TCVN **TIÊU CHUẨN QUỐC GIA**

TCVN 13723-3:2023
ISO/IEC 19896-3:2018

Xuất bản lần 1

KỸ THUẬT AN TOÀN CÔNG NGHỆ THÔNG TIN – YÊU CẦU VỀ NĂNG LỰC ĐỐI VỚI KIỂM THỬ VIÊN VÀ ĐÁNH GIÁ VIÊN BẢO MẬT THÔNG TIN – PHẦN 3: YÊU CẦU VỀ KIẾN THỨC, KỸ NĂNG VÀ TÍNH HIỆU QUẢ ĐỐI VỚI ĐÁNH GIÁ VIÊN THEO TCVN 8709 (ISO/IEC 15408)

IT security techniques - Competence requirements for information security testers and evaluators - Part 3: Introduction, concepts and general requirements

HÀ NỘI – 2023

Mục lục

Lời nói đầu

TCVN 13723-3:2023 hoàn toàn tương đương với ISO/IEC 19896-3:2018.

TCVN 13723-3:2023 do Cục Quản lý mật mã dân sự và Kiểm định sản phẩm mật mã biên soạn, Ban Cơ yếu Chính phủ đề nghị, Tổng cục Tiêu chuẩn Đo lường Chất lượng thẩm định, Bộ Khoa học và Công nghệ công bố

Bộ tiêu chuẩn TCVN 13723, Kỹ thuật an toàn công nghệ thông tin – Yêu cầu về năng lực đối với Kiểm thử viên và Đánh giá viên bảo mật thông tin, gồm 3 phần:

- TCVN 13723-1, Kỹ thuật an toàn công nghệ thông tin – Yêu cầu về năng lực đối với Kiểm thử viên và Đánh giá viên bảo mật thông tin – Phần 1: Giới thiệu, khái niệm và yêu cầu chung.
- TCVN 13723-2, Kỹ thuật an toàn công nghệ thông tin – Yêu cầu về năng lực đối với Kiểm thử viên và Đánh giá viên bảo mật thông tin – Phần 2: Yêu cầu về kiến thức, kỹ năng và tính hiệu quả đối với Kiểm thử viên theo TCVN 11295 (ISO/IEC 19790).
- TCVN 13723-3, Kỹ thuật an toàn công nghệ thông tin – Yêu cầu về năng lực đối với Kiểm thử viên và Đánh giá viên bảo mật thông tin – Phần 3: Yêu cầu về kiến thức, kỹ năng và tính hiệu quả đối với Đánh giá viên theo TCVN 8709 (ISO/IEC 15408).

Giới thiệu

Bộ tiêu chuẩn TCVN 8709 (ISO/IEC 15408) cho phép so sánh giữa các kết quả của các đánh giá an toàn độc lập. Như vậy nó cung cấp một tập hợp các yêu cầu chung cho chức năng an toàn của các sản phẩm công nghệ thông tin và các biện pháp đảm bảo được áp dụng cho các sản phẩm công nghệ thông tin này trong quá trình đánh giá an toàn. Nhiều chương trình xác nhận và đánh giá cũng như các cơ quan đánh giá đã được phát triển bằng cách áp dụng bộ tiêu chuẩn TCVN 8709 (ISO/IEC 15408) và TCVN 11386:2016 (ISO/IEC 18045:2008) làm cơ sở, cho phép so sánh giữa các kết quả của các dự án đánh giá.

Một yếu tố quan trọng trong việc đảm bảo khả năng so sánh các kết quả đánh giá đó là hiểu được quá trình đánh giá bao gồm đặc điểm của các biện pháp đảm bảo khách quan và chủ quan. Do đó, năng lực của từng đánh giá viên là rất quan trọng khi khả năng so sánh và tính lặp lại của các kết quả đánh giá là nền tảng để thừa nhận lẫn nhau.

TCVN ISO/IEC 17025:2017 (ISO/IEC 17025:2017), đưa ra các yêu cầu chung về năng lực của các phòng thử nghiệm và hiệu chuẩn. Trong tiêu chuẩn TCVN ISO/IEC 17025:2017 (ISO/IEC 17025:2017), thường được quy định các cơ sở thử nghiệm tuân theo tiêu chuẩn, trong điều khoản 5.2.1 nêu rõ rằng "Tất cả nhân sự của phòng thử nghiệm, cả nội bộ hoặc bên ngoài, có thể ảnh hưởng đến hoạt động thử nghiệm đều phải có năng lực, hành động một cách khách quan và thực hiện công việc đúng theo hệ thông quản lý của phòng thử nghiệm".

Tiêu chuẩn này thiết lập phạm vi năng lực tối thiểu của các chuyên gia đánh giá áp dụng TCVN 8709 (ISO/IEC 15408) với mục tiêu thiết lập sự phù hợp trong các yêu cầu đối với việc đào tạo các chuyên gia đánh giá TCVN 8709 (ISO/IEC 15408) liên quan đến các cơ quan và chương trình đánh giá sản phẩm công nghệ thông tin. Nó cung cấp các yêu cầu chuyên môn để chứng minh năng lực của các cá nhân trong việc thực hiện đánh giá sản phẩm an toàn công nghệ thông tin phù hợp với TCVN 8709 (ISO/IEC 15408) và TCVN 11386:2016 (ISO/IEC 18045:2008). TCVN 8709-1:2011 (ISO/IEC 15408-1:2009) mô tả khuôn khổ chung về năng lực bao gồm các yếu tố khác nhau như năng lực, kiến thức, kỹ năng, kinh nghiệm, đào tạo và hiệu quả. Tiêu chuẩn này bao gồm các kiến thức và kỹ năng đặc biệt trong các lĩnh vực sau đây.

- An toàn thông tin

  Kiến thức: Các nguyên tắc an toàn thông tin, các thuộc tính an toàn thông tin, các mối đe dọa và lỗ hổng an toàn thông tin.

  Kỹ năng: Hiểu các yêu cầu về an toàn thông tin, hiểu bối cảnh.

- Đánh giá an toàn thông tin

  Kiến thức: Kiến thức về TCVN 8709 (ISO/IEC 15408) và TCVN 8709-1:2011 (ISO/IEC 15408-1:2009), hệ thống quản lý phòng thử nghiệm.

  Kỹ năng: Kỹ năng đánh giá cơ bản, kỹ năng đánh giá điểm trung tâm, kỹ năng cần có khi đánh giá các lớp đảm bảo an toàn cụ thể, các kỹ năng cần có khi đánh giá các lớp yêu cầu chức năng an toàn cụ thể.

- Kiến trúc hệ thống thông tin

  Kiến thức: Công nghệ đang được đánh giá.

  Kỹ năng: Hiểu sự tương tác của các thành phần an toàn và thông tin.

- Kiểm thử an toàn thông tin

  Kiến thức: Kỹ thuật kiểm thử an toàn thông tin, công cụ kiểm thử an toàn thông tin, vòng đời phát triển sản phẩm, kiểu kiểm thử.

  Kỹ năng: Tạo và quản lý kế hoạch kiểm thử an toàn thông tin, kiểm thử thiết kế an toàn thông tin, chuẩn bị và tiến hành kiểm thử an toàn thông tin.

Đối tượng của tiêu chuẩn này này bao gồm: các cơ quan có thẩm quyền phê duyệt và chứng nhận, các cơ quan công nhận phòng thử nghiệm, các kế hoạch đánh giá, cơ sở thử nghiệm, đánh giá viên và các tổ chức cung cấp chứng chỉ nghề nghiệp.

Kỹ thuật an toàn công nghệ thông tin – Yêu cầu về năng lực đối với Kiểm thử viên và Đánh giá viên bảo mật thông tin – Phần 3: Yêu cầu về kiến thức, kỹ năng và tính hiệu quả đối với Đánh giá viên theo TCVN 8709 (ISO/IEC 15408)

IT security techniques - Competence requirements for information security testers and evaluators - Part 3: Knowledge, skills and effectiveness requirements for: ISO/IEC 15408 evaluators

1 Phạm vi áp dụng

Tiêu chuẩn này cung cấp các yêu cầu chuyên môn để chứng minh năng lực của các cá nhân trong việc thực hiện đánh giá an toàn sản phẩm công nghệ thông tin phù hợp với TCVN 8709 (ISO/IEC 15408) và TCVN 11386:2016 (ISO/IEC 18045:2008).

2 Tài liệu viện dẫn

Các tài liệu viện dẫn sau đây là cần thiết cho việc áp dụng tiêu chuẩn này. Đối với các tài liệu có ghi năm công bố thì áp dụng phiên bản đã nêu. Đối với các tài liệu không ghi năm công bố thì áp dụng phiên bản mới nhất (bao gồm cả sửa đổi, bổ sung).

- TCVN 8709 (ISO/IEC 15408), Công nghệ thông tin - Kỹ thuật an toàn - Tiêu chí đánh giá an toàn về công nghệ thông tin.
- TCVN 11386:2016 (ISO/IEC 18045:2008), Công nghệ thông tin - Kỹ thuật an toàn - Phương pháp đánh giá an toàn công nghệ thông tin.
- TCVN ISO/IEC 17025:2017 (ISO/IEC 17025:2017), Yêu cầu chung về năng lực của các phòng thử nghiệm và hiệu chuẩn.
- TCVN 13723-1:2023 (ISO/IEC 19896-1), Kỹ thuật an toàn công nghệ thông tin – Yêu cầu về năng lực đối với Kiểm thử viên và Đánh giá viên bảo mật thông tin – Phần 1: Giới thiệu, khái niệm và yêu cầu chung.

3 Thuật ngữ và định nghĩa

Tiêu chuẩn này sử dụng các định nghĩa và thuật ngữ sau đây:

3.1

Kế hoạch đánh giá (evaluation scheme)

Tổ chức thực hiện các chính sách và bộ quy tắc do cơ quan đánh giá thiết lập, xác định môi trường đánh giá, bao gồm các tiêu chí và phương pháp luận cần thiết để tiến hành đánh giá an toàn công nghệ thông tin.

