đánh giá của các loại hình doanh nghiệp tương tự.
- QSA cũng nên phù hợp với văn hóa, vị trí địa lý, ngôn ngữ. Mặc dù đánh giá sẽ kết luận liệu các yêu cầu của PCI DSS có được đáp ứng hay không, các QSA có thể cung cấp hỗ trợ ngoài đánh giá, làm việc với tổ chức của bạn để giúp bạn 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 đến bảo mật như đánh giá và khắc phục lỗ hổng đang diễn ra.
- Danh sách các QSA có sẵn tại https://listings.pcisecuritystandards.org/assessors_and_solutions/qualified_security_assessors

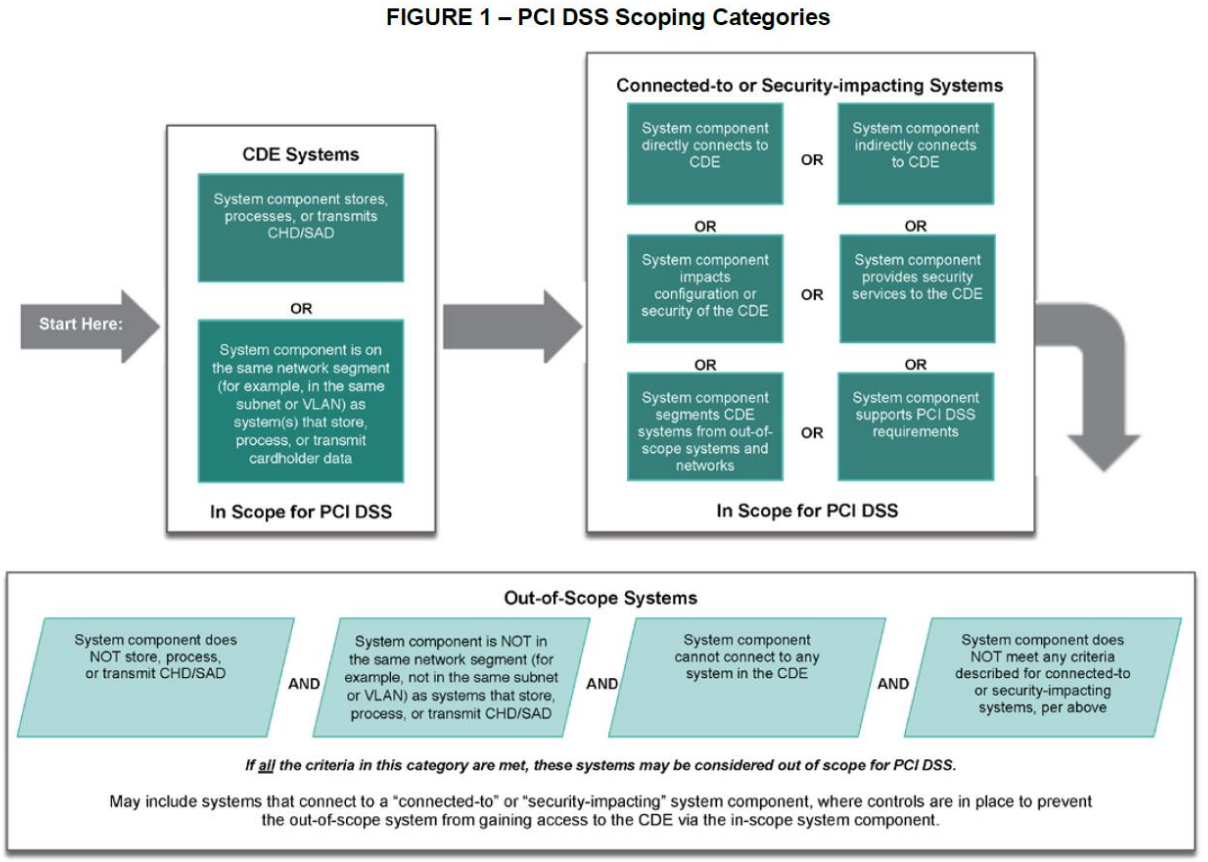
bsi.

