TCVN **TIÊU CHUẨN QUỐC GIA**

TCVN 11778-2:2017
ISO/IEC TR 15443-2:2012

CÔNG NGHỆ THÔNG TIN - CÁC KỸ THUẬT AN TOÀN - KHUNG CHO ĐẢM BẢO AN TOÀN CÔNG NGHỆ THÔNG TIN - PHẦN 2: PHÂN TÍCH

Information technology - Security techniques - Security assurance framework - Part 2: Analysis

HÀ NỘI - 2017

Mục lục

Lời nói đầu

TCVN 11778-2:2017 hoàn toàn tương đương với Tiêu chuẩn ISO/IEC 15443-2:2012 Information technology - Security techniques - Security assurance framework Part 2: Analysis.

TCVN 11778-2:2017 do Học viện Công nghệ Bưu chính Viễn thông biên soạn, Bộ Thông tin và Truyền thông đề nghị, Tổng cục Tiêu chuẩn Đo lường Chất lượng thẩm định, Bộ Khoa học và Công nghệ công bố.

TCVN 11778-2:2017

Lời giới thiệu

Tiêu chuẩn TCVN 11778-2:2017 sẽ được sử dụng cùng với tiêu chuẩn TCVN 11778-1:2017.

TCVN 11778-1:2017 giới thiệu và thảo luận các khái niệm đảm bảo, mô tả mô hình đáp ứng các yêu cầu đảm bảo an toàn cho giao phẩm thông qua các bằng chứng an toàn được thu thập qua các luận cứ đảm bảo an toàn trong tuyên bố đảm bảo an toàn, các luận cứ đảm bảo an toàn CNTT được xác nhận bởi việc áp dụng các phương pháp đánh giá sự phù hợp đảm bảo an toàn, nhãn hiệu hay biểu tượng được gán phù hợp.

TCVN 11778-1:2017 giới thiệu khái niệm về các phương pháp thu nhận tính bí mật trong các tuyên bố đảm bảo an toàn thực hiện cho giao phẩm. Điều này bao gồm các phương pháp dựa trên các phương pháp, đặc tả và tiêu chuẩn phù hợp với quốc gia hoặc quốc tế cũng như các phương pháp, đặc tả và tiêu chuẩn tồn tại trên thực tiễn nhưng chưa được công nhận mà có một đặc tính, một phương pháp được xác định và lặp lại có hệ thống để thu nhận đảm bảo an toàn. Điều này có thể được bổ sung bởi lưu đồ đánh giá sự phù hợp quản trị có trách nhiệm giám sát tuân thủ việc áp dụng tiêu chuẩn hoặc đặc tả, phương pháp kiểm thử và thường xuyên đảm nhận nhiệm vụ khác chẳng hạn như việc cấp các nhãn hiệu đảm bảo an toàn.

Tiêu chuẩn TCVN 11778-2:2017 được định nghĩa như là một khung hướng dẫn chuyên gia công nghệ thông tin trong việc lựa chọn và kết hợp các phương pháp đảm bảo thích hợp cho sản phẩm, hệ thống hay dịch vụ an toàn CNTT và môi trường hoạt động của chúng.

Người sử dụng tiêu chuẩn này bao gồm các trường hợp cụ thể sau đây:

Bên thu mua (một cá nhân hoặc tổ chức thu mua một hệ thống, sản phẩm phần mềm hoặc dịch vụ phần mềm từ một bên cung cấp);

Bên phát triển (một cá nhân hoặc tổ chức thực hiện các hoạt động phát triển bao gồm phân tích các yêu cầu, thiết kế, kiểm thử và có thể tích hợp trong tiến trình vòng đời phần mềm)

Bên bảo trì (một cá nhân hoặc tổ chức thực hiện các hoạt động bảo trì);

Bên cung cấp (một cá nhân hoặc tổ chức ký hợp đồng với nhà thu mua để cung cấp một hệ thống, sản phẩm phần mềm hoặc dịch vụ phần mềm tuân theo các điều khoản trong hợp đồng);

Người dùng (một cá nhân hoặc tổ chức sử dụng sản phẩm để thực hiện một chức năng riêng biệt);

Bên đánh giá, kiểm thử/ đánh giá (một cá nhân hoặc tổ chức thực hiện một đánh giá; ví dụ bên đánh giá có thể là phòng kiểm thử, phòng chất lượng của một tổ chức phát triển phần mềm, tổ chức quản trị hoặc một người dùng);

Mục tiêu của tiêu chuẩn này là mô tả tiêu chí được sử dụng trong phân tích để thu nhận tính bí mật trong một số mô hình đánh giá sự phù hợp đảm bảo an toàn CNTT (SACA), và liên quan đến tiêu chí đã được mô tả với mô hình đảm bảo an toàn trong phần 1. Trọng tâm ở đây là xác định tiêu chí, thường là chất lượng và có thể là định lượng, được sử dụng để thu nhận tính bí mật có trong các bản tuyên bố, các kết quả và nhãn hiệu đã thu được từ mô hình SACA liên quan.

Tiêu chuẩn này cung cấp khung cần thiết nhằm đặc tả tiêu chí được sử dụng để đánh giá chất lượng của mô hình đối tượng. Nhiều tiêu chí đưa ra trong khung này dựa trên phân tích chủ quan, với các

yếu tố đánh giá dựa vào cá nhân, tổ chức và tiêu chuẩn quốc gia, nền văn hóa và tín ngưỡng của những nơi đó.

Công nghệ thông tin - Các kỹ thuật an toàn - Khung cho đảm bảo an toàn công nghệ thông tin - Phần 2: Phân tích

Information technology - Security techniques - Security assurance framework Part 2: Analysis

1 Phạm vi áp dụng

Tiêu chuẩn này xây dựng dựa trên các khái niệm đã được trình bày trong tiêu chuẩn TCVN 11778-1:2017.

Tiêu chuẩn này đề cập về các thuộc tính của các phương pháp đánh giá sự phù hợp đảm bảo an toàn góp phần hướng tới việc tạo các tuyên bố đảm bảo và đưa ra bằng chứng đảm bảo để đạt được đầy đủ các yêu cầu đảm bảo cho giao phẩm.

Tiêu chuẩn này đề xuất tiêu chí để so sánh và phân tích các phương pháp SACA khác nhau. Các phương pháp được sử dụng làm ví dụ trong tiêu chuẩn này là đại diện cho các phương pháp được dùng phổ biến tại thời điểm soạn thảo. Các phương pháp mới có thể xuất hiện, sửa đổi hoặc thu hồi các phương pháp đã đề cập. Mục đích là tiêu chí có thể được sử dụng để mô tả và so sánh phương pháp SACA bất kỳ.

2 Tài liệu viện dẫn

Các tài liệu viện dẫn sau rất cần thiết cho việc áp dụng tiêu chuẩn này. Với những tài liệu viện ghi năm ban hành thì áp dụng phiên bản được nêu. Với những tài liệu không ghi rõ ngày tháng, áp dụng lần phiên bản mới nhất (bao gồm tất cả các sửa đổi).

TCVN 11778-1:2017 - Công nghệ thông tin - Các kỹ thuật an toàn - Khung cho đảm bảo an toàn công nghệ thông tin - Phần 1:Giới thiệu và khái niệm.

3 Thuật ngữ, định nghĩa và từ viết tắt

Tiêu chuẩn này sử dụng các thuật ngữ và định nghĩa trong TCVN 11778-1:2017 và các thuật ngữ sau:

CAP: Thành viên có thẩm quyền cấp chứng chỉ

CCP: Thành viên công nhận chứng chỉ

CCRA: Tổ chức thừa nhận lẫn nhau về tiêu chí chung

CCMC: Uỷ ban quản lý tiêu chí chung

PCI: Thẻ thanh toán

4 Khung phân tích đảm bảo an toàn công nghệ thông tin

Tiêu chuẩn này cung cấp các điều khoản mô tả tiêu chí sẽ được đánh giá chủ quan và có thể được sử dụng để tăng tính bí mật trong các yếu tố khác nhau của mô hình SACA. Tiêu chí phân tích các mô

hình, lưu đồ và hệ thống SACA được mô tả trong điều 6, tiêu chí liên quan đến đánh giá cơ quan SACA được đưa ra trong điều 7, tiêu chí liên quan đánh giá các phương pháp trong điều 8; tiêu chí đánh giá SDOs và các tiêu chuẩn được tìm thấy trong điều 9 và tiêu chí đánh giá các kết quả SACA được cung cấp tại điều 10.