3.2

Phương pháp chủ quan (subjective method)

Phương pháp dựa trên kinh nghiệm và sự hiểu biết nhất định của một người.

4 Kiến thức

4.1 Yêu cầu chung

Kiến thức là những gì một đánh giá viên biết và có thể mô tả. Các điều khoản từ 4.2 đến 4.8 đề cập đến kiến thức cần thiết để đánh giá theo TCVN 8709 (ISO/IEC 15408) và TCVN 11386:2016 (ISO/IEC 18045:2008).

4.2 Kiến thức về TCVN 8709 (ISO/IEC 15408) và TCVN 11386:2016

4.2.1 TCVN 8709-1:2011 (ISO/IEC 15408-1:2009)

Tất cả đánh giá viên phải có kiến thức về:

a) Các thuật ngữ và định nghĩa được xác định trong TCVN 8709-1:2011 (ISO/IEC 15408-1:2009);
b) Các thuật ngữ và định nghĩa được xác định trong TCVN 11386:2016 (ISO/IEC 18045:2008);
c) Phạm vi đánh giá TCVN 8709-1:2011 (ISO/IEC 15408-1:2009);

d) Mô hình tổng thể cho bộ TCVN 8709 (ISO/IEC 15408) được nêu trong TCVN 8709-1:2011 (ISO/IEC 15408-1:2009);
e) Điều chỉnh các yêu cầu an toàn: hoạt động, sự phụ thuộc giữa các thành phần và các thành phần mở rộng;
f) Hồ sơ bảo vệ và các gói hồ sơ bảo vệ;
g) Kết quả đánh giá;
h) Đặc điểm kỹ thuật của các mục tiêu an toàn.

4.2.2 TCVN 8709-2:2011 (ISO/IEC 15408-2:2008)

Tất cả đánh giá viên phải có kiến thức về các yêu cầu chức năng an toàn (security functional requirements - SFR) trong TCVN 8709-2:2011 (ISO/IEC 15408-2:2008) được sử dụng cho các loại công nghệ mà đánh giá viên được ủy quyền làm việc, cũng như bất kỳ SFR phụ thuộc nào. Các loại SFR được đưa ra trong TCVN 8709-2:2011 (ISO/IEC 15408-2:2008) là:

a) Kiểm thử an toàn (security audit - FAU);
b) Trao đổi thông tin (communication - FCO);
c) Hỗ trợ mật mã (cryptographic support - FCS);
d) Bảo vệ dữ liệu người dùng (user data protection - FDP);
e) Xác thực và định danh (identification and authentication - FIA);
f) Quản lý an toàn (security management - FMT);
g) Quyền riêng tư (privacy - FPR);
h) Bảo vệ mục tiêu trong đánh giá chức năng an toàn (protection of the target of evaluation security functions - FPT);
i) Sử dụng tài nguyên (resource utilisation - FRU);
j) Mục tiêu của tiếp cận đánh giá (target of evaluation access - FTA)
k) Đường dẫn/Kênh tin cậy (trusted path/channels - FTP).

4.2.3 TCVN 8709-3:2011 (ISO/IEC 15408-3:2008)

Tất cả đánh giá viên phải có kiến thức về các yêu cầu đảm bảo an toàn (security assurance requirements - SAR) được đưa ra trong TCVN 8709-3:2011 (ISO/IEC 15408-3:2008) được quy định bởi mục tiêu an toàn (security targets - ST) mà đánh giá viên được ủy quyền làm việc.

Kiến thức về các thành phần SAR cụ thể phải bao gồm những thành phần mà đánh giá viên được phép làm việc. Các dạng SAR được đưa ra trong TCVN 8709-3:2011 (ISO/IEC 15408-3:2008) là:

a) Phát triển (development - ADV);
b) Tài liệu hướng dẫn (guidance documentation - ADG);
c) Hỗ trợ vòng đời (life-cycle support - ALC);
d) Cấu trúc mục tiêu an toàn (security target structure - ASE);
e) Cấu trúc hồ sơ bảo vệ (protection profile structure - APE);
f) Kiểm thử (tests - ATE);
g) Đánh giá tính dễ tổn thương (vulnerability assessment - AVA);
h) Thành phần cấu tạo (composition - ACO).

4.2.4 TCVN 11386:2016 (ISO/IEC 18045:2008)

Tất cả đánh giá viên phải có kiến thức về:

a) Quy trình đánh giá: Quy trình này được mô tả trong điều khoản 8 của TCVN 11386:2016 (ISO/IEC 18045:2008);

b) Phương pháp và hoạt động đánh giá an toàn: Thông tin này được nêu trong TCVN 11386:2016 (ISO/IEC 18045:2008).

4.3 Kiến thức về mô hình bảo đảm

4.3.1 Kiến thức, sự hiểu biết của cơ quan đánh giá

Tất cả các đánh giá viên phải có kiến thức, hiểu được các yêu cầu của cơ quan đánh giá hoặc cơ quan đánh giá có thể áp dụng cho các chương trình đánh giá mà họ được ủy quyền làm việc.

CHÚ THÍCH: Ví dụ về thẩm quyền đánh giá như vậy bao gồm: "Thỏa thuận thừa nhận tiêu chí chung (CCRA)" và "Hệ thống an toàn thông tin của nhóm cao cấp (SOG-IS)".

Các yêu cầu thẩm quyền đánh giá có thể bao gồm các chủ đề như:

a) Phạm vi thẩm quyền đánh giá;

b) Các thỏa thuận công nhận;

c) Các chính sách thẩm quyền đánh giá;

d) Hướng dẫn các kết hoạch đánh giá, tổ chức công nhận và Đánh giá viên;

e) Cách diễn giải;

f) Các tài liệu hỗ trợ;

g) Kiến thức về các tiêu chuẩn liên quan;

h) Yêu cầu chất lượng.

4.3.2 Kiến thức về quy trình đánh giá

Chương trình đánh giá thường xác định các khía cạnh hoạt động như các chính sách và thủ tục cụ thể cho từng chương trình đánh giá. Các mục như vậy thường dựa trên phạm vi của chương trình đánh giá.

Tất cả những đánh giá viên phải có kiến thức về:

a) Các yêu cầu của chương trình đánh giá hoặc các kế hoạch mà họ được ủy quyền làm việc;

Ví dụ:

- Bất kỳ chính sách, quy định và luật pháp cụ thể nào đối với ngành nghề đó;
- Các yêu cầu phê duyệt của phòng thử nghiệm đối với chương trình đánh giá;
- Chính sách chương trình đánh giá liên quan đến các dự án đánh giá bao gồm: các tiêu chí đầu vào, thời hạn, yêu cầu báo cáo, yêu cầu khảo sát thực địa;
- Hướng dẫn của người phê duyệt hoặc đánh giá viên;
- Các diễn giải cụ thể về chương trình đánh giá;
- Hướng dẫn cụ thể chương trình đánh giá;
- Hồ sơ bảo vệ được phê duyệt và các tài liệu hỗ trợ của chúng;
- Kế hoạch các phương pháp đánh giá và hoạt động đảm bảo cụ thể;
- Yêu cầu báo cáo.

b) Các yêu cầu về năng lực của chương trình đánh giá đối với đánh giá viên.

CHÚ THÍCH: Xem TCVN 11386:2016 (ISO/IEC 18045:2008), A.5 để biết hướng dẫn về các chương trình đánh giá về chủ đề này.

4.3.3 Kiến thức và hệ thống quản lý của phòng thử nghiệm

Tất cả những đánh giá viên phải có kiến thức về:

a) Hệ thống quản lý của phòng thử nghiệm, bao gồm các chính sách, quy trình và thủ tục có thể áp dụng cho đánh giá viên;

b) Các phương pháp được phòng thử nghiệm phê duyệt;

c) Các yêu cầu về năng lực của phòng thử nghiệm.

CHÚ THÍCH: Các hệ thống quản lý khác nhau rất nhiều trong việc triển khai các yêu cầu. Tuy nhiên, các hạng mục như: kiểm soát tài liệu, kiểm soát hồ sơ, kiểm soát công việc kiểm thử hoặc hiệu chuẩn không phù hợp, xử lý hồ sơ kỹ thuật và xung đột lợi ích thường là trách nhiệm liên quan trực tiếp đến đánh giá viên. Hầu hết các hệ thống quản lý phòng thử nghiệm đều áp dụng theo TCVN ISO/IEC 17025:2017 (ISO/IEC 17025:2017).

4.4 Kiến thức về an toàn thông tin

Tất cả đánh giá viên phải có kiến thức về:

a) Các nguyên tắc an toàn;

b) Thuộc tính an toàn;

c) Cơ chế tấn công;

d) Khái niệm về khả năng tấn công;

e) Vòng đời phát triển an toàn;

f) Kiểm thử an toàn;

g) Các lỗ hổng và điểm yếu.

4.5 Kiến thức về công nghệ được đánh giá

4.5.1 Kiến thức về công nghệ được đánh giá

TCVN 8709 (ISO/IEC 15408) và TCVN 11386:2016 (ISO/IEC 18045:2008) có thể được sử dụng trong đánh giá trong công nghệ thông tin ở phạm vi rộng. Các công nghệ này thường được phân loại thành các loại công nghệ khác nhau theo các chương trình đánh giá, cơ quan đánh giá hoặc các cơ quan khác.

Tất cả những đánh giá viên phải có kiến thức về các loại công nghệ thông tin được họ đánh giá, bao gồm cả các kiến trúc an toàn chung được triển khai cho loại công nghệ đó.

CHÚ THÍCH: Phụ lục A cung cấp thông tin về danh sách các chủ đề kiến thức được trình bày bởi các loại công nghệ thường được xác định.

Ví dụ: Các loại công nghệ thường được xác định bao gồm:

- Các thiết bị và hệ thống kiểm soát truy cập;
- Mã hóa, quản lý khóa và hệ thống PKI, các sản phẩm cho chữ ký số;
- Cơ sở dữ liệu;
- Hệ điều hành;
- Mạng và các thiết bị và hệ thống liên quan đến mạng;
- Thiết bị và hệ thống di động;
- Các thiết bị đa chức năng;
- IC, thẻ thông minh và các thiết bị và hệ thống liên quan đến thẻ thông minh;
- Thiết bị phần cứng;
- Hệ thống và phát hiện thiết bị;
- Bảo vệ dữ liệu, thiết bị sinh trắc học và hệ thống, máy tính tin cậy.