Cập nhật tài sản mới nhất trong phạm vi PCI

Tham khảo: https://www.pcisecuritystandards.org/document_library/
PCI-DSS 4.0

Cập nhật các tài liệu:
- Network Diagram
- Dataflow Diagram
- Asset Inventory
- Card Data Matrix
- List of VLANs
- List of ATM, POS
- List of Branches

QSA sẽ xác nhận lại phạm vi đánh giá trước Cuộc đánh giá



Xác định nhân sự đối ứng với QSA

Mục tiêu đánh giá là tìm kiếm bằng chứng cho sự
Phù hợp/ tuân thủ đối với yêu cầu tiêu chuẩn. Bằng chứng
Được thu thập qua 3 phương pháp: phỏng vấn,
xem xét hồ sơ tài liệu, Và kiểm tra cấu hình thiết bị

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

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.

Thảo luận về Compensating Controls

Compensating controls hay Biện pháp kiểm soát bù, là biện pháp ngắn hạn 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 nên chưa thể đáp ứng chính xác yêu cầu của tiêu chuẩn.

- 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.

Compensating Control sẽ được sử dụng trong trường hợp này. QSA sẽ giúp tổ chức thiết kế Compensating control phù hợp.
Compensating controls có 3 đặc điểm:

1 – Phải giải quyết được Rủi ro của yêu cầu tương ứng. Ví dụ khi thiết kế CC cho yêu cầu mã hoá thông tin đăng nhập trên đường truyền, khi chưa thế triển khai mã hoá trên đường truyền ngay như yêu cầu, thì các biện pháp như độ phức tạp của mật khẩu ko 'compensate' được cái rủi ro đang đối mặt
2 – có thể sử dụng 1 yêu cầu khác nhưng phải áp dụng 1 cách nghiêm ngặt hơn tại những tài sản/ khu vực chưa đáp ứng chính xác yêu cầu. Ví dụ định kỳ rà quét lỗ hổng yêu cầu hàng quý thì nay có thể sẽ phải thực hiện hàng tháng
3 – có thể sẽ phải triển khai nhiều biện pháp khác nhau. Ví dụ: nếu một công ty không thể cập nhật lỗ hổng vì bản cập nhật bảo mật chưa có sẵn từ nhà cung cấp, biện pháp kiểm soát bù có thể bao gồm các biện pháp kiểm soát sau: 1) phân vùng mạng nội bộ, 2) giới hạn quyền truy cập mạng vào giao diện dễ bị tổn thương chỉ đối với các thiết bị được yêu cầu (lọc địa chỉ IP hoặc địa chỉ MAC) và 3) IDS/IPS giám sát tất cả lưu lượng truy cập đến giao diện dễ bị tấn công.

Customize Approach hay Compensating Controls

Mục đích là như nhau bởi vì bản chất đều là Biện pháp kiểm soát rủi ro.

Nó khác nhau ở bối cảnh được sử dụng.

Customized Approach thường sẽ dùng cho các tổ chức mới triển khai PCI hơn, nơi mà các biện pháp kiểm soát sẽ được hoạch định để triển khai. Vì vậy các 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 rồi và vẫn đang duy trì các biện pháp kiểm soát truyền thống.

Tiêu chuẩn PCI-DSS đã được 20 năm tuổi, hiện đã khá ổn định. Nhiều tổ chức lớn bé áp dụng 1 thời gian đã lâu. Vì vậy những yêu cầu PCI đưa ra là đã qua 1 thời gian chứng thực rằng nó hiệu quả và có thể áp dụng tại đại đa số các tổ chức. Vì vậy, tổ chức nên cân nhắc các yêu cầu của PCI, xem xét đó là trạng thái mong đợi. Trong quá trình đánh giá gap nếu như có các điểm không phù hợp yêu cầu của PCI thì tổ chức hay cân nhắc 1 trong 2 phương án: customized approach hay compensating controls

Appendix B,C: Compensating Controls

1) Phân đoạn mạng nội bộ,

2) Giới hạn quyền truy cập mạng vào giao diện dễ bị tổn thương chỉ cho các thiết bị được yêu cầu (lọc địa chỉ IP hoặc địa chỉ MAC) và

3) IDS/IPS giám sát tất cả lưu lượng truy cập đến giao diện dễ bị tấn công.