Tiêu chí được liệt kê trong tiêu chuẩn này được mong đợi để sử dụng hỗ trợ việc thu nhận tính bí mật trong kết quả SACA. Phụ thuộc vào các mục tiêu của người sử dụng danh mục một số tiêu chí có thể là không phù hợp nhưng những tiêu chí khác có thể vẫn cần được định nghĩa.

Một số chuẩn CASCO hiện có nên hướng dẫn các bên liên quan về định nghĩa và hoạt động của các yếu tố khác nhau trong mô hình SACA bao gồm các lưu đồ, cơ quan và hệ thống SACA đã dùng. Mục tiêu là để đánh giá xem những tài liệu này có liên hệ với các tài liệu CASCO được thảo luận tại điều 9 trong phần 1 của bộ tiêu chuẩn này. Hơn nữa, để thu nhận tính bí mật trong kết quả SACA thì cần phải xem xét về chất lượng của kết quả.

Cấu trúc của các điều khoản sau đây bao gồm thảo luận theo chủ đề, và xem xét tiêu chí đã được xác định cùng với các chú thích và ví dụ thích hợp.

5 Tiêu chí phân tích mô hình SACA

Có nhiều ví dụ về các lưu đồ SACA gồm đầy đủ các loại tổ chức từ các phòng ban nội bộ trong một tổ chức phát triển hoặc tích hợp, các lưu đồ hoạt động thương mại, lưu đồ trợ giúp ngành công nghiệp, cũng như những hoạt động của các phòng ban và các cơ quan chính phủ.

5.1 Tính sẵn sàng sắp xếp của thỏa thuận và thừa nhận

5.1.1 Thảo luận

Thông thường, lưu đồ SACA có trách nhiệm tham gia vào các thoả thuận và xếp đặt thừa nhận phù hợp. Việc xem xét về sự thừa nhận các thoả thuận hoặc xếp đặt có thể là một tiêu chí quan trọng đối với các nhà sản xuất các giao phẩm cung cấp cho nhiều đối tượng sử dụng.

5.1.2 Tiêu chí

a) Các thoả thuận và xếp đặt thừa nhận chính thức hoặc không chính thức được đưa ra.

b) Giá trị hữu ích cho các bên liên quan SACA trong bất kỳ việc thừa nhận các thoả thuận và xếp đặt;

CHÚ THÍCH: Các bên liên quan có thể quan tâm nếu như thoả thuận hoặc xếp đặt đó được thực hiện ở cấp quốc tế, quốc gia, chính trị hay ngành công nghiệp, và nếu như vậy thoả thuận hay xếp đặt dễ dàng đạt được mục tiêu của các bên liên quan.

c) Thỏa thuận hay xếp đặt được thực hiện bao gồm việc xem xét sự phát triển, cấp phát và vận hành của các thỏa thuận để được thừa nhận và chấp nhận kết quả đã tạo bởi cơ quan SACA cam kết tương đương việc đánh giá sự phù hợp và các hoạt động có liên quan.

VÍ DỤ: TCVN 7780:2008

5.2 Sự xem xét về địa lý và chính trị

5.2.1 Thảo luận

Mô hình SACA có thể bao gồm các hoạt động ở cấp quốc tế, quốc gia, chính trị hay ngành công nghiệp. Người tiêu dùng được cung cấp sự đảm bảo và các bên liên quan khác có thể chỉ rõ các lưu đồ SACA với quyền hạn trong từng vùng riêng biệt. Điều này cần được xem xét với các bên lựa chọn mô hình SACA.

5.2.2 Tiêu chí

a) Mô hình SACA hoạt động trong các vùng địa lý-chính trị thích hợp;

b) Sự khác biệt văn hóa giữa các khu vực địa lý được xem xét bởi các bên liên quan;

c) Tồn tại các phiên bản về các chuẩn và đặc tả trong các vùng địa lý - chính trị hay chính sách khu vực khác nhau.

CHÚ THÍCH: Nếu các phiên bản được tạo ra khác nhau trong các vùng địa lý khác nhau thì việc đánh giá các kết quả SACA và giá trị của nhãn hiệu được gán trong mỗi vùng nên được xem xét để đảm bảo rằng tính bí mật tương xứng thu được trong mỗi trường hợp.

6. Tiêu chí phân tích lưu đồ SACA và hệ thống SACA

6.1 Độc lập

6.1.1 Thảo luận

Lưu đồ SACA là một cách tổ chức được tin cậy để xác định những tuyên bố SACA được đưa ra bởi những tổ chức khác.

Tính bí mật trong đảm bảo đã tuyên bố có thể đạt được nếu lưu đồ quy định một tiêu chuẩn hoặc đặc tả đã được thừa nhận cho SACA, cùng với một phương pháp đã chọn thích hợp, nhất là nếu các tiêu chuẩn và đặc tả được phát triển bởi bên thứ ba hoặc sử dụng một quy trình phát triển mở. Hơn nữa tính bí mật có thể được cung cấp cho bên thứ ba quan tâm nếu việc cung cấp các đảm bảo như vậy được xác nhận bởi một bên thứ ba độc lập tin cậy.

Nếu lưu đồ SACA là không độc lập với một số bên liên quan thì xung đột lợi ích có thể phát sinh, hoặc có thể được nhận ra bởi bên liên quan khác.

6.1.2 Tiêu chí

a) Mức độ độc lập của tổ chức lưu đồ từ các bên liên quan khác trong mô hình SACA;

VÍ DỤ: Trong một số trường hợp lưu đồ có một tầm quan trọng trong việc giảm rủi ro của chính nó thông qua sự uỷ quyền SACA. Ví dụ mức độ độc lập giữa cơ quan chính phủ khác nhau có thể cần được xem xét.

CHÚ THÍCH: Mong muốn một vài mối quan hệ tồn tại. Ví dụ nhiều lưu đồ SACA có các thành viên hoặc người tham gia là quản trị của lưu đồ. Tuy nhiên, những mong muốn này nên được điều tra và nắm bắt các mối quan hệ và đánh giá ảnh hưởng của chúng đến độ độc lập bởi việc tìm kiếm tính bí mật trong lưu đồ.

b) Hiệu quả của công tác quản trị lưu đồ SACA;

CHÚ THÍCH: Sử dụng tiêu chí này có thể bao gồm việc điều tra danh tiếng của lưu đồ SACA, một đánh giá có thể bao gồm thu thập sự liên quan từ các tiêu chí khác với kinh nghiệm vận hành của lưu đồ SACA.

c) Sự công nhận cho chính lưu đồ SACA bởi một tổ chức công nhận khác.

VÍ DỤ: Trong tổ chức thừa nhận lẫn nhau về tiêu chí chung (CCRA), Uỷ ban quản lý tiêu chí chung (CCMC) xác định quốc gia nào có thể gia nhập vào CCRA như thành viên công nhận chứng chỉ (CCP). CCMC cũng xác định quốc gia nào có thể thay đổi trạng thái của thành viên có thẩm quyền cấp chứng chỉ (CAP) xây dựng kế hoạch đề xuất xem xét từ CCES

CHÚ THÍCH: Trong một số trường hợp, tổ chức công nhận có thể tự thực hiện các lưu đồ SACA. Trong trường hợp khác bên thực hiện có thể được công nhận bởi tổ chức công nhận độc lập, đôi khi cả hai trường hợp trên đều đúng.

Trong một vài mô hình SACA một quá trình công nhận là không sẵn sàng hoặc là một lựa chọn. Vì vậy trên thực tế một lưu đồ không được công nhận bởi chính nó không có nghĩa là nó không phải là một tổ chức có uy tín. Điều đó nói lên rằng, nhiều lưu đồ được chọn để tìm kiếm sự công nhận, ngay cả khi nó không phải là bắt buộc, để có thể chứng minh khả năng xác nhận độc lập của chúng.