4.5.2 Hồ sơ bảo vệ, cách đóng gói và tài liệu hỗ trợ

Tất cả những đánh giá viên phải có kiến thức theo mô tả sau đây để áp dụng trong đánh giá công nghệ thông tin:

a) Hồ sơ bảo vệ, đóng gói và bất kỳ tài liệu hỗ trợ liên quan nào được chỉ định liên quan đến công việc của đánh giá viên;

b) Kiến thức cần thiết để đáp ứng bất kỳ phương pháp đánh giá bổ sung nào và các hoạt động đảm bảo được chỉ định để áp dụng cho một cuộc đánh giá;

c) Cách xác định xem có bất kỳ diễn giải hoặc hướng dẫn nào liên quan đến hồ sơ bảo vệ, cách đóng gói và các tài liệu hỗ trợ liên quan đã được ban hành hay không và liệu chúng có thể áp dụng cho một dự án đánh giá cụ thể nào hay không.

4.6 Kiến thức cần thiết cho các lớp đảm bảo cụ thể

Đánh giá viên cần có kiến thức theo yêu cầu của các phương pháp đánh giá và các hoạt động được chỉ định đảm bảo cho các lớp mà họ được ủy quyền làm việc. Các ví dụ về kiến thức theo yêu cầu của TCVN 11386:2016 (ISO/IEC 18045:2008) được nêu trong Phụ lục B.

4.7 Kiến thức cần thiết khi đánh giá các yêu cầu chức năng an toàn cụ thể

Đánh giá viên phải có kiến thức cần thiết theo yêu cầu chức năng an toàn mà họ được ủy quyền để đánh giá như quy định trong TCVN 8709-2:2011 (ISO/IEC 15408-2:2008). Thông tin yêu cầu về kiến thức theo mô tả trong TCVN 8709-2:2011 (ISO/IEC 15408-2:2008) được nêu trong Phụ lục C.

4.8 Kiến thức cần thiết khi đánh giá các công nghệ cụ thể

Vì công nghệ có thể thay đổi và liên tục phát triển nên không thể xác định tất cả các kỹ năng cần thiết. Phụ lục A cung cấp thông tin về danh sách các kiến thức và kỹ năng đối với một số công nghệ. Ngoài ra, tài liệu tham khảo cũng cung cấp nhiều tài liệu liên quan đến công nghệ.

Kiến thức về loại công nghệ có thể thu được thông qua kinh nghiệm tương tác với công nghệ đó. Kinh nghiệm có thể tích luy được thông qua:

a) Tham dự khóa đào tạo kỹ năng liên quan đến công nghệ;

b) Làm việc với tư cách là một thực tập sinh cùng với một Đánh giá viên có kinh nghiệm;

c) Làm việc trong quá trình phát triển các công nghệ đó

d) Thực hiện nghiên cứu về công nghệ.

5 Kỹ năng

5.1 Kỹ năng đánh giá cơ bản

5.1.1 Phương pháp đánh giá

Tất cả đánh giá viên phải có kỹ năng về các phương pháp đánh giá cơ bản. Chúng bao gồm phương pháp khách quan và chủ quan, bao gồm:

a) Lấy mẫu;

b) Phân tích thống kê cơ bản;

c) Quan sát;

d) Phân tích;

e) So sánh;

f) Ghi kết quả.

5.1.2 Công cụ đánh giá

Đánh giá viên phải có kỹ năng:

a) Việc sử dụng các công cụ được phòng thử nghiệm hoặc chương trình đánh giá quy định để hỗ trợ đánh giá, tạo báo cáo, cung cấp hoặc bảo vệ các tài liệu và kết quả;

Ví dụ:

- Công cụ mã hóa;
- Công cụ tài liệu.

b) Các công cụ chuyên dụng cho các nhiệm vụ đánh giá nhất định theo quy định của phòng thử nghiệm hoặc chương trình đánh giá hoặc các tài liệu hỗ trợ.

Ví dụ:

- Các công cụ toán học chuyên dụng để phân tích dữ liệu đo được;
- Các công cụ để xác minh việc thực hiện các thuật toán mã.

5.2 Các kỹ năng đánh giá cốt lõi được đưa ra trong TCVN 8709-3:2011 và TCVN 11386:2016

5.2.1 Nguyên tắc đánh giá

Tất cả đánh giá viên sẽ có thể thực hiện công việc của họ theo cách:

a) Công bằng;

b) Khách quan;

c) Khả năng lặp lại;

d) Khả năng tái tạo.

5.2.2 Các phương pháp và hoạt động đánh giá

Tất cả đánh giá viên phải có kỹ năng về các phương pháp và hoạt động đánh giá cốt lõi được quy định trong TCVN 11386:2016 (ISO/IEC 18045:2008), hồ sơ bảo vệ và các tài liệu hỗ trợ.

Các từ sau đây có ý nghĩa đặc biệt trong TCVN 11386:2016 (ISO/IEC 18045:2008) và đánh giá viên phải có kỹ năng thực hiện các hoạt động phù hợp với các định nghĩa được đưa ra trong TCVN 11386:2016 (ISO/IEC 18045:2008). Chúng được diễn đạt bằng các từ sau:

a) Kiểm tra;

b) Xác nhận;

c) Chứng minh;

d) Mô tả;

e) Xác định;

f) Đảm bảo;

g) Khảo sát toàn diện;

h) Xem xét;

i) Giải thích;

j) Biện minh;

k) Chứng minh;

l) Báo cáo;

m) Ghi chép;

n) Ghi chú;

o) Lưu bằng chứng;

p) Xác minh.

CHÚ THÍCH: Các thuật ngữ này được định nghĩa và giải thích trong TCVN 8709-1:2011 (ISO/IEC 15408-1:2009) hoặc TCVN 11386:2016 (ISO/IEC 18045:2008).

5.3 Các kỹ năng cần thiết khi đánh giá các lớp đảm bảo an toàn cụ thể

5.3.1 Yêu cầu chung

Đánh giá viên thực hiện các hoạt động đánh giá phải có thể viết báo cáo nhận xét.

Các kỹ năng cần thiết khác được liệt kê cho mỗi lớp trong Bảng 1 đến Bảng 7. Trong từng phần được mô tả dưới đây, các kỹ năng cần thiết đó mở rộng về cả chiều rộng lẫn chiều sâu. Các kỹ năng cao được liệt kê bổ sung trong thêm trong từng phần trong khi các kỹ năng đòi hỏi ở mức ở độ sâu hơn không được đề cập rõ ràng nhưng sẽ được xem xét khi ủy quyền cho đánh giá viên.

Ví dụ 1: Đánh giá viên được ủy quyền đánh giá ADV_FSP.2 cần có khả năng kiểm tra theo dõi các liên kết của các SFR trước khi nhận được ủy quyền cho ADV_FSP.3.

Ví dụ 2: Đối với ADV_TDS.1, chỉ yêu cầu các kỹ năng cơ bản liên quan đến kiến trúc TOE, trong khi đối với ADV_TDS.6, các kỹ năng xử lý các phương thức chính thức cho kiến trúc được yêu cầu.

5.3.2 Lớp ADV (Phát triển)

Đánh giá viên thực hiện các hoạt động đánh giá liên quan đến lớp ADV phải có các kỹ năng được xác định trong Bảng 1 cho các thành phần đảm bảo cho đến và bao gồm cả thành phần mà họ đang đánh giá.

Bảng 1 - Kỹ năng cần thiết cho đánh giá viên lớp ADV

Thành phần đảm bảo	Kỹ năng đánh giá cần thiết
ADV_ARC.1	a) Có khả năng kiểm tra chéo kiến trúc thông tin với các bằng chứng khác được cung cấp cho việc đánh giá.
ADV_FSP.1	a) Có khả năng xác định các giao diện chương trình và ứng dụng; b) Có khả năng xác định TSFIs.
ADV_FSP.2	Không có yêu cầu bổ sung.
ADV_FSP.3	c) Có thể kiểm tra theo dõi các liên kết của các SFR;
ADV_FSP.4	Không có yêu cầu bổ sung.
ADV_FSP.5	d) Có khả năng hiểu một phần ngôn ngữ diễn đạt;
ADV_FSP.6	e) Có khả năng hiểu hình thức ngôn ngữ diễn đạt; f) Có thể xác minh tính đúng đắn của mô hình chính và tính hoàn chỉnh của lập luận.
ADV_IMP.1	a) Sử dụng các kỹ thuật lấy mẫu; b) Có khả năng đọc và hiểu mã nguồn hoặc sơ đồ phần cứng hoặc mã ngôn ngữ thiết kế phần cứng IC hoặc dữ liệu bố trí được sử dụng trong việc triển khai TOE; c) Có khả năng sử dụng các công cụ cho phép tháo vỏ bảo vệ hoặc gỡ rối; d) Có khả năng hiểu các công cụ mới phát sinh trong quá trình đánh giá, cách sử dụng và tác dụng của chúng. Ví dụ: Các cấu hình của trình biên dịch.

ADV_IMP.2	Không có yêu cầu bổ sung.
ADV_INT.1	Không có yêu cầu bổ sung.
ADV_INT.2	a) Có khả năng xác định các tiêu chuẩn liên quan đến TSF để xác định xem TSF có được cấu trúc tốt hay không;
ADV_INT.3	b) Có khả năng đánh giá mức độ phức tạp bên trong TSF;
ADV_SPM.1	Có thể hiểu mô hình chính sách an toàn và xác định xem mô hình đó có hoàn chỉnh hay không;
ADV_TDS.1	Có thể hiểu cấu trúc của TOE.
ADV_TDS.2	Không có yêu cầu bổ sung.
ADV_TDS.3	Không có yêu cầu bổ sung.
ADV_TDS.4	Không có yêu cầu bổ sung.
ADV_TDS.5	Không có yêu cầu bổ sung.
ADV_TDS.6	Không có yêu cầu bổ sung.