5. Giải quyết rủi ro bổ sung do không tuân thủ yêu cầu PCI DSS.

6. Giải quyết yêu cầu hiện tại và trong tương lai. Kiểm soát bù không thể giải quyết một yêu cầu đã bị bỏ lỡ trong quá khứ(ví dụ: khi yêu cầu thực hiện một nhiệm vụ hai phần tư trước, nhưng nhiệm vụ đó đã không được thực hiện).

Người đánh giá được yêu cầu đánh giá kỹ lưỡng các biện pháp kiểm soát bù trừ trong mỗi lần đánh giá PCI DSS hàng năm để xác nhận rằng mỗi biện pháp kiểm soát bù trừ giải quyết thỏa đáng rủi ro mà yêu cầu PCI DSS ban đầu được thiết kế để giải quyết, theo các mục 1-6 ở trên. Để duy trì sự tuân thủ, các quy trình và biện pháp kiểm soát phải được thực hiện để đảm bảo các biện pháp kiểm soát bù trừ vẫn có hiệu lực sau khi đánh giá hoàn tất. Ngoài ra, kết quả kiểm soát bù phải được được ghi lại trong báo cáo áp dụng cho đánh giá (ví dụ: Báo cáo về Tuân thủ hoặc Bảng câu hỏi Tự đánh giá) trong phần yêu cầu PCI DSS tương ứng và được đưa vào khi báo cáo áp dụng được gửi cho tổ chức yêu cầu.

Các việc sẽ phải thực hiện với Customized Approach

Tổ chức triển khai phương pháp tùy chỉnh phải đáp ứng các tiêu chí sau:

Ma trận Kiểm soát theo Phụ lục E1.

Phân tích rủi ro mục tiêu (Yêu cầu PCI DSS 12.3.2) cho từng kiểm soát tùy chỉnh, theo Phụ lục E2.

Tiến hành Test từng kiểm soát tùy chỉnh để chứng minh tính hiệu lực và kiểm tra tài liệu được thực hiện, các phương pháp được sử dụng, những gì đã được kiểm tra, khi thử nghiệm được thực hiện và kết quả thử nghiệm trong ma trận kiểm soát.

Theo dõi và duy trì bằng chứng về tính hiệu quả của từng biện pháp kiểm soát tùy chỉnh.

Cung cấp (các) ma trận kiểm soát hoàn chỉnh, phân tích rủi ro mục tiêu, bằng chứng kiểm tra và bằng chứng về hiệu quả kiểm soát tùy chỉnh cho giám định viên.

QSA company đánh giá phải đáp ứng các tiêu chí sau:

- Xem xét (các) ma trận kiểm soát của tổ chức, phân tích rủi ro được nhắm mục tiêu và bằng chứng về hiệu quả kiểm soát để hiểu đầy đủ (các) kiểm soát tùy chỉnh và để xác minh Tổ chức đáp ứng tất cả các yêu cầu về bằng chứng và tài liệu Phương pháp tiếp cận tùy chỉnh.
- Xuất phát và ghi lại các quy trình thử nghiệm phù hợp cần thiết để tiến hành thử nghiệm kỹ lưỡng từng Kiểm soát tùy chỉnh.
- Kiểm tra từng Kiểm soát tùy chỉnh để xác định xem việc triển khai của Tổ chức 1) đáp ứng Mục tiêu tiếp cận tùy chỉnh của yêu cầu và 2) dẫn đến kết quả tìm kiếm "in-place" cho yêu cầu.
- Tại mọi thời điểm, các QSA luôn duy trì các yêu cầu về tính độc lập được xác định trong Yêu cầu Đủ điều kiện của QSA. Điều này có nghĩa là nếu một QSA tham gia vào việc thiết kế hoặc triển khai một biện pháp kiểm soát tùy chỉnh, thì QSA đó cũng không đưa ra các quy trình thử nghiệm để đánh giá, đánh giá hoặc hỗ trợ việc đánh giá biện pháp kiểm soát tùy chỉnh đó.

bsi.