6.2 Khả năng của lưu đồ

6.2.1 Thảo luận

Lưu đồ SACA chịu trách nhiệm về chất lượng của các kết quả SACA, thường xuyên giám sát các tổ chức đánh giá sự phù hợp SACA như phòng thử nghiệm, ITSEF và tổ chức đánh giá. Một số tiêu chí đóng góp cho tính bí mật trong khả năng của lưu đồ SACA.

6.2.2 Tiêu chí

a) Sự phù hợp với các tiêu chuẩn CASCO liên quan đến lưu đồ SACA;

VÍ DỤ: ISO/IEC 17020 đưa ra các tiêu chí chung cho hoạt động của các cơ quan khác nhau thực hiện việc điều tra.

b) Kinh nghiệm kỹ thuật và khả năng của nhân lực thực thi lưu đồ với kiểu và công nghệ của giao phẩm;

CHÚ THÍCH: Các chủ đề đào tạo nhân lực được đề cập trong ISO/IEC 17020, tuy nhiên tiêu chí này được xem xét nếu chương trình cũng như toàn bộ có thể cung cấp khả năng trong từng kiểu giao phẩm.

VÍ DỤ: Trong mô hình tiêu chí chung, ở một số quốc gia lưu đồ đã phát triển chuyên biệt trong việc đánh giá các công nghệ thẻ thông minh, trong khi những nước khác tập trung vào hệ điều hành. Qua đó các lưu đồ sẽ cung cấp một đánh giá hoàn thiện hơn về công nghệ, mặc dù, thông qua quá trình kiểm định chất lượng lưu đồ, tất cả các lưu đồ tham gia sẽ đưa ra một khả năng tối thiểu trong mỗi kiểu công nghệ.

c) Kinh nghiệm của tổ chức chịu trách nhiệm trong thực hiện lưu đồ SACA;

CHÚ THÍCH: Các thành phần có thể đóng góp vào kinh nghiệm đánh giá bao gồm bên quản lý lưu đồ đã và đang thực thi bất kỳ lưu đồ nào khác, và khoảng thời gian mà lưu đồ này đã đi vào hoạt động.

d) Lưu đồ cung cấp giải thích và hướng dẫn liên quan đến các chính sách của lưu đồ, hệ thống SACA và phương pháp SACA đã áp dụng bởi lưu đồ này;

e) Lưu đồ có đầy đủ chính sách liên quan đến trách nhiệm pháp lý và phù hợp đảm bảo pháp lý;

CHÚ THÍCH: Lưu đồ có thể nhận lấy rủi ro thông qua việc cung cấp đảm bảo cho bên tiêu dùng đảm bảo. Trong một số trường hợp, lưu đồ phải chịu trách nhiệm trước pháp luật hoặc tổ chức mà lưu đồ là thành viên

6.3 Đánh giá sự phù hợp

6.3.1 Thảo luận

Lưu đồ SACA thông thường chịu trách nhiệm đảm bảo sự phù hợp giữa các cơ quan SACA làm việc dưới sự bảo trợ của lưu đồ, và do đó các đánh giá lẫn nhau được thực hiện bởi các cơ quan SACA khác nhau.

6.3.2 Tiêu chí

a) Việc cung cấp các chính sách lưu đồ về việc đánh giá sự phù hợp của các cơ quan SACA cung cấp kết quả SACA;

CHÚ THÍCH: Chính sách có thể bao gồm tiêu chí như sự phù hợp với các chuẩn CASCO để các cơ quan SACA thực hiện các hoạt động SACA dưới sự bảo trợ của lưu đồ.

b) Lưu đồ cung cấp công cụ cho các tổ chức SACA thực hiện các hoạt động đánh giá sự phù hợp;

CHÚ THÍCH: Bao gồm cả việc xem xét mọi công cụ được cung cấp nếu các công cụ đó đã được đánh giá về chất lượng, và nếu là bắt buộc thì với mọi công cụ được sử dụng bởi cơ quan SACA.

c) Cung cấp hoặc đặc tả bởi lưu đồ đào tạo nhân lực làm việc trong lưu đồ;

CHÚ THÍCH: Việc này rất quan trọng khi lưu đồ thực thi bao gồm xác nhận công việc của cơ quan SACA.

d) Việc cung cấp hoặc đặc tả bởi lưu đồ cho việc đào tạo nhân lực cơ quan SACA thực hiện đánh giá.

CHÚ THÍCH: Bên cạnh lĩnh vực đào tạo về năng lực cho nhân lực lưu đồ một số lưu đồ SACA cũng cung cấp một cơ sở đào tạo và thậm chí chứng nhận nhân lực cho bên đánh giá làm việc với các cơ quan SACA đã công nhận lưu đồ.

6.4 Hỗ trợ cho người sử dụng và bên cung cấp đảm bảo an toàn

6.4.1 Thảo luận

Trong một số trường hợp lưu đồ cung cấp hỗ trợ bổ sung cho người tham gia. Điều này có thể tạo ra các hình thức đào tạo, cung cấp mẫu, tài liệu hướng dẫn và các sự kiện.

6.4.2 Tiêu chí

a) Lưu đồ cung cấp các dịch vụ hỗ trợ cho người sử dụng lưu đồ:

b) Lưu đồ được tham gia bởi các bên liên quan khác nhau.

6.5 Cung cấp các giải thích về tiêu chuẩn và phương pháp

6.5.1 Thảo luận

Trong hầu hết các trường hợp, tiêu chuẩn hoặc đặc tả có yêu cầu giải thích hay đính chính để làm sáng tỏ những điều không rõ ràng chưa được lường trước. Điều này có thể là do phát triển công nghệ, thay đổi các yêu cầu hay các chính sách lưu đồ, trong bối cảnh mối đe doạ bùng nổ hay lý do khác.

Quan trọng là bất kỳ sự giải thích nào đều là sẵn sàng phục vụ các bên liên quan và áp dụng một cách thống nhất.

6.5.2 Tiêu chí

a) Lưu đồ cung cấp sự giải thích liên quan của các tiêu chuẩn, các đặc tả và các phương pháp;

b) Sự giải thích liên quan sẵn sàng cho tất cả các bên liên quan, được áp dụng thống nhất;

CHÚ THÍCH: Xem điều 5.2.

c) Sự giải thích được xem xét, cập nhật và duy trì thường xuyên.

CHÚ THÍCH: Điều này có thể bao gồm sự giải thích kết hợp với SDOs, các lưu đồ khác và người sử dụng các tiêu chuẩn, các đặc tả và các phương pháp

6.6 Các chính sách liên quan đến lưu đồ

6.6.1 Thảo luận

Ngoài bất kỳ chính sách đã quy định bởi hoặc được áp dụng cho tổ chức thu mua giao phẩm, một lược đồ SACA có thể thực thi các chính sách có thể áp dụng cho người sử dụng lưu đồ.

6.6.2 Tiêu chí

a) Các chính sách lưu đồ điều chỉnh mục như một ứng viên đánh giá;

b) Các chính sách lưu đồ có ảnh hưởng đến kết quả đánh giá sự phù hợp đảm bảo an toàn;

VÍ DỤ: Trong các lưu đồ tham gia CCRA, chính sách quốc gia đối với việc đánh giá kỹ thuật mã hóa thường được áp dụng.

c) Lưu đồ đã xác định các chính sách để xử lý bất kỳ lỗ hổng hoặc điểm yếu được tìm thấy trong quá trình đánh giá, hoặc còn tồn tại trong đối tượng đánh giá sau khi đánh giá hoàn thành.

6.7 Hệ thống SACA

6.7.1 Thảo luận

Một lưu đồ SACA có thể dùng một hay nhiều hệ thống SACA mặc dù như một điều lệ chung chỉ có một hệ thống được xác định. Hệ thống SACA có thể thích ứng với CASCO hoặc các chuẩn khác cung cấp độ tin cậy hơn trong việc xác định và hoạt động của hệ thống.