5.3.3 Lớp AGD (Tài liệu hướng dẫn)

Đánh giá viên thực hiện các hoạt động đánh giá liên quan đến lớp AGD phải có các kỹ năng được xác định trong Bảng 2 đảm bảo cho các thành phần mà họ đang đánh giá.

Bảng 2 - Các kỹ năng cần thiết cho đánh giá viên lớp AGD

Thành phần đảm bảo	Kỹ năng đánh giá cần thiết
AGD.OPE.1	Có thể hiểu rằng hoạt động là chính xác và an toàn theo các bằng chứng;
AGD_PRE.1	Có thể hiểu rằng việc cài đặt là chính xác và an toàn theo các bằng chứng;

5.3.4 Lớp ALC (Hỗ trợ vòng đời)

Đánh giá viên thực hiện các hoạt động đánh giá liên quan đến lớp ALC phải có các kỹ năng được xác định trong Bảng 3 đảm bảo cho các thành phần mà họ đang đánh giá.

Bảng 3 - Các kỹ năng cần thiết cho đánh giá viên lớp ALC

Thành phần đảm bảo	Kỹ năng đánh giá cần thiết
ALC_CMC.1	Có khả năng quan sát việc sử dụng hệ thống CM như đã mô tả trong kế hoạch CM;
ALC_CMC.2	Không có yêu cầu bổ sung.
ALC_CMC.3	Không có yêu cầu bổ sung.
ALC_CMC.4	Không có yêu cầu bổ sung.
ALC_CMC.5	Không có yêu cầu bổ sung.
ALC_CMS.1	a) Có khả năng hiểu lược đồ xác định và lập phiên bản; b) Có thể xác định xem các mục cấu hình có được xác định duy nhất hay không.
ALC_CMS.2	Không có yêu cầu bổ sung.
ALC_CMS.3	Không có yêu cầu bổ sung.
ALC_CMS.4	Không có yêu cầu bổ sung.
ALC_CMS.5	Không có yêu cầu bổ sung.

ALC_DEL.1	Có thể tuân thủ các quy trình bàn giao và thiết lập bằng văn bản.
ALC_DVS.1	a) Lập kế hoạch khảo sát thực địa; b) Kỹ thuật đánh giá tại chỗ và nhân sự; c) Có khả năng quan sát việc áp dụng các biện pháp an toàn trong quá trình phát triển và duy trì TOE như được mô tả trong tài liệu phát triển an toàn; d) Có khả năng quan sát việc áp dụng thực tế các thủ tục bàn giao như được mô tả trong tài liệu bàn giao.
ALC_DVS.2	Không có yêu cầu bổ sung.
ALC_FLR.1	Có khả năng hiểu các quy trình khắc phục sai sót.
ALC_FLR.2	Không có yêu cầu bổ sung.
ALC_LCD.1	Có khả năng phân tích các quy trình vòng đời do nhà phát triển trình bày.
ALC_LCD.2	Không có yêu cầu bổ sung.
ALC_TAT.1	Có khả năng phân tích các công cụ và kỹ thuật được trình bày bởi nhà phát triển.
ALC_TAT.2	Không có yêu cầu bổ sung.
ALC_TAT.3	Không có yêu cầu bổ sung.

5.3.5 Các lớp ASE và APE (Đánh giá ST và PP)

Đánh giá viên thực hiện các hoạt động đánh giá liên quan đến lớp ASE phải có các kỹ năng được xác định trong Bảng 4 cho các thành phần đảm bảo mà họ đang đánh giá.

Bảng 4 - Các kỹ năng cần thiết cho Đánh giá viên lớp ASE và APE

Thành phần đảm bảo		Kỹ năng đánh giá cần thiết
ASE_CCL.1	APE_CCL.1	Có thể kiểm tra xem tuyên bố về sự phù hợp là đúng.
ASE_ECD.1	APE_ECD.1	Có thể hiểu rằng định nghĩa các thành phần mở rộng là đúng.
ASE_INT.1	APE_INT.1	Có thể hiểu rằng phần giới thiệu mô tả TOE và phạm vi TOE một cách chính xác.
ASE_OBJ.1	APE_OBJ.1	a) Có khả năng xác định xem các mục tiêu an toàn có giải quyết đầy đủ và giải quyết các vấn đề an toàn đã xác định hay không; b) Có khả năng xác định xem các mục tiêu an toàn có được phân chia hợp lý giữa các mục tiêu an toàn của TOE và các mục tiêu an toàn cho môi trường TOE một cách chính xác và giải quyết các vấn đề an toàn đã xác định hay không.
ASE_OBJ.2	APE_OBJ.2	Không có yêu cầu bổ sung.
ASE_REQ.1	APE_REQ.1	Có thể xác định rằng các yêu cầu an toàn là rõ ràng, không rõ ràng và được xác định rõ ràng.
ASE_REQ.2	APE_REQ.2	Không có yêu cầu bổ sung.
ASE_SPD.1	APE_SPD.1	Có thể hiểu rằng định nghĩa vấn đề an toàn là đúng.
ASE_TSS.1		Có thể ánh xạ tường thuật đến các SFR cụ thể.

5.3.6 Lớp ATE (Kiểm thử)

Đánh giá viên thực hiện các hoạt động đánh giá liên quan đến lớp ATE phải có các kỹ năng được xác định trong Bảng 5 đảm bảo cho các thành phần mà họ đang đánh giá.

Bảng 5 - Các kỹ năng cần thiết cho đánh giá viên lớp ATE

Thành phần đảm bảo	Yêu cầu kỹ năng đánh giá
ATE_COV.1	a) Có khả năng hiểu được phạm vi kiểm thử được đưa ra; b) Có khả năng hiểu các bài kiểm thử và xác minh rằng kết quả của các bài kiểm thử là chính xác;
ATE_COV.2	Không có yêu cầu bổ sung.
ATE_COV.3	Không có yêu cầu bổ sung.
ATE_DPT.1	a) Có thể hiểu tài liệu về phạm vi kiểm thử do nhà phát triển cung cấp; b) Có thể hiểu được kiểm thử ở cấp hệ thống con.
ATE_DPT.2	Có thể hiểu được kiểm thử ở cấp độ mô-đun.
ATE_DPT.3	Không có yêu cầu bổ sung.
ATE_DPT.4	Không có yêu cầu bổ sung.
ATE_FUN.1	Có thể hiểu tài liệu kiểm thử chức năng do nhà phát triển cung cấp.
ATE_FUN.2	Không có yêu cầu bổ sung.
ATE_IND.1	a) Xây dựng kế hoạch kiểm thử; b) Phát triển các trường hợp kiểm thử thích hợp; c) Cấu hình của TOE; d) Thiết lập và cấu hình môi trường TOE; e) Duy trì tính toàn vẹn của môi trường kiểm thử; f) Cấu hình và sử dụng các công cụ kiểm thử được chỉ định trong kế hoạch kiểm thử; g) Khai thác vận hành các bộ kiểm thử thích hợp và các tập lệnh kiểm thử. LƯU Ý: Điều này có thể bao gồm việc sử dụng các ngôn ngữ lập trình, kịch bản ngôn ngữ và các phương tiện gỡ lỗi.
ATE_IND.2	Không có yêu cầu bổ sung.
ATE_IND.3	Không có yêu cầu bổ sung.

5.3.7 Lớp AVA (Đánh giá lỗ hổng)

Đánh giá viên thực hiện các hoạt động đánh giá liên quan đến lớp AVA phải có các kỹ năng được xác định trong Bảng 6 đảm bảo cho các thành phần mà họ đang đánh giá.

Bảng 6 - Các kỹ năng cần thiết cho đánh giá viên lớp AVA

Thành phần đảm bảo	Kỹ năng đánh giá cần thiết
AVA_VAN.1	a) Có khả năng xác định các từ khóa thích hợp để tìm kiếm lỗ hổng; b) Có khả năng xác định các nguồn thông tin thích hợp về các lỗ hổng được biết đến công khai đối với một TOE cụ thể; c) Có khả năng hiểu bằng chứng phân tích lỗ hổng và xác minh rằng kết quả bằng chứng là chính xác; d) Có khả năng phân tích nguyên nhân các mối quan hệ và tác động của chức năng TOE; e) Có khả năng xác định các lỗ hổng còn sót lại; f) Có khả năng tính toán khả năng tấn công.
AVA_VAN.2	Không có yêu cầu bổ sung.

AVA_VAN.3	g) Khả năng phát triển giả thuyết lỗi;
AVA_VAN.4	Không có yêu cầu bổ sung.
AVA_VAN.5	Không có yêu cầu bổ sung.

5.3.8 Lớp ACO (Thành phần)

Đánh giá viên thực hiện các hoạt động đánh giá liên quan đến lớp ACO phải có các kỹ năng được xác định trong Bảng 7 đảm bảo cho các thành phần mà họ đang đánh giá.

Bảng 7 - Các kỹ năng cần thiết cho đánh giá viên cấp ACO

Thành phần đảm bảo	Kỹ năng đánh giá cần thiết
ACO_COR.1	Không có yêu cầu bổ sung.
ACO_DEV.1	Không có yêu cầu bổ sung.
ACO_DEV.2	Không có yêu cầu bổ sung.
ACO_DEV.3	Không có yêu cầu bổ sung.
ACO_REL.1	Không có yêu cầu bổ sung.
ACO_REL.2	Không có yêu cầu bổ sung.
ACO_CTT.1	Các kỹ năng được xác định cho lớp ADV_FSP cho trong Bảng 1;
ACO_CTT.2	Không có yêu cầu bổ sung.
ACO_VUL.1	a) Các kỹ năng được xác định cho lớp AVA_VAN cho trong Bảng 6; b) Có khả năng xác định xem các giả định và mục tiêu được chỉ định cho từng môi trường hoạt động thành phần có còn đúng đối với một TOE tổng hợp hay không; c) Có khả năng xác định các lỗ hổng được đưa vào do kết quả của việc cấu thành; d) Có khả năng thực hiện kiểm thử xâm nhập.
ACO_VUL.2	Không có yêu cầu bổ sung.
ACO_VUL.3	Không có yêu cầu bổ sung.