Các việc sẽ phải thực hiện với Compensating controls

Tổ chức có thể nhờ sự giúp đỡ của QSA
Để thiết lập Compensating Controls.

Tại cuộc đánh giá chứng nhận, QSA sẽ
Kiểm tra hiệu lực của các biện pháp
Kiểm soát theo compensating control đã
Thiết kế.

Tham khảo Phụ lục B,C tiêu chuẩn PCI-DSS 4.0

Requirement Number and Definition:

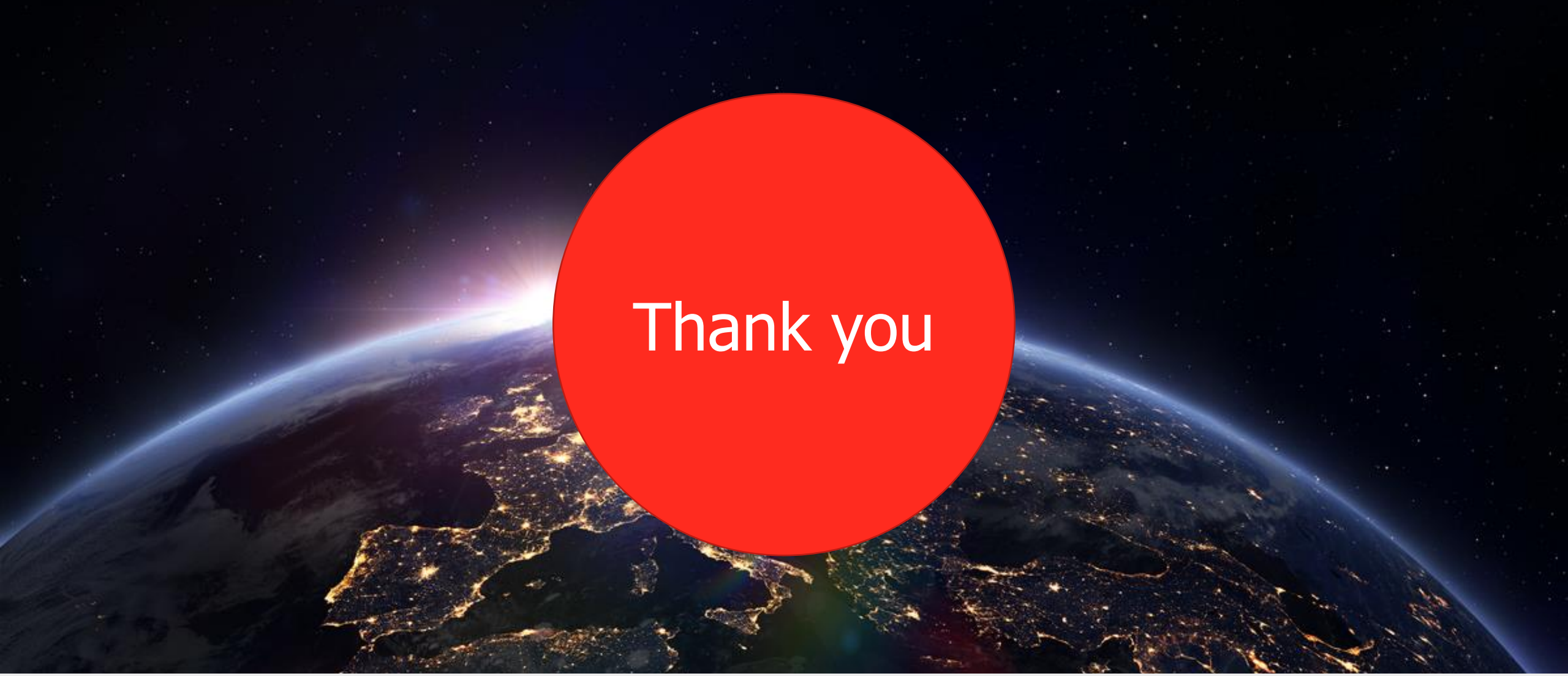
	Information Required	Explanation
1. Constraints	Document the legitimate technical or business constraints precluding compliance with the original requirement.	
2. Definition of Compensating Controls	Define the compensating controls: explain how they address the objectives of the original control and the increased risk, if any.	
3. Objective	Define the objective of the original control (for example, the Customized Approach Objective).	
	Identify the objective met by the compensating control *(note: this can be, but is not required to be, the stated Customized Approach Objective for the PCI DSS requirement)*.	
4. Identified Risk	Identify any additional risk posed by the lack of the original control.	
5. Validation of Compensating Controls	Define how the compensating controls were validated and tested.	
6. Maintenance	Define process(es) and controls in place to maintain compensating controls.	