6.7.2 Tiêu chí

a) Hệ thống SACA được xác nhận phù hợp các tiêu chuẩn;

VÍ DỤ: ISO/PAS 17005 Đánh giá sự phù hợp - Sử dụng hệ thống quản lý - Các nguyên tắc và yêu cầu; TCVN ISO/IEC 27001 Công nghệ thông tin - Kỹ thuật an toàn - Hệ thống quản lý an toàn thông tin – Các yêu cầu; và TCVN ISO 9001 Hệ thống quản lý chất lượng - Các yêu cầu, đó là những ví dụ về tiêu chuẩn có thể được áp dụng.

b) Việc sửa đổi bất kỳ phương pháp SACA đã xác định bởi lưu đồ đã được công bố;

CHÚ THÍCH: Trong nhiều trường hợp một phương thức SACA mở được thông qua bởi một lưu đồ nhưng được sửa đổi thông qua áp dụng các chính sách hoặc các diễn giải. Việc sửa đổi có thể ảnh hưởng sự phù hợp của đánh giá khi được xem xét sử dụng cùng phương thức SACA bởi lưu đồ khác nhau.

c) Quản lý bất kỳ chi tiết bằng chứng SACA được xem xét bởi lưu đồ;

CHÚ THÍCH: Các thành phần có thể được xem xét đến việc quản lý bằng chứng bao gồm tính bí mật của bằng chứng chi tiết và giai đoạn duy trì.

d) Một hướng dẫn hệ thống được cung cấp đảm bảo rằng các quá trình liên quan có hiệu quả và có thể lặp lại.

6.8 Xem xét về mặt thương mại

6.8.1 Thảo luận

Tiêu chí thương mại thường là một yếu tố quan trọng đối với các bên liên quan. Đối với các bên cung cấp cung cấp giải pháp cho người dung cuối, các nguồn lực tiêu tốn trong việc cung cấp bảo đảm an toàn cũng là một mối quan tâm. Các khía cạnh thương mại này có thể ảnh hưởng đến thời gian để một sản phẩm ra thị trường hoặc ảnh hưởng đến tính kịp thời của việc cung cấp các chức năng bảo mật quan trọng để giải quyết giảm thiểu những điểm yếu và lỗ hổng.

CHÚ THÍCH: Xem điều 7.4

6.8.2 Tiêu chí

a) Khoảng thời gian thực hiện các hoạt động xác nhận kết quả SACA;

b) Khoảng thời gian thực hiện để sản xuất nhãn hiệu SACA;

c) Chi phí trực tiếp cho một cơ quan đảm bảo để thu được kết quả SACA;

d) Các chi phí trực tiếp liên tục để duy trì nhãn hiệu SACA.

e) Các phương thức SACA xác định việc cung cấp các điều kiện tiên quyết nhãn hiệu SACA từ cùng một lưu đồ SACA hoặc một lưu đồ SACA khác.

6.9 Kết quả SACA

6.9.1 Thảo luận

Phụ thuộc vào mô hình SACA đã triển khai, lưu đồ SACA có thể truy cập kết quả SACA và thường chịu trách nhiệm cho việc duy trì chúng.

6.9.2 Tiêu chí

a) Kết quả SACA được xử lý sao cho tính bí mật và tính toàn vẹn được bảo toàn.

CHÚ THÍCH: Kết quả chính như là các tài liệu mô tả ranh giới, các giả định, và các cấu hình cần phải được cung cấp một cách thích hợp tới các bên liên quan. Tính toàn vẹn của kết quả liên quan đến việc đảm bảo các tài liệu như vậy đã không được sửa đổi kể từ khi SACA được thực hiện, và đã được cập nhật và duy trì thích hợp với bất kỳ các hoạt động duy trì SACA là quan trọng.

VÍ DỤ: Duy trì và cung cấp tài liệu thích hợp mô tả ranh giới SACA giống như các tài liệu Mục tiêu an toàn, tài liệu Chính sách an toàn, báo cáo về việc tuân thủ, và báo cáo đánh giá.

b) Duy trì sự đảm bảo được xử lý một cách thích hợp.

CHÚ THÍCH: Một số hệ thống gọi cho một đánh giá lại kết quả định kỳ, hệ thống khác thì xem xét lại việc cập nhật các thay đổi bảo mật trong sản phẩm.

6.10 Nhãn hiệu và biểu tượng SACA

6.10.1 Thảo luận

Nhãn hiệu và biểu tượng liên quan đến đảm bảo an toàn cần được quản lý và sử dụng một cách thích hợp. Trong hầu hết một số mô hình SACA đó là chính sách cái mà các nhãn hiệu được gán công khai, nhưng trong một số trường hợp các nhãn hiệu có thể được giữ kín.

Nếu điều này thể hiện rằng một hệ thống SACA là phù hợp với các tiêu chuẩn CASCO có liên quan, ví dụ tiêu chuẩn ISO Guide 27 hướng dẫn cho tổ chức chứng nhận thực hiện hoạt động hiệu chỉnh trong trường hợp lạm dụng Nhãn phù hợp, sau đó tính bí mật có thể được thể hiện là thỏa mãn nhiều tiêu chí được ấn định bởi các tiêu chuẩn này.

6.10.2 Tiêu chí

a) Danh sách nhãn hiệu được cấp bởi lưu đồ SACA được công bố hoặc sẵn sàng cho những người có nhu cầu được biết;

VÍ DỤ: Danh sách sản phẩm được phê chuẩn (APL), giấy chứng nhận, nhãn hiệu.

b) Trách nhiệm lưu đồ hoạt động truy tìm việc dùng sai nhãn hiệu và biểu tượng SACA;

c) Các nhãn hiệu được gán có thể được cập nhật một cách thích hợp cho những thay đổi kỹ thuật;

CHÚ THÍCH: Một sửa đổi nhỏ của một sản phẩm công nghệ thông tin không ảnh hưởng đến kết quả đánh giá.

d) Các nhãn hiệu được gán có thể được cập nhật cho mục đích quản trị;

VÍ DỤ: Nếu thay đổi tên và địa chỉ của tổ chức thì nhãn hiệu có thể cần phải được cập nhật với thông tin hiện tại

7 Tiêu chí phân tích các cơ quan SACA

Tổ chức đánh giá sự phù hợp được đặt tên khác nhau tương ứng trong từng lĩnh vực đánh giá sự phù hợp đảm bảo an toàn. Ví dụ, trong một lưu đồ tiêu chí chung chúng có thể được đặt tên là "phòng thử nghiệm" hoặc "cơ sở đánh giá an toàn công nghệ thông tin" (ITSEF) hoặc các phòng thử nghiệm kiểm tra tiêu chí chung (CCTL); Trong TCVN ISO/IEC 27001 chúng có thể được đặt tên là "Cơ quan chứng nhận" hoặc "Bên đăng kiểm", đối với ngành công nghiệp thẻ thanh toán chúng được đặt tên là "Các công ty đánh giá an toàn hợp chuẩn"

7.1 Độc lập

7.1.1 Thảo luận

Một cơ quan SACA đại diện cho một tổ chức cung cấp các hoạt động SACA trên các giao phẩm cần để cung cấp việc đánh giá sự phù hợp đảm bảo an toàn.

7.1.2 Tiêu chí

a) Các loại cơ quan đánh giá;

CHÚ THÍCH: Tức là kiểu đánh giá mà cơ quan SACA vận hành là A, B hay C? Như đã đề cập trong Phần 1 của tiêu chuẩn này, tồn tại một số vấn đề suy xét có liên quan đến tính độc lập của cơ quan SACA dựa trên lợi ích của họ trong giao phẩm, đánh giá bên thứ nhất, bên thứ hai và bên thứ ba đưa ra các suy xét khác nhau về tính độc lập.

b) Mức độ độc lập của cơ quan SACA từ các bên liên quan khác trong mô hình SACA;

VÍ DỤ: Tổ chức công nhận, lưu đồ SACA và bên thu mua.

CHÚ THÍCH Tồn tại một vài mối quan hệ. Ví dụ nhiều lưu đồ SACA có các thành viên hoặc người tham gia có thể liên quan vào việc quản lý lưu đồ, hoặc liên quan phát triển kỹ thuật mô hình SACA. Tuy nhiên, mục này sẽ được điều tra và bất kỳ hoạt động nắm bắt và đánh giá về cách chúng ảnh hưởng đến tính độc lập của cơ quan SACA.

c) Hiệu quả của công tác quản trị cơ quan SACA;

CHÚ THÍCH: Sử dụng các tiêu chí này có thể bao gồm việc điều tra danh tiếng của cơ quan SACA; việc đánh giá có thể bao gồm thu thập tham chiếu từ những cái khác với kinh nghiệm hoạt động của cơ quan SACA.

d) Các chính sách xử lý những xung đột lợi ích tiềm ẩn.