5.4 Các kỹ năng cần thiết khi đánh giá các lớp yêu cầu chức năng an toàn cụ thể

5.4.1 Yêu cầu chung

Đối với mỗi lớp, đánh giá viên sẽ có thể sẽ:

a) Hiểu và kiểm thử sự phù hợp với các tiêu chuẩn, công nghệ liên quan;

b) Tìm kiếm các lỗ hổng tiềm ẩn và các kênh kề.

5.4.2 Các kỹ năng cần thiết khi đánh giá lớp FCS (Hỗ trợ mật mã)

Có thể xác định xem các thuật toán mật mã và giao thức có được triển khai chính xác hay không.

5.5 Các kỹ năng cần thiết khi đánh giá các công nghệ cụ thể

Vì công nghệ có thể thay đổi và liên tục phát triển nên không thể xác định tất cả các kỹ năng cần thiết. Phụ lục A cung cấp thông tin về danh sách các kiến thức và kỹ năng đối với một số công nghệ.

Các kỹ năng liên quan đến công nghệ có thể đạt được thông qua kinh nghiệm với công nghệ đó. Kinh nghiệm như vậy có thể được phát triển bằng cách:

a) Tham dự khóa đào tạo kỹ năng liên quan đến công nghệ;

b) Làm việc với tư cách là một thực tập sinh cùng với một đánh giá viên có kinh nghiệm;

c) Làm việc trong quá trình phát triển các công nghệ;

d) Thực hiện nghiên cứu về công nghệ.

6 Kinh nghiệm

Kinh nghiệm cốt lõi về các kỹ năng đánh giá, nêu trong điều khoản 5, có được trong lần đánh giá đầu tiên và các lần tiếp theo do đánh giá viên thực hiện. Với tư cách là một học viên, những kinh nghiệm đó cần đạt được dưới sự giám sát hoặc cố vấn của một đánh giá viên khác có năng lực.

Kinh nghiệm trước đây trong các nhiệm vụ liên quan đến việc áp dụng TCVN 8709 (ISO/IEC 15408) và các tài liệu liên quan bao gồm nhưng không giới hạn ở việc thực hiện các công việc liên quan như: tư vấn, phát triển sản phẩm, nghiên cứu và trình bày chi tiết của các yêu cầu có thể góp phần vào các yếu tố kiến thức cần thiết đối với năng lực.

7 Trình độ đào tạo

Tất cả đánh giá viên phải trải qua các trình độ đào tạo, chẳng hạn như: Cao đẳng, Cử nhân hoặc cao hơn, có liên quan đến các yêu cầu được đề cập trong TCVN 8709 (ISO/IEC 15408) và các yêu cầu về phương pháp đánh giá trong TCVN 11386:2016 (ISO/IEC 18045:2008).

Tất cả những đánh giá viên, ở mức tối thiểu, họ phải chứng minh:

a) Hoàn thành tốt chương trình đào tạo đại học phù hợp với ít nhất 3 năm học trong các ngành bao gồm các chuyên ngành kỹ thuật cụ thể liên quan đến công nghệ thông tin (CNTT) hoặc an toàn thông tin;

b) Có kinh nghiệm cung cấp kiến thức, kỹ năng và hiệu quả tương đương với kiến thức, kỹ năng và hiệu quả đạt được khi học đại học trong các chuyên ngành liên quan đến CNTT hoặc an toàn thông tin.

Ví dụ: về các chuyên ngành kỹ thuật cụ thể bao gồm:

- Công nghệ kỹ thuật;
- Kỹ thuật điện;
- Kỹ sư cơ khí;
- Kỹ thuật vật liệu;
- Công nghệ thông tin máy tính;
- Kỹ thuật máy tính;
- Khoa học máy tính;
- Mạng máy tính;
- An ninh mạng;
- Vật lý học;
- Toán học;
- Hệ thống thông tin;
- Phát triển phần mềm và an toàn.

8 Tính hiệu quả

8.1 Yêu cầu chung

Đánh giá viên phải có khả năng áp dụng kiến thức và kỹ năng một cách hiệu quả, được đặc trưng bởi các thuộc tính như: năng khiếu, sáng kiến, nhiệt tình, sẵn sàng, kỹ năng giao tiếp, làm việc nhóm và lãnh đạo.

8.2 Hiệu quả của việc đánh giá

Điều khoản 5.2.1 liệt kê các nguyên tắc đánh giá bắt buộc phải tuân theo để đạt được một đánh giá hiệu quả.

8.3 Các trách nhiệm của chương trình đánh giá đối với tính hiệu quả của đánh giá viên

TCVN 11386:2016 (ISO/IEC 18045:2008), A.5, cung cấp hướng dẫn về các chương trình đánh giá và trách nhiệm dự kiến đánh giá viên.

Nhiều mục liên quan có liên quan trực tiếp hoặc gián tiếp đến hiệu quả của Đánh giá viên và cần được các cơ sở đánh giá xem xét khi xác định tính hiệu quả.

8.4 Hiệu quả trong việc thực hiện các đánh giá kịp thời

Tiêu chí đo lường hiệu quả của đánh giá viên được tìm thấy trong Phần 1 của bộ tiêu chuẩn này.

8.5 Hiệu quả trong việc thực hiện các đánh giá chính xác

Tất cả đánh giá viên phải (có thể) thực hiện các nhiệm vụ đánh giá được giao tuân theo các phương pháp và hoạt động đánh giá đã xác định yêu cầu về độ chính xác.

8.6 Tính hiệu quả trong báo cáo kết quả

Tất cả đánh giá viên phải có khả năng trình bày kết quả đánh giá sao cho cơ sở lý luận của các quyết định và các tài liệu tham chiếu liên quan có thể nhanh chóng giúp người đọc dễ dàng hiểu được.

Phụ lục A
(Tham khảo)
Loại công nghệ: Kiến thức và Kỹ năng

A.1 Kiến thức liên quan đến các loại công nghệ cụ thể

A.1.1 Yêu cầu chung

Sự phân loại của các loại công nghệ thay đổi tùy theo nhu cầu của các chủ thể phân loại chúng.

Các loại công nghệ được trình bày trong A.1 là các loại công nghệ được sử dụng thường xuyên, người đọc cần lưu ý để có thể xác định được các loại công nghệ khác.

Mức độ hiểu biết mà Đánh giá viên yêu cầu thay đổi tùy thuộc vào các yêu cầu an toàn mà Đánh giá viên đánh giá. Những Đánh giá viên tham gia vào các lớp đảm bảo ADV, ASE và APE, ATA, AVA và ACO cần có kiến thức chuyên sâu hơn so với những Đánh giá viên lớp ALC. Nói chung, những Đánh giá viên tham gia vào việc đánh giá các yêu cầu chức năng an toàn sẽ cần phải hiểu công nghệ được sử dụng.

Tuy nhiên, tùy thuộc vào các phương pháp đánh giá và các hoạt động được chỉ định, điều này có thể không cần thiết.

Các nhà đánh giá làm việc với các loại công nghệ cụ thể xác định những kiến thức sau là cần thiết:

a) Các PP liên quan đến loại công nghệ;

b) Các phương pháp đánh giá và các hoạt động liên quan đến loại công nghệ;

c) Tiêu chuẩn công nghệ liên quan đến loại công nghệ.

A.1.2 Các thiết bị và hệ thống kiểm soát ra vào

Các phương pháp kiểm soát truy cập.

A.1.3 Hệ thống và thiết bị sinh trắc học

a) Kỹ thuật thống kê;

b) Các phương thức sinh trắc học.

A.1.4 Bảo vệ dữ liệu

a) Cơ sở dữ liệu;

b) Kỹ thuật quét;

c) Phát hiện xâm nhập.

A.1.5 Cơ sở dữ liệu

a) Các khái niệm về kiến trúc hệ thống quản lý cơ sở dữ liệu;

b) Các phương pháp kiểm soát truy cập.

A.1.6 Các thiết bị và hệ thống phát hiện

a) Khái niệm về thiết bị phát hiện và kiến trúc hệ thống;

b) Các khái niệm về nhận dạng mẫu.

A.1.7 IC, thẻ thông minh và các thiết bị và hệ thống liên quan đến thẻ thông minh

a) Các khái niệm về cấu trúc thẻ thông minh;

b) Đầu đọc thẻ thông minh và trình điều khiển của chúng;

c) Bộ xử lý mật mã;

d) Lưu giữ khóa an toàn;

e) Giao diện có dây/không dây;

f) Bộ tạo bit ngẫu nhiên vật lý;

g) Các khái niệm về chống giả mạo, chống lại, phát hiện, bằng chứng, phản ứng;

h) Phân tích kênh kề.

A.1.8 Thiết bị phần cứng

a) An toàn vật lý;

b) Các khái niệm về chống giả mạo, chống lại, phát hiện, bằng chứng, phản ứng;

c) Phân tích kênh kề.

A.1.9 Hệ thống quản lý chính

a) Các phương pháp và kỹ thuật quản lý chính;

b) Sinh số ngẫu nhiên;

c) Các khái niệm về entropy;

d) Tạo khóa;

e) Thiết lập khóa;

f) Khóa đầu và đầu ra;

g) Lưu giữ khóa;

h) Đưa khóa về không;

i) Vận chuyển khóa.

A.1.10 Thiết bị và hệ thống di động

a) Các khái niệm về kiến trúc thiết bị di động;

b) Các khái niệm về quản lý thiết bị di động.

A.1.11 Thiết bị đa chức năng

Các khái niệm về kiến trúc thiết bị đa chức năng.

A.1.12 Mạng và các thiết bị và hệ thống liên quan đến mạng

a) Kiến trúc mạng và cấu trúc liên kết;

b) Các giao thức mạng thường được sử dụng.