Lộ trình chuyển đổi sang phiên bản 4.0

- 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.

Checklist

1) Cập nhật mới nhất các tài liệu sau: danh mục tài sản, sơ đồ mạng, sơ đồ luồng dữ liệu thẻ, ma trận dữ liệu thẻ, danh sách các VLANs trong phạm vi
2) Làm việc trước với các đầu mối tại các phòng ban sẽ đối ứng trong cuộc đánh giá để làm quen lại với cách thức trao đổi thông tin, cung cấp bằng chứng trong cuộc đánh giá
3) Chuẩn bị 1 máy chủ để lưu giữ các bằng chứng phục vụ cuộc đánh giá. 1 số bằng chứng ví dụ như các quy định bảo mật, các kết quả pentest, 1 số change request ticket và các hồ sơ đính kèm .. Nên được upload lên. Vì sẽ có nhiều bằng chứng có thể từ đây mà cung cấp trong cuộc đánh giá. Tất nhiên sẽ có các hạng mục cần chọn mẫu đánh giá, sẽ chọn mẫu khác với bằng chứng đã chuẩn bị, nhưng việc chuẩn bị cũng là 1 lần tập dượt để quá trình đánh giá trôi chảy nhanh chóng.
4) Thực hiện đánh giá thử với QSA
5) Book lịch Đánh giá chính thức. Lưu ý 1 số QSA có quá trình QA khá nghiêm ngặt, đòi hỏi thời gian hết sức chính xác.



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

Xin cám ơn Quý Anh/ Chị đã tham dự hội thảo được tổ chức bởi BSI Việt Nam

Liên hệ hoặc quét mã QR để tìm hiểu thêm:

Viện tiêu chuẩn Anh - BSI Việt Nam

Trụ sở chính: Tầng 15, Tòa nhà AP, 518B Điện Biên Phủ, Phường 21, Quận Bình Thạnh, Thành phố Hồ Chính Minh

T: +84 (28) 3820 0066

F: +84 (28) 3820 0022

Info.Vietnam@bsigroup.com | www.bsigroup.com

Văn phòng Hà Nội: Tầng 12, Tòa nhà PV Oil, 148 Hoàng Quốc Việt, Phường Nghĩa Tân, Quận Cầu Giấy, Thủ Đô Hà Nội

T: +84 (24) 3762 1170

F: +84 (24) 3762 1171

Info.Hanoi@bsigroup.com | www.bsigroup.com

Văn phòng Đà Nẵng: Lô G, Tầng 8, Công viên phần mềm Đà Nẵng, 02 Quang Trung, Quận Hải Châu Thành phố Đà Nẵng

T: +84 (23) 6388 8468

F: +84 (23) 6388 8719

VanBac.Doan@bsigroup.com | www.bsigroup.com

bsi.