CHÚ THÍCH: Xung đột lợi ích tiềm ẩn có thể xuất hiện ở cấp độ tổ chức. Nhiều lưu đồ SACA cung cấp chính sách trên một cơ quan SACA thực hiện các hoạt động tư vấn cũng như các hoạt động đánh giá độc lập. Ngoài ra các chính sách cơ quan SACA liên quan đến các xung đột lợi ích ảnh hưởng đến cả nhân bên định giá nên được phát triển. Những xung đột lợi ích tiềm ẩn này có thể xuất phát từ việc đánh giá các giao phẩm tương tự; nếu một người đánh giá có mối quan hệ với bên tài trợ của việc đánh giá hoặc bên sản xuất của giao phẩm; và nếu tổ chức đánh giá có lợi ích trong việc cung cấp các dịch vụ và các sản phẩm khác cũng như dịch vụ mà họ đánh giá.

7.2 Công nhận

7.2.1 Thảo luận

Trong nhiều mô hình, việc công nhận của các cơ quan SACA là bắt buộc. Đối với những mô hình khác việc công nhận không phải là một nghĩa vụ và thực tế là một cơ quan SACA không được công nhận bởi chính nó, không có nghĩa là nó không phải là một tổ chức có uy tín.

Điều đó nói lên rằng, nhiều cơ quan SACA lựa chọn để tìm kiếm việc công nhận, ngay cả khi nó không phải là bắt buộc, để có thể chứng minh xác nhận độc lập về năng lực của họ.

7.2.2 Tiêu chí

a) Việc công nhận bởi cơ quan SACA thông qua đáp ứng các yêu cầu của lưu đồ có liên quan;

CHÚ THÍCH: Các yêu cầu thường bao gồm việc tuân thủ các tiêu chuẩn như ISO/IEC 17025, ISO/IEC 17021, TCVN ISO 9001; hoàn thành các yêu cầu đào tạo bắt buộc; chứng minh năng lực.

b) Tình trạng công nhận: bắt buộc, tự nguyện và bổ sung

CHÚ THÍCH: Việc công nhận được sử dụng ở đâu có thể được điều tra nếu một cơ quan SACA đã duy trì việc công nhận có hiệu quả hoặc đã bị xử phạt về việc không phù hợp với các yêu cầu công nhận. Một số tổ chức công nhận cung cấp danh sách công khai của các cơ quan SACA với trạng thái đã công nhận.

7.3 Năng lực cơ quan SACA

7.3.1 Thảo luận

Điều quan trọng là phải xem xét năng lực của cơ quan SACA thực hiện công tác đánh giá. Năng lực của tổ chức cũng như của cá nhân cơ quan SACA được giao đánh giá đều có liên quan vì cả hai đều là những yếu tố góp phần cho việc đánh giá thành công.

7.3.2 Tiêu chí

a) Năng lực của cơ quan SACA;

CHÚ THÍCH: Một yếu tố góp phần là quá trình công nhận đã thảo luận ở trên. Ngoài ra một tổ chức có thể tạo các nỗ lực để nâng cao năng lực.

Ví DỤ Các ví dụ bao gồm chứng nhận tự nguyện giống như sự phù hợp với các tiêu chuẩn hệ thống quản lý như ISO 9001 hoặc ISO/IEC 27001; công bố các báo cáo, nghiên cứu, thuyết trình công nghiệp và tham gia vào diễn đàn công nghiệp, và phát triển các tiêu chuẩn.

a) Năng lực của nhân viên đánh giá. Có sử dụng kinh nghiệm của họ trong các phương pháp đảm bảo an toàn không?

c) Năng lực của nhân viên đánh giá. Có đánh giá kinh nghiệm của họ trong mục đích đánh giá về sản phẩm và công nghệ không?

b) Có xác nhận độc lập về năng lực của cá nhân đánh giá không?

CHÚ THÍCH: Các cơ quan SACA được công nhận nhiều nhất được yêu cầu phải chứng tỏ năng lực đánh giá của nhân viên. Chặt chẽ về đào tạo như vậy và liệu một xác nhận độc lập về năng lực của nhân viên như vậy, ví dụ thông qua một chứng nhận chuyên gia được công nhận, nên được xem xét. Có nghĩa là làm như thế nào một cơ quan SACA đánh giá hiệu quả về đào tạo cũng là một yếu tố được xem xét.

7.4 Xem xét về mặt thương mại

7.4.1 Thảo luận

Tiêu chí thương mại thường là một yếu tố quan trọng trong thế giới thực. Đối với các bên bán các sản phẩm COTS, các bên phát triển và bên tích hợp các nguồn lực chi tiêu trong việc cung cấp đảm bảo an toàn là một xem xét. Các tiêu chí này có thể ảnh hưởng đến thời gian thâm nhập thị trường của một sản phẩm hoặc ảnh hưởng tính kịp thời của việc cung cấp các chức năng bảo mật quan trọng để giải quyết vấn đề giảm thiểu những điểm yếu và lỗ hổng. Cân nhắc thương mại có thể được phân loại mặc dù chúng được chịu bởi các nhà tài trợ, hoặc như là một chi phí trực tiếp từ cơ quan SACA.

CHÚ THÍCH: Xem điều 6.8

7.4.2 Tiêu chí

a) Sự sẵn sàng tài nguyên;

CHÚ THÍCH: Theo các bên định giá, nguồn tài nguyên có thể bao gồm thiết bị, tiền bạc và nhân viên hỗ trợ, đó là những thứ cần thiết để hỗ trợ quá trình đánh giá. Cái này có thể bao gồm một quản lý dự án, tư vấn hỗ trợ, bên cung cấp danh sách chuyên gia, các nhà chuyên môn.

b) Chi phí đánh giá bổ sung

CHÚ THÍCH: Nếu bất kỳ lỗ hổng, sự tuân theo hoặc kiến nghị được xác định trong đánh giá thì những điều này có thể xử lý được bởi bên phát triển hoặc được thảo luận trong lưu đồ.

c) Độ phức tạp của đối tượng;

CHÚ THÍCH: Nếu đối tượng đánh giá là phức tạp bất thường, liên quan đến công nghệ mới hoặc bất thường, hoặc rất khó để áp dụng phương thức thì các tài nguyên cần thiết bao gồm cả thời gian và chi phí có thể bị ảnh hưởng.

d) Chi phí cơ quan SACA;

CHÚ THÍCH: Các chi tiêu và chi phí cơ quan SACA có thể được trả bởi bên tài trợ dự án, Đối với nhiều mô hình SACA cái này được trả bởi bên phát triển, nhưng cũng có thể được trả bởi các bên liên quan khác.

e) Thời gian cần thiết để cung cấp đảm bảo;

CHÚ THÍCH: Đối với đánh giá mà thời gian thực hiện để đánh giá là quan trọng thì chiều dài của quá trình cần được xem xét, các yếu tố của biện pháp này bao gồm thời gian thực hiện cho quá trình lưu đồ, các hoạt động đánh giá và khắc phục.

f) Cơ quan SACA có thể giả định một số trách nhiệm về các kết quả đánh giá, Điều này có thể dẫn đến các hoạt động giảm thiểu rủi ro này bao gồm chi phí bảo hiểm hoặc việc bổ sung các ngôn ngữ hợp đồng;

CHÚ THÍCH: Khía cạnh này thay đổi trong mô hình đang được xem xét.

g) Tính bí mật và yêu cầu bảo vệ tài sản;

CHÚ THÍCH: Nếu đánh giá bao gồm phân tích các thông tin bí mật như quy trình sản xuất, tài liệu thiết kế và mã nguồn thì phương thức bảo vệ thông tin này của cơ quan SACA nên được đánh giá. Phụ thuộc vào các yêu cầu mô hình SACA hoặc áp dụng luật cơ quan SACA có thể được yêu cầu giữ lại các tài sản này ngay cả sau khi đánh giá hoàn thành.

h) Xem xét về địa lý

CHÚ THÍCH Đối với một số đánh giá tiêu chí địa lý là một vấn đề. Ví dụ việc xem xét có thể liên quan tới chi phí đi lại cho đánh giá như gần địa điểm phát triển, vị trí của cơ quan SACA, hoặc giới hạn địa lý bởi lưu đồ SACA. Việc xem xét như vậy cũng mở rộng xem xét các yêu cầu của luật kiểm soát xuất khẩu.