A.1.13 Các hệ điều hành

a) Khởi động an toàn;

b) Vòng bảo vệ,

c) Quản lý bộ nhớ;

d) Nguyên tắc đặc quyền tối thiểu;

e) Các cơ chế kiểm soát truy cập;

f) Các nguyên tắc của ảo hóa;

g) Sự tách biệt;

h) Bộ tạo bit ngẫu nhiên tất định.

A.1.14 Các sản phẩm dành cho chữ ký điện tử

a) Công nghệ chữ ký số;

b) Cơ sở hạ tầng khóa công khai (PKI);

c) Cơ quan cấp chứng chỉ (CA);

d) Các thuật toán tạo khóa.

Ví dụ: RSA, DSA và ECDSA.

A.1.15 Máy tính tin cậy

a) Các khái niệm công nghệ máy tính khóa tin cậy.

1) Nền tảng mô-đun khóa tin cậy như: khóa xác nhận (EK) và lưu giữ khóa gốc (SRK);

2) Thanh ghi cấu hình nền tảng;

3) Đầu vào và đầu ra an toàn;

4) Tạo màn che bộ nhớ;

5) Bảo quản kín;

6) Chứng thực từ xa.

A.2 Các kỹ năng liên quan đến các loại công nghệ cụ thể

A.2.1 Yêu cầu chung

Khi xem xét các kỹ năng cần thiết cho các loại công nghệ nhất định, các kỹ năng cụ thể cần thiết hầu hết liên quan đến ATE (kiểm thử) cho loại công nghệ đó. Những kỹ năng này được xây dựng dựa trên những kỹ năng cơ bản được xác định trong tiêu chuẩn này.

Các kỹ năng sau được xác định là cần thiết bởi những Đánh giá viên làm việc với các loại công nghệ cụ thể:

a) Việc thực hiện các phương pháp đánh giá và các hoạt động liên quan đến loại công nghệ;

b) Có khả năng hiểu các tiêu chuẩn công nghệ liên quan.

A.2.2 Các thiết bị và hệ thống kiểm soát ra vào

a) Có thể cài đặt các thiết bị và hệ thống kiểm soát truy cập.

A.2.3 Hệ thống và thiết bị sinh trắc học

a) Sử dụng các kỹ thuật thống kê.

A.2.4 Bảo vệ dữ liệu

a) Có thể cài đặt các thiết bị và hệ thống kiểm soát truy cập.

A.2.5 Cơ sở dữ liệu

a) Có khả năng cấu hình chính xác các nền tảng của hệ thống quản lý cơ sở dữ liệu (DBMS);

b) Có thể sử dụng ngôn ngữ truy vấn có cấu trúc (SQL) hoặc các ngôn ngữ truy vấn cơ sở dữ liệu khác.

A.2.6 Các thiết bị và hệ thống phát hiện

a) Có thể cài đặt và cấu hình các thiết bị và hệ thống phát hiện.

A.2.7 IC, thẻ thông minh và các thiết bị và hệ thống liên quan đến thẻ thông minh

a) Có thể cài đặt đầu đọc thẻ thông minh và trình điều khiển của chúng trên các nền tảng kiểm thử;

b) Có khả năng chuẩn bị các mạch tích hợp để kiểm thử;

Ví dụ: Việc sử dụng các đầu dò.

c) Có khả năng cấu hình và sử dụng thiết bị điện tử kiểm thử;

Ví dụ: Máy hiện sóng, máy phân tích giao thức.

d) Có thể cấu hình và sử dụng trình giả lập và trình mô phỏng;

e) Sử dụng các kỹ thuật an toàn để kiểm thử xâm nhập vật lý;

f) Có thể bắt đầu và thực hiện các cuộc tấn công kênh kề.

A.2.8 Thiết bị phần cứng

a) Sử dụng các kỹ thuật an toàn để kiểm thử xâm nhập vật lý;

b) Có thể bắt đầu và thực hiện các cuộc tấn công kênh kề;

c) Có khả năng cấu hình và sử dụng thiết bị điện tử kiểm thử;

Ví dụ: Máy hiện sóng, máy phân tích giao thức.

d) Có thể cấu hình và sử dụng trình giả lập và trình mô phỏng.

A.2.9 Hệ thống quản lý khóa

Không có kỹ năng chuyên môn nào cho loại công nghệ này đã được xác định.

A.2.10 Thiết bị và hệ thống di động

Không có kỹ năng chuyên môn nào cho loại công nghệ này đã được xác định.

A.2.11 Thiết bị đa chức năng

Không có kỹ năng chuyên môn nào cho loại công nghệ này đã được xác định.

A.2.12 Mạng và các thiết bị và hệ thống liên quan đến mạng

A.2.13 Hệ điều hành

Có khả năng xác định giao diện chức năng an toàn TOE của hệ điều hành (TSFI).

A.2.14 Các sản phẩm dành cho chữ ký điện tử - Products for digital signatures

Không có kỹ năng chuyên môn nào cho loại công nghệ này đã được xác định.

A.2.15 Máy tính tin cậy

Không có kỹ năng chuyên môn nào cho loại công nghệ này đã được xác định.

Phụ lục B
(Tham khảo)
Ví dụ về kiến thức cần thiết để đánh giá các lớp đảm bảo yêu cầu an toàn

Phụ lục này bao gồm các ví dụ về kiến thức mà Đánh giá viên yêu cầu để đánh giá các lớp yêu cầu đảm bảo an toàn được đưa ra trong TCVN 8709-3:2011 (ISO/IEC 15408-3:2008).

Các ví dụ dựa trên phương pháp đánh giá được đưa ra trong TCVN 11386:2016 (ISO/IEC 18045:2008).

B.1 Kiến thức cần thiết cho các lớp đảm bảo cụ thể

B.1.1 Lớp ADV (Development)

Đánh giá viên thực hiện các hoạt động đánh giá liên quan đến lớp ADV phải có kiến thức được xác định trong Bảng B.1, đảm bảo cho đến và bao gồm mức độ chi tiết của các thành phần trong lĩnh vực được giao trách nhiệm đánh giá của họ.

Bảng B.1 - Kiến thức cần thiết cho Đánh giá viên lớp ADV

Thành phần đảm bảo	Yêu cầu kiến thức tối thiểu
ADV_ARC.1	a) Tính chất tự bảo vệ; b) Tính chất phân tách theo vùng; c) Tính chất không thể bỏ qua; d) Khái niệm kiến trúc an toàn và thiết kế.
ADV_FSP.1	a) Khái niệm về giao diện; b) Khái niệm về TSFI hỗ trợ SFR và thực thi SFR; c) Phương pháp mô tả các giao diện chương trình.
ADV_FSP.2	d) Kiến trúc an toàn; e) Thông báo lỗi;
ADV_FSP.3	f) Thông số;
ADV_FSP.4	Không có yêu cầu bổ sung.
ADV_FSP.5	g) Khuôn mẫu về mô hình chính sách an toàn; h) Dạng bán chính thức; i) Định dạng chuẩn hóa với cú pháp được xác định rõ ràng; j) Các phương pháp trình bày có cấu trúc (mã giả, lưu đồ, sơ đồ khối).
ADV_FSP.6	Không có yêu cầu bổ sung.
ADV_IMP.1	a) Kỹ thuật lấy mẫu; b) Ngôn ngữ mã nguồn hoặc mô tả sơ đồ phần cứng hoặc ngôn ngữ mã thiết kế phần cứng IC hoặc dữ liệu bố trí được sử dụng trong việc triển khai TOE; c) Kỹ thuật xáo trộn hoặc che giấu; d) Trình biên dịch.
ADV_IMP.2	e) Cung cấp hướng dẫn chương trình đánh giá; f) Các kỹ thuật tạo TSF từ một biểu thị triển khai (ví dụ: Trình biên dịch, thông dịch viên).
ADV_INT.1	a) Cấu trúc bên trong; b) Tính phức tạp.
ADV_INT.2	Không có yêu cầu bổ sung.
ADV_INT.3	Không có yêu cầu bổ sung.

ADV_SPM.1	a) Các mô hình chính sách an toàn chính thức bao gồm sự hiểu biết về các chính sách kiểm soát truy cập, kiểm thử, nhận dạng, xác thực, mã hóa và quản lý; b) Kiến trúc an toàn; c) Các phương pháp mẫu.
ADV_TDS.1	a) Mức độ phân rã; b) Các khái niệm và mô tả hệ thống con bao gồm phân loại, mục đích, hành vi, tương tác, giao diện; c) Các khái niệm và mô tả mô-đun bao gồm phân loại, mục đích, hành vi, tương tác, giao diện; d) Các khái niệm về thực thi SFR, hỗ trợ SFR và SFR không can thiệp.
ADV_TDS.2	Không có yêu cầu bổ sung.
ADV_TDS.3	Không có yêu cầu bổ sung.
ADV_TDS.4	Không có yêu cầu bổ sung.
ADV_TDS.5	e) Mô tả thiết kế bán chính thức;
ADV_TDS.6	f) Các bằng chứng tương ứng.

B.1.2 Lớp AGD (Guidance Documents)

Đánh giá viên thực hiện các hoạt động đánh giá liên quan đến lớp AGD phải có kiến thức được xác định trong Bảng B.2, đảm bảo cho đến và bao gồm mức độ chi tiết của các thành phần trong lĩnh vực được giao trách nhiệm đánh giá của họ.

Bảng B.2 - Kiến thức cần thiết cho Đánh giá viên lớp AGD

Thành phần đảm bảo	Yêu cầu kiến thức tối thiểu
AGD.OPE.1	a) Các khái niệm về vai trò của người dùng; b) Các khái niệm về nhóm; c) Các chức năng và đặc quyền người dùng có thể truy cập; d) Hoạt động an toàn; e) Môi trường hoạt động.
AGD_PRE.1	a) Thủ tục vận chuyển; b) Kỹ thuật lắp đặt an toàn; c) Cấu hình an toàn.

B.1.3 Lớp ALC (Life-Cycle Support)

Đánh giá viên thực hiện các hoạt động đánh giá liên quan đến lớp ALC phải có kiến thức được xác định trong Bảng B.3, đảm bảo cho đến và bao gồm mức độ chi tiết của các thành phần trong lĩnh vực được giao trách nhiệm đánh giá của họ.

Bảng B.3 - Kiến thức cần thiết cho Đánh giá viên lớp ALC

Thành phần đảm bảo	Yêu cầu kiến thức tối thiểu
ALC_CMC.1	a) Vòng đời của sản phẩm; b) Các khái niệm về quản lý cấu hình; c) Các khái niệm về phát triển an toàn; d) Các công cụ và kỹ thuật điển hình được sử dụng trong phát triển TOE; e) Quy trình vá lỗi và khắc phục sai sót; f) Các quá trình tích hợp và chấp nhận; g) Quá trình vận chuyển;

	h) Xây dựng quy trình (quy trình chuyển đổi một biểu diễn thực thi thành TOE); i) Các khái niệm về quản lý cấu hình; j) Các hệ thống quản lý cấu hình thường được sử dụng; k) Việc áp dụng quản lý cấu hình, đảm bảo rằng tính toàn vẹn của TOE được duy trì; l) Các biện pháp, thủ tục và tiêu chuẩn liên quan đến việc phân phối an toàn TOE, đảm bảo rằng biện pháp bảo vệ an toàn do TOE cung cấp không bị xâm phạm trong quá trình chuyển giao cho người dùng.
ALC_CMC.2	m) Hệ thống an toàn quản lý cấu hình (kiểm soát truy cập);
ALC_CMC.3	n) Các khái niệm về một kế hoạch hệ thống quản lý cấu hình;
ALC_CMC.4	o) Các thủ tục chấp nhận quản lý cấu hình;
ALC_CMC.5	Không có yêu cầu bổ sung.
ALC_CMS.1	a) Các khái niệm về quản lý cấu hình; b) Các hệ thống quản lý cấu hình thường được sử dụng.
ALC_CMS.2	Không có yêu cầu bổ sung.
ALC_CMS.3	Không có yêu cầu bổ sung.
ALC_CMS.4	Không có yêu cầu bổ sung.
ALC_CMS.5	Không có yêu cầu bổ sung.
ALC_DEL.1	Các biện pháp, thủ tục và tiêu chuẩn liên quan đến việc phân phối an toàn TOE, đảm bảo rằng biện pháp bảo vệ an toàn do TOE cung cấp không bị xâm phạm trong quá trình chuyển đến trang web của người dùng; b) Các kỹ thuật giả mạo bao gồm kiểm chứng giả mạo, chống lại, phát hiện và bằng chứng.
ALC_DVS.1	Các biện pháp an ninh, được sử dụng để bảo vệ môi trường phát triển bao gồm: 1) Kiểm soát an toàn; 2) An toàn vật lý; 3) An toàn nhân sự; 4) Biện pháp an toàn.
ALC_DVS.2	Không có yêu cầu bổ sung.
ALC_FLR.1	a) Phương pháp khắc phục sai sót; b) Báo cáo lỗi an toàn trong từng giai đoạn phát triển; c) Quy trình vá lỗi và khắc phục sai sót; d) Phân phối an toàn các bản vá lỗi và thay đổi.
ALC_FLR.2	e) Hành động khắc phục.
ALC_LCD.1	a) Các mô hình vòng đời phát triển Ví dụ: 1) Nhanh nhẹn; 2) Mô hình thác nước; 3) Tài liệu đầu vào và đầu ra của vòng đời.
ALC_LCD.2	Không có yêu cầu bổ sung
ALC_TAT.1	a) Các công cụ và kỹ thuật được sử dụng để phát triển sản phẩm, bao gồm:

	1) Các công cụ phát triển được xác định rõ ràng; Ví dụ: Ngôn ngữ lập trình hoặc hệ thống thiết kế hỗ trợ máy tính (CAD); 2) Các tiêu chuẩn thực hiện.
ALC_TAT.2	Không có yêu cầu bổ sung.
ALC_TAT.3	Không có yêu cầu bổ sung.

B.1.4 Lớp ASE & APE (ST and PP evaluation)

Đánh giá viên thực hiện các hoạt động đánh giá liên quan đến các lớp ASE và APE phải có kiến thức được xác định trong Bảng B.4, cho đến và bao gồm mức độ chi tiết của các thành phần đảm bảo trong lĩnh vực được giao trách nhiệm đánh giá của họ.

Bảng B.4 - Kiến thức cần thiết cho Đánh giá viên lớp ASE và APE

Thành phần đảm bảo		Yêu cầu kiến thức tối thiểu
ASE_CCL.1	APE_CCL.1	a) PP, ST, các gói yêu cầu an toàn; b) Công bố hợp quy.
ASE_ECD.1	APE_ECD.1	a) Có thể xem xét định nghĩa của một thành phần mở rộng cho mỗi yêu cầu an toàn mở rộng; b) Có thể xem xét chứng minh về sự phù hợp hoặc không phù hợp với các yếu tố này.
ASE_INT.1	APE_INT.1	Không có yêu cầu bổ sung.
ASE_OBJ.1	APE_OBJ.1	Môi trường hoạt động.
ASE_OBJ.2	APE_OBJ.2	Không có yêu cầu bổ sung.
ASE_REQ.1	APE_REQ.1	a) Chủ thể; b) Đối tượng; c) Hoạt động; d) Các thuộc tính an toàn; e) Các thực thể bên ngoài.
ASE_REQ.2	APE_REQ.2	Không có yêu cầu bổ sung.
ASE_SPD.1	APE_SPD.1	a) Định nghĩa vấn đề an toàn; b) Mục tiêu an toàn; c) Tài sản; d) Đe doạ; e) Tác nhân đe dọa.
ASE_TSS.1	-	Không có yêu cầu bổ sung.

B.1.5 Lớp ATE (Tests)

Đánh giá viên thực hiện các hoạt động đánh giá liên quan đến lớp ATE phải có kiến thức được xác định trong Bảng B.5, đảm bảo cho đến và bao gồm mức độ chi tiết của các thành phần trong lĩnh vực được giao trách nhiệm đánh giá của họ.

Bảng B.5 - Kiến thức cần thiết cho Đánh giá viên lớp ATE

Thành phần đảm bảo	Yêu cầu kiến thức tối thiểu
Tất cả các thành phần	a) Khái niệm về kế hoạch kiểm thử; 1) Các nguồn lực cần thiết để kiểm thử; 2) Các công cụ kiểm thử thường được sử dụng; 3) Điều kiện quyết định kiểm thử;

	4) Môi trường kiểm thử; 5) Các bước kiểm thử (kịch bản kiểm thử); 6) Kết quả mong muốn của lần kiểm thử; 7) Phương pháp ghi kết quả kiểm thử thực tế; 8) Kết quả kiểm thử. b) Các phương pháp kiểm thử thông thường (ví dụ: đặc điểm kỹ thuật chức năng, thiết kế chân kết nối, mô-đun, ...).
ATE_COV.1	Các khái niệm về phạm vi kiểm thử.
ATE_COV.2	Không có yêu cầu bổ sung.
ATE_COV.3	Không có yêu cầu bổ sung.
ATE_DPT.1	a) Các khái niệm về độ sâu của kiểm thử và liên kết với hệ thống con.
ATE_DPT.2	b) Các khái niệm về độ sâu của kiểm thử và liên kết với mô-đun.
ATE_DPT.3	Không có yêu cầu bổ sung.
ATE_DPT.4	Không có yêu cầu bổ sung.
ATE_FUN.1	a) Các khái niệm về kiểm thử chức năng;
ATE_FUN.2	Không có yêu cầu bổ sung.
ATE_IND.1	a) Loại giao diện (ví dụ: chương trình, dòng lệnh, giao thức); b) Phát triển các giả thuyết về sai sót; c) Kỹ thuật kiểm thử; d) Kỹ thuật kiểm thử hộp đen và hộp trắng.
ATE_IND.2	e) Kỹ thuật lấy mẫu; f) Phát triển các trường hợp kiểm thử độc lập.
ATE_IND.3	Không có yêu cầu bổ sung.

B.1.6 Lớp AVA (Vulnerability Assessment)

Đánh giá viên thực hiện các hoạt động đánh giá liên quan đến lớp AVA phải có kiến thức được xác định trong Bảng B.6, đảm bảo cho đến và bao gồm mức độ chi tiết của các thành phần trong lĩnh vực được giao trách nhiệm đánh giá của họ.

Bảng B.6 - Kiến thức cần thiết cho Đánh giá viên lớp AVA

Thành phần đảm bảo	Yêu cầu kiến thức tối thiểu
AVA_VAN.1	a) Phân loại lỗ hổng; b) Phân loại tấn công; c) Xác định các nguồn thông tin công khai về tình trạng dễ bị tổn thương; d) Kiểm thử xâm nhập.
AVA_VAN.2	Không có yêu cầu bổ sung.
AVA_VAN.3	e) Phát triển các giả định về sai sót;
AVA_VAN.4	f) Các phương pháp, công cụ và kỹ thuật cụ thể của chương trình đánh giá.
AVA_VAN.5	Không có yêu cầu bổ sung.

B.1.7 Lớp ACO (Composition)

Đánh giá viên thực hiện các hoạt động đánh giá liên quan đến lớp ACO phải có kiến thức được xác định trong Bảng B.7, đảm bảo cho đến và bao gồm mức độ chi tiết của các thành phần trong lĩnh vực được giao trách nhiệm đánh giá của họ.