8 Tiêu chí để phân tích các phương pháp SACA

8.1 Tiêu chí chung cho các phương pháp SACA

8.1.1 Thảo luận

Các phương pháp SACA khác nhau có thể được định nghĩa, hướng tới mục tiêu đảm bảo khác nhau, các loại công nghệ khác nhau và/hoặc mức độ đảm bảo khác nhau. Tất cả các phương pháp đó cần phải có những điều chung sau đây:

8.1.2 Tiêu chí

a) Phương pháp xác định rõ các mục tiêu đảm bảo;

b) Phương pháp xác định rõ đối tượng mà chúng sẽ được áp dụng;

c) Phương pháp xác định rõ các đầu vào cần thiết để thực hiện việc đánh giá;

d) Các phương pháp, bao gồm sự giải thích và các bước hoạt động đánh giá được thực hiện như một phần của đánh giá, được xác định rõ ràng;

e) Phương pháp định danh rõ ràng kết quả đánh giá và cách thức mà các kết quả này có thể và nên được sử dụng bởi người sử dụng thuộc đối tượng đánh giá;

VÍ DỤ 1: Bên tích hợp một thành phần đánh giá có thể sử dụng kết quả SACA như là đầu vào để đánh giá đảm bảo các sản phẩm hoặc các hệ thống, sử dụng cách tổng hợp kết quả SACA.

VÍ DỤ 2: Bên cung cấp sản phẩm bao gồm thành phần đánh giá nên xác định rõ ràng như là một phần của sản phẩm các kết quả áp dụng.

f) Phương pháp xác định rõ ràng các giới hạn của phương pháp đánh giá, trong đó nêu những gì không thể được đánh giá bằng cách sử dụng phương pháp cũng như những hạn chế về việc sử dụng các kết quả đánh giá.

g) Phương pháp xác định rõ ràng nếu kết quả hoặc nhãn hiệu thu được từ sử dụng các phương pháp khác có thể được tái sử dụng.

8.2 Tính bí mật trong phương pháp đảm bảo

8.2.1 Thảo luận

Các bên liên quan phải giữ bí mật về phương pháp SACA được sử dụng và điều đó lại cho phép các bên liên quan có được tính bí mật trong kết quả SACA. Nếu kết quả SACA không thể hiểu được thuộc tính bởi cơ quan đảm bảo, ví dụ các biên không được định nghĩa rõ ràng hoặc được định nghĩa theo cách thức không hỗ trợ các mục tiêu an toàn.

Một yếu tố khác là sự hiểu biết và nhận thức về phương pháp SACA của các bên liên quan. Thiếu kiến thức, quan niệm sai lầm về các yêu cầu của phương pháp, hoặc các mô hình đảm bảo có thể ảnh hưởng đến tính bí mật mà các bên liên quan có được trong kết quả.

VÍ DỤ Báo cáo kỹ thuật Đại học Cambridge Số 711, "Suy đoán bên trong hộp: lỗi mức hệ thống về chống giả mạo", phần 5.2 minh họa một số xem xét của chủ đề này.

8.2.2 Tiêu chí

a) Phương pháp đảm bảo rằng các ranh giới bảo mật được xác định rõ ràng và có sẵn cho các cơ quan đảm bảo;

b) Phương pháp đảm bảo rằng bất kỳ thành phần đã loại trừ sẽ được mô tả hoặc liệt kê rõ ràng;

c) Phương pháp đảm bảo rằng bất kỳ giả định hoặc các yêu cầu về môi trường được mô tả hoặc liệt kê rõ ràng;

d) Phương pháp bao gồm việc truyền đạt mô hình nguy cơ đã sử dụng trong đánh giá SACA;

e) Tài liệu yêu cầu hỗ trợ đánh giá được sắp xếp thích hợp;

CHÚ THÍCH: Có quá nhiều tài liệu chi tiết nhằm trợ giúp tại cơ quan đảm bảo có thể có mục đích che giấu những thông tin quan trọng cần thiết để mô tả các vấn đề an toàn, các giả định và các nguy cơ.

f) Các rủi ro và hạn chế của phương pháp SACA được đánh dấu tới các cơ quan đảm bảo và các bên liên quan khác;

VÍ DỤ: Một phương pháp SACA bao gồm đánh giá điểm yếu mang rủi ro đó là những điểm yếu nghiêm trọng bị bỏ qua trong phạm vi hoạt động đánh giá.

8.3 Thừa nhận độc lập

8.3.1 Thảo luận

Loại A, hoặc đánh giá bên thứ nhất, là đáng tin cậy nhất bởi vì tổ chức tự thực hiện đánh giá. Tuy nhiên kết quả SACA có thể bỏ sót các mục mà tổ chức cảm thấy không quan trọng. Các kết quả SACA thường không có độ tin cậy giống nhau với các tổ chức khác nhau.

Loại B, hoặc đánh giá bên thứ hai, có thể giúp các bên liên quan được giao xây dựng độ tin cậy trong các kết quả SACA kể từ khi họ có thể thực hiện đánh giá tập trung vào nhu cầu của họ. Tuy nhiên các kết quả SACA có thể không có độ tin cậy giống nhau với các tổ chức khác nhau.

[2] Một trích dẫn đầy đủ cho thông tin này được đưa ra trong thư mục trong phần 1 của Bộ tiêu chuẩn này.

Loại C, hoặc đánh giá bên thứ ba cung cấp tính bí mật độc lập trong các kết quả SACA và đem lại sự tin tưởng từ phạm vi các bên liên quan rộng hơn.

Trong khi lựa chọn các loại đánh giá có sẵn, có hay không chương trình tạo nên sự khác biệt rõ ràng trong việc đảm bảo mà có thể được cung cấp bởi từng loại?

8.3.2 Tiêu chí

a) Sự xem xét đó là chương trình dựa trên đánh giá bên thứ nhất, bên thứ hai hoặc bên thứ ba.

b) Lựa chọn bất kỳ loại đánh giá đã có;

c) Các phương pháp SACA đã áp dụng là giống nhau đối với từng loại đánh giá;

d) Đối với các loại đánh giá khác nhau sử dụng cùng một phương pháp nếu các yêu cầu năng lực và đào tạo đối với bên đánh giá trong từng loại là như nhau;

e) Bên định giá khác có thể làm theo phương pháp và tạo ra các kết quả tương tự một cách độc lập.

8.4 Các chính sách tin cậy

8.4.1 Thảo luận

Bên tiêu thụ có thể thiết lập các chính sách tin cậy về phương pháp và kết quả SACA. Điều này phản ánh tính bí mật rằng mô hình bao gồm các cảnh báo, phương pháp và giám sát có khả năng tạo lập kết quả và Nhãn đã được bí mật từ bên tiêu thụ.

8.4.2 Tiêu chí

a) Chính sách bí mật được thiết lập liên quan đến mô hình SACA hoặc bất kỳ thành phần nào của nó;

VÍ DỤ: Trong tiêu chí chung việc tăng cường bảo vệ hồ sơ mà không đáp ứng được nhu cầu của cơ quan đảm bảo dẫn đến sự thiếu độ bí mật trong việc sử dụng.

b) Chính sách bí mật dựa trên kiến thức chuyên sâu và hiểu biết về mô hình SACA.

CHÚ THÍCH Một số mô hình rất phức tạp và việc thiết lập chính sách bí mật có thể được dựa trên sự hiểu biết không đầy đủ các tính năng của mô hình.

8.5 Tính hoàn thiện của phương pháp đảm bảo

8.5.1 Thảo luận

Như bất kỳ quá trình được định nghĩa hoạt động theo một hệ thống cho phép cải tiến để tạo nên một phương pháp SACA sẽ nâng cao thông qua ứng dụng của bất kỳ bài học kinh nghiệm trong quá trình ứng dụng được lặp lại, để đáp ứng phát triển công nghệ, và thông qua phát triển các công cụ và kỹ thuật trong ngành công nghiệp SACA.

8.5.2 Tiêu chí

a) Khoảng thời gian phương pháp này được thiết lập;

CHÚ THÍCH: Phương pháp đã được thiết lập và thử nghiệm trong một thời gian có thể cung cấp tính bí mật hơn trong kết quả SACA liên quan.

b) Quy trình cải tiến và phát triển phương pháp.

CHÚ THÍCH: Giới thiệu công nghệ mới, sự tăng trưởng các nguy cơ an toàn và sự cải tiến trong các kỹ thuật đánh giá có nghĩa rằng các cập nhật phương pháp là cần thiết

c) Một cơ chế phản hồi cho phép bên phát triển phương pháp thu được kiến thức từ bên thực hành hiện có.

9 Tiêu chí phân tích tài liệu tiêu chuẩn, tài liệu đặc tả và tài liệu SACA

9.1 Tổ chức phát triển các tiêu chuẩn

9.1.1 Thảo luận

Một đánh giá về nguồn gốc của các tiêu chuẩn, đặc tả hoặc phương pháp đánh giá được sử dụng làm cơ sở để kiểm tra sự phù hợp hoặc đánh giá nên được thực hiện. Đánh giá bao gồm việc đánh giá các thuộc tính của tổ chức phát triển các tiêu chuẩn tạo ra các tài liệu cơ sở cho việc đánh giá.

9.1.2 Tiêu chí

a) Tính trung thực của SDO;

CHÚ THÍCH: Việc này bao gồm việc đánh giá về việc cai quản của SDO, cách thức xử lý về quyền sở hữu trí tuệ

c) Tính độc lập của SDO;

CHÚ THÍCH: Sự xem xét những lợi ích mà SDO đem lại thành công thương mại của tiêu chuẩn, hoặc bất kỳ lưu đồ/chương trình nào có liên quan? Cũng nên xem xét các đặc tính thành viên của SDO.

d) Chất lượng tiêu chuẩn làm nên bởi tổ chức;

CHÚ THÍCH: Cái này bao gồm đánh giá hệ thống SDO để xây dựng các tiêu chuẩn và đặc tả bao gồm các thủ tục nghiệm thu và các chính sách xây dựng đồng thuận.

e) Tầm quan trọng của tổ chức với khu vực đề xuất sẽ sử dụng giao phẩm;

CHÚ THÍCH: Điều này có thể bao gồm cách thức đánh giá của các chuyên gia được tuyển dụng góp phần vào sự phát triển các tiêu chuẩn và đặc tả.

e) Các nguồn lực cần thiết để phát triển các tiêu chuẩn.

CHÚ THÍCH: Các nguồn lực cần thiết có thể bao gồm chi phí thành viên SDO; tham dự cuộc họp phát triển và chi phí liên quan đến việc cung cấp các chuyên gia thích hợp.

9.2 Tiêu chuẩn hoặc quy định

9.2.1 Thảo luận

Một đánh giá về nguồn gốc của tiêu chuẩn, đặc tả hoặc tài liệu khác được sử dụng bao gồm việc xem xét ít nhất các yếu tố sau:

9.2.2 Tiêu chí

a) Tính trung thực của tài liệu, tiêu chuẩn hoặc đặc tả;

b) Quá trình phát triển SDO được xác định rõ;

VÍ DỤ: ISO/IEC 17007, Đánh giá sự phù hợp - Hướng dẫn soạn thảo văn bản quy phạm thích hợp để sử dụng cho việc đánh giá sự phù hợp, cung cấp hướng dẫn cho SDOs trong phát triển các tài liệu liên quan đến SACA.

c) Sự liên quan trong ngành công nghiệp trong đó tài liệu được áp dụng;

d) Sử dụng trong ngành công nghiệp đã đề xuất bởi những tổ chức khác, và nó là sự nhận biết;

e) Sự sẵn sàng và chi phí giấy phép để sử dụng các tài liệu có liên quan;

f) Các kỹ thuật đảm bảo an toàn được dùng trong tiêu chuẩn hay đặc tả và việc sử dụng chúng trong các phương pháp đánh giá liên hợp.

10 Tiêu chí phân tích các kết quả SACA

Điều khoản này mô tả tiêu chí đánh giá các khía cạnh về các kết quả của một phương pháp SACA. Kết quả SACA đã tạo sẵn cho cơ quan đảm bảo có thể đủ để cho cơ quan đảm bảo và các bên liên quan khác để nắm bắt những tuyên bố đảm bảo an toàn, ranh giới của việc đánh giá, các yếu tố liên quan đến các thành phần của việc đảm bảo an toàn đã tuyên bố.

10.1 Tài liệu đã xây dựng

10.1.1 Thảo luận

Có nhiều kết quả phương pháp SACA khác nhau trong khi tạo bằng chứng hỗ trợ, thông thường chúng ở dạng tài liệu.

10.1.2 Tiêu chí

a) Các kết quả được tạo sẵn cho cơ quan đảm bảo đưa ra thông tin đầy đủ để xây dựng một trường hợp đảm bảo lớn hơn bao gồm cả các kết quả này và các kết quả khác;

b) Bất kỳ giả định của việc đánh giá là được xác định rõ ràng;

CHÚ THÍCH: Điều này có thể bao gồm việc xem xét hoạt động ví dụ như "NO EVIL ADMIN", sự quan tâm về môi trường, và mô hình nguy cơ sử dụng trong đánh giá.

c) Kết quả SACA chứa bất kỳ thông tin độc quyền;

CHÚ THÍCH: Điều này có nghĩa rằng các kết quả chỉ có thể thu được theo các hạn chế tính bí mật. Ngoài ra bất kỳ kết quả bảo mật và bằng chứng hỗ trợ có thể cần được chia sẻ bởi các đơn vị tham gia khác?

VÍ DỤ: Tổ chức công nhận, lưu đồ SACA khác sử dụng các thỏa thuận công nhận.

CHÚ THÍCH: Điều này có nghĩa rằng các kết quả chỉ có thể thu được theo các hạn chế tính bí mật.

d) Kỹ năng đặc biệt hoặc kiến thức cần thiết để giải thích các kết quả;

CHÚ THÍCH: Nếu kết quả cần được đọc và hiểu bởi cơ quan đảm bảo thì chúng nên được viết với năng lực kỹ thuật mong muốn của cơ quan đó.

e) Tính sẵn sàng của các kết quả chi tiết hơn nữa;

CHÚ THÍCH: Trong một số trường hợp kết quả chi tiết hơn nữa có thể là sẵn sàng để hỗ trợ các kết quả được công bố.

f) Một quy trình thông báo các bản cập nhật về kết quả đã được công bố

VÍ DỤ: Trong trường hợp các kết quả được tìm thấy từ một ứng dụng không tuân theo phương pháp, các lỗi trong đánh giá đã được tìm thấy hoặc thông tin mới có liên quan về việc đánh giá cần phải được cung cấp cho cơ quan đảm bảo.

10.2 Định danh các thành phần của giao phẩm

10.2.1 Thảo luận

Như đã đề cập trong phần 1 của tiêu chuẩn này, sự thích hợp và tính khả dụng của các tiêu chuẩn, đặc tả và phương pháp đối với các giao phẩm được đánh giá (bao gồm bất kỳ thành phần đã tích hợp nào) phải được lập tài liệu.

Kiến trúc của giao phẩm, bao gồm hệ thống hoàn chỉnh (không chỉ là mục tiêu của đánh giá) cần phải được truyền đạt trong các kết quả SACA. Điều này cho phép cơ quan đảm bảo để xem xét thành phần, và giải thích kết quả cho các vấn đề an toàn cụ thể.

Các thành phần này có thể bao gồm:

- Các thành phần phần cứng,
- Các thành phần phần sụn,
- Các thành phần phần mềm,
- Các cơ sở dữ liệu,
- Các dịch vụ trực tuyến,
- Các thiết bị mạng,
- Các hệ thống,

- Các dịch vụ,
- Các hoạt động,
- Các tổ chức,
- Nhân lực

10.2.2 Tiêu chí

a) Các kết quả tài liệu hoá các chức năng đã đánh giá và bao gồm thảo luận về một hệ thống lớn hơn được sử dụng khi thích hợp.

10.3 Phạm vi và ranh giới của mục tiêu đánh giá

10.3.1 Thảo luận

Bắt buộc phải hiểu ranh giới của việc đánh giá đã đề xuất, và cách chúng liên quan đến bản phân bổ hoàn chỉnh, bao gồm.

10.3.2 Tiêu chí

a) Các thành phần được bao gồm trong đánh giá đã được mô tả;

b) Các ngoại lệ trong ranh giới đánh giá đã mô tả;

c) Các ranh giới được xác định cho việc đánh giá là thích hợp để cung cấp đảm bảo đã tuyên bố;

VÍ DỤ: Sau đây là ví dụ về các tài liệu SACA liên quan mô tả ranh giới của các hoạt động SACA và tài liệu tuyên bố đảm bảo chi tiết sau:

- Hồ sơ bảo vệ (từ TCVN 8709)
- Mục tiêu an toàn (từ TCVN 8709)
- Tài liệu chính sách an toàn (từ ISO/IEC 19790)
- Hiện trạng phạm vi (từ TCVN ISO/IEC 27001)
- Chương trình giảng dạy (cho đảm bảo nhân lực)

10.4 Chức năng của giao phẩm đã đánh giá

10.4.1 Thảo luận

Một số phương pháp SACA hạn chế chỉ đánh giá chức năng an toàn. Về bản chất, sự phù hợp dựa trên phương pháp hạn chế việc đánh giá trên các yêu cầu của đặc tả. Các phương pháp khác có thể cung cấp đảm bảo đối với chức năng hoàn chỉnh của giao phẩm thông qua việc sử dụng các kỹ thuật phát hiện lỗ hổng.

10.4.2 Tiêu chí

a) Hạn chế về chức năng được xem xét bởi phương pháp SACA;

CHÚ THÍCH: Bao gồm tất cả các chức năng hay chức năng được chọn lựa?

VÍ DỤ: TCVN 8709 thường bị hạn chế để đánh giá chức năng bảo mật, các tính năng không xác định có liên quan đến việc cung cấp đảm bảo an toàn có thể không phải là vấn đề để phân tích lỗ hổng ảnh hưởng đến các thành phần bên ngoài mục tiêu đánh giá.

VÍ DỤ: ISO/IEC 24759 bị hạn chế để thử nghiệm các tính năng bảo mật được xác định trong ISO/IEC 19790 Đặc tả, độ tin cậy trong các kết quả do đó bị hạn chế với những tính năng đó của mô-đun mã hóa được định nghĩa trong đặc tả.

10.5 Tiêu chí chuỗi cung ứng

10.5.1 Thảo luận

Nhiều cơ quan đảm bảo xây dựng một trường hợp đảm bảo cho hệ thống hoàn chỉnh cần phải xem xét các mối đe dọa và các lỗ hổng có thể đã được giới thiệu thông qua các chuỗi cung ứng của giao phẩm.

10.5.2 Tiêu chí

a) Phương pháp này bao gồm bất kỳ đánh giá đảm bảo an toàn đã có trong toàn bộ chuỗi cung ứng.

CHÚ THÍCH: Phương pháp bao gồm tiêu chí cho SACA liên quan đến:

- Vận chuyển giao phẩm an toàn, tức là cách thức giao phẩm được phân phối.
- Việc đối phó với sự phân mảnh hay lỗi đã phát sinh trong các giai đoạn vòng đời khác nhau;
- Bảo trì;
- Kết thúc chuỗi.

10.6 Phân tích các vấn đề an toàn

10.6.1 Thảo luận

Việc cung cấp các SACA dựa trên một định nghĩa rõ ràng về các vấn đề an toàn và các thành phần của SACA phụ thuộc vào định nghĩa rõ ràng về kiến trúc an toàn của giao phẩm. Quan trọng là đảm bảo các mục này được truyền tải rõ ràng tới cơ quan đảm bảo. Chứng minh rằng vấn đề an toàn đã nêu và mô tả kiến trúc là chính xác thường được cung cấp thông qua một quá trình phân tích rủi ro (ví dụ TCVN ISO/IEC 27001) hoặc bằng cách đảm bảo rằng vấn đề an toàn cũng được xác định (ví dụ TCVN 8709 và ISO/IEC 18045).

Các phương pháp tiêu biểu sử dụng kỹ thuật đánh giá tạo lập tài liệu trung gian trong đó quy định vấn đề an toàn (ví dụ Mục tiêu an toàn của ISO/IEC 15408, hoặc tài liệu Chính sách an toàn ISO/IEC 19790). Kỹ thuật kiểm tra sự phù hợp dựa vào một vấn đề bảo mật là được xác định trước trong một đặc tả, thường đã được chuẩn hóa, Ví dụ PCI DSS và ISO/IEC 19790 hoặc FIPS 140-2.

CHÚ THÍCH: Trong ISO/IEC 15408 mô hình một phương tiện truyền bá (a vehicle) được biết đến như là Hồ sơ bảo vệ mô tả một vấn đề an toàn chung cho một loại bản phân phối, như là tài liệu Mục tiêu an toàn mô tả vấn đề an toàn cho Mục tiêu đánh giá cụ thể.

10.6.2 Tiêu chí

b) Vấn đề an toàn được nhận thấy, mô tả và trình bày một cách phù hợp;

c) Bao gồm mô tả các giả định và môi trường;

d) Một phân tích hoặc mô tả nguy cơ và đặc tính của chúng;

10.7 Vòng đời

10.7.1 Thảo luận

Một phương pháp đặc thù có thể cản trở các hoạt động đánh giá khi phân tích một giai đoạn hay nhiều giai đoạn vòng đời đặc thù. Điều này có thể ảnh hưởng đến trường hợp đảm bảo đang được phát triển bởi cơ quan đảm bảo.

10.7.2 Tiêu chí

a) Bất kỳ hạn chế trong phạm vi đánh giá trong các giai đoạn vòng đời được mô tả trong các kết quả.

10.8 Xem xét vận hành

10.8.1 Thảo luận

Cho dù một số phương pháp đảm bảo được thực hiện trong giai đoạn phát triển, hoặc tại một số điểm "chụp nhanh (snapshot)", việc đảm bảo được cấp bởi một phương pháp như vậy có thể chỉ ở mặt ngoài nếu các kiểm soát vận hành trung tâm hay các suy xét môi trường cũng trong giai đoạn này. Những cái này thường được chuyển tải thông qua tài liệu hướng dẫn cụ thể liên quan đến mục tiêu của việc đảm bảo an toàn. Ví dụ như Mục tiêu an toàn đối với các tiêu chí chung chỉ rõ một số trạng thái giả định chắc chắn về môi trường, hoặc các điểm thông tin cấu hình cụ thể cho mục tiêu đánh giá. Tương tự như vậy đảm bảo đủ khả năng bởi ISO/IEC 19790 dựa trên kỹ thuật sẽ chỉ được thực hiện nếu các mô-đun mã hóa được cài đặt, cấu hình và hoạt động phù hợp với các tài liệu Chính sách an toàn.

Cũng có thể có trường hợp đặc biệt chẳng hạn như việc bảo trì phải được xem xét.

10.8.2 Tiêu chí

a) Phương pháp hay chính sách liên quan bao gồm các yêu cầu liên tục giám sát;

CHÚ THÍCH: Nhiều phương pháp xác định các hoạt động như quét điểm yếu và kiểm tra thâm nhập mạng được thực hiện để cung cấp đảm bảo liên tục. Trong trường hợp này cơ quan đảm bảo yêu cầu độ tin cậy đó là các hoạt động đang diễn ra là được thực hiện.

b) Phương pháp xác định rõ ràng các tri gơ (triggers) cho việc giám sát liên tục.

CHÚ THÍCH: Điều này có thể là định kỳ, ví dụ hàng năm, hoặc dựa trên một số tri gơ khác ví dụ trên phiên bản của giao phẩm chính, hoặc một "thay đổi quan trọng". Trong trường hợp sau cùng điều quan trọng là một định nghĩa về "thay đổi quan trọng" đã được đưa ra.