Bảng B.7 - Kiến thức cần thiết cho Đánh giá viên lớp ACO

Thành phần đảm bảo	Yêu cầu kiến thức tối thiểu
Tất cả các thành phần ACO	a) Nguyên tắc cấu thành; b) Kiểu bố cục: 1) Phân lớp; 2) Mạng lưới; 3) Thành phần. c) Nguyên tắc tích hợp hệ thống; d) Nguyên tắc dựa vào.
ACO_COR.1	Không có yêu cầu bổ sung.
ACO_DEV.1	Kiến thức cần thiết cho lớp ADV;
ACO_DEV.2	Không có yêu cầu bổ sung.
ACO_DEV.3	Không có yêu cầu bổ sung.
ACO_REL.1	a) Các thành phần tương tác; b) Khái niệm về sự phụ thuộc; c) Các kỹ thuật bảo vệ giả mạo bao gồm: chống giả mạo, tính kháng, phát hiện và bằng chứng; d) Kỹ thuật chống nhiễu.
ACO_REL.2	Không có yêu cầu bổ sung.
ACO_CTT.1	a) Kiến thức cần thiết cho lớp ATE; b) Tổng hợp kiểm thử TOE;
ACO_CTT.2	Không có yêu cầu bổ sung.
ACO_VUL.1	a) Kiến thức cần thiết cho lớp AVA; b) Kiến thức về các lỗ hổng áp dụng cho sáng tác; c) Luồng thông tin.
ACO_VUL.2	Không có yêu cầu bổ sung.
ACO_VUL.3	Không có yêu cầu bổ sung.

Phụ lục C

(Tham khảo)

Ví dụ về yêu cầu kiến thức cần thiết để đánh giá các lớp chức năng an toàn

C.1 Yêu cầu chung

Phụ lục này bao gồm các ví dụ về yêu cầu kiến thức mà Đánh giá viên yêu cầu để đánh giá các lớp chức năng an toàn được nêu trong TCVN 8709-2:2011 (ISO/IEC 15408-2:2008).

C.2 Kiến thức cần thiết cho các lớp yêu cầu chức năng an toàn cụ thể

C.2.1 Lớp FAU (Security Audit)

a) Kiểm thử khởi tạo dữ liệu;

b) Danh tính người dùng;

c) Dấu thời gian;

d) Kiểm thử các kỹ thuật lưu giữ dữ liệu;

e) Kiểm thử phân tích dữ liệu;

f) Các cuộc tấn công có thể được xác định thông qua đánh giá dữ liệu;

g) Các kỹ thuật để bảo vệ dữ liệu kiểm toán.

C.2.2 Lớp FCO (Communication)

a) Bằng chứng nguồn gốc;

b) Phủ nhận nguồn gốc;

c) Phủ nhận việc tiếp nhận.

C.2.3 Lớp FCS (Cryptographic Support)

a) Các khái niệm về entropy (không thể đoán trước);

b) Các khái niệm về tính ngẫu nhiên (phân phối ngẫu nhiên);

c) Tạo bit ngẫu nhiên;

d) Mật mã;

e) Các thuật toán mật mã;

Ví dụ: AES, ECC, RSA.

f) Các giao thức mật mã;

Ví dụ: TLS, IPsec, SSH.

g) Tạo khóa mật mã, phân phối khóa, quản lý khóa và hủy khóa;

h) Hoạt động mật mã.

C.2.4 Lớp FDP (User Data Protection)

a) Kỹ thuật kiểm soát truy cập;

Ví dụ: Kiểm soát truy cập được gắn nhãn, kiểm soát truy cập dựa trên vai trò.

b) Kiểm soát luồng thông tin;

c) Chuyển giao TOE nội bộ;

d) Các kỹ thuật bảo vệ thông tin còn sót;

e) Phục hồi;

f) Tính toàn vẹn của dữ liệu được lưu giữ;

g) Giám sát tính toàn vẹn;

h) Kỹ thuật lưu giữ, nhập và xuất ngoại tuyến;

i) Các kỹ thuật xác thực dữ liệu.

C.2.5 Lớp FIA (Identification and Authentication)

a) Kiểm soát truy cập dựa trên thuộc tính an toàn;

b) Chủ thể, đối tượng và hoạt động;

c) Xác thực dữ liệu;

d) Quản lý các lỗi xác thực;
e) Các khái niệm về các thuộc tính của người dùng;
f) Ràng buộc chủ thể người dùng;
g) Tên người dùng/mật khẩu;
h) Cơ sở dữ liệu xác thực;
Ví dụ: Kerberos, LDAP, Radius.
i) Mã xác thực thông báo;
j) Xác thực dựa trên chứng chỉ;
k) Các kỹ thuật nhận dạng và xác thực dựa trên sinh trắc học;
l) Bí mật (ví dụ: mật khẩu và cụm mật khẩu, khóa);
m) Quản lý các cơ chế và quy tắc xác thực.

C.2.6 Lớp FMT (Security Management)

a) Quản lý dữ liệu TSF;
b) Quản lý các thuộc tính an toàn;
c) Quản lý các chức năng TSF;
d) Thu hồi;
e) Các vai trò quản lý an toàn.

C.2.7 Lớp FPR (Privacy)

a) Khái niệm ẩn danh;
b) Khái niệm về bút danh;
c) Kác khái niệm về tính không liên kết;
d) Các khái niệm về khả năng không quan sát được.

C.2.8 Lớp FPT (Protection of the TSF)

a) Kiến thức cần thiết cho lớp FCS nêu trong C.2.3;
b) Kiến thức cần thiết cho lớp FDP cho trong C.2.4;
c) Các kỹ thuật giả mạo vật lý bao gồm: chống giả mạo, tính kháng, phát hiện và bằng chứng;
d) Các kỹ thuật khôi phục đáng tin cậy;
e) Các cuộc tấn công phát lại;
f) Kỹ thuật đóng dấu thời gian;
g) Các khái niệm về tự kiểm tra;
h) Trạng thái đồng bộ;
i) Bảo vệ dữ liệu;
j) Khái niệm về nguyên tắc không an toàn.

C.2.9 Lớp FRU (Resource Utilisation)

a) Kỹ thuật chịu lỗi;
b) Mức độ ưu tiên của các kỹ thuật dịch vụ;
c) Kỹ thuật phân bổ nguồn lực;
d) Các cuộc tấn công từ chối dịch vụ.

C.2.10 Lớp FTA (TOE Access)

a) Các khái niệm về phiên: phiên đồng thời;
b) Thiết lập phiên họp;
c) Khóa phiên và kết thúc;
d) Lịch sử truy cập.

C.2.11 Lớp FTP (Trusted Path/Channels)

a) Khái niệm về một đường dẫn tin cậy;
b) Khái niệm về một kênh tin cậy;

c) Kiến thức cần thiết cho lớp FCS nêu trong **C.2.3**;

d) Khái niệm về một bên thứ ba tin cậy (TTP).

Tài liệu tham khảo

Các mục liên quan đến các kỹ thuật an toàn CNTT chung:

[1] TCVN 12210:2018, Công nghệ thông tin - Các kỹ thuật an toàn - Đánh giá an toàn hệ thống vận hành (ISO/IEC 19791, Information technology - IT Security techniques - Security assessment of operational systems.)

[2] ISO/IEC 29193, Information technology - IT Security techniques - Secure system engineering principles and techniques.

[3] ISO/IEC/TS 30104, Information Technology - Security Techniques - Physical Security Attacks, Mitigation Techniques and Security Requirements.

[4] Anderson R.J. Security Engineering: A Guide to Building Dependable Distributed Systems: [ONLINE]: Wiley: Available at http://www.cl.cam.ac.uk/~rja14/book.html.

Các mục liên quan đến chủ đề năng lực của Đánh giá viên

[5] TCVN ISO/IEC TS 17027:2015 Đánh giá sự phù hợp - Từ vựng về năng lực cá nhân sử dụng trong chứng nhận năng lực cá nhân.

Các mục liên quan đến các lớp yêu cầu đảm bảo an ninh

Các mục liên quan đến lớp đảm bảo ADV

[6] ISO/IEC/TS 19249, Information technology - Security techniques - Catalogue of architectural and design principles for secure products, systems and applications.

Các mục liên quan đến lớp đảm bảo AGD

[7] ISO/IEC/IEEE 26513, Systems and software engineering - Requirements for testers and reviewers of information for users.

Các mục liên quan đến lớp đảm bảo ALC

[8] TCVN 10539:2014 (ISO/IEC/IEEE 12207:2008), Kỹ thuật hệ thống và phần mềm - Các quá trình vòng đời phần mềm.

[9] TCVN 10607 (ISO/IEC 15026), Kỹ thuật phần mềm và hệ thống – Đảm bảo phần mềm và hệ thống.

[10] TCVN ISO/IEC 27001:2019 (ISO/IEC 27001:2013), Công nghệ thông tin - Các kỹ thuật an toàn - Hệ thống quản lý an toàn thông tin - Các yêu cầu.

[11] TCVN ISO/IEC 27002:2011 (ISO/IEC 27002:2005), Công nghệ thông tin - Các kỹ thuật an toàn - Quy tắc thực hành quản lý an toàn thông tin.

[12] ISO/IEC 15446, Information technology - IT Security techniques - Guidance for the production of Protection Profiles and Security Targets.

[13] ISO/IEC/TR 18018, Information technology - Systems and software engineering - Guide for configuration management tool capabilities.

[14] ISO/IEC 27034 (all parts), Information technology - Application security Items relating to the ASE and APE assurance classes.

Các mục liên quan đến lớp đảm bảo ATE

[15] TCVN 12849 (ISO/IEC/IEEE 29119), Kỹ thuật hệ thống và phần mềm - Kiểm thử phần mềm.

[16] ISO/IEC 29128, Information technology - Security techniques - Verification of cryptographic protocols.

[17] Patton Ron Software Testing: Sams Publishing.

Các mục liên quan đến lớp đảm bảo AVA

[18] ISO/IEC/TR 20004, Information technology - Security techniques - Refining software vulnerability analysis under TCVN 8709: 2011 (ISO/IEC 15408) and TCVN 11386:2016 (ISO/IEC 18045:2008).

[19] MITRE. Common Attack Pattern and Enumeration: Mechanisms of Attack. [ONLINE]: Available at http://capec.mitre.org/data/definitions/1000.html

Các mục liên quan đến lớp đảm bảo ACO

[20] ISO/IEC/TS 24748-6, Systems and software engineering - Life cycle management - Part 6: System integration engineering.

[21] Karger P.A., & Kurth H. Increased Information Flow Needs for High-Assurance Composite Evaluations. in Second IEEE International Information Assurance Workshop. 8-9 April 2004, Charlotte, NC: IEEE Computer Society. p. 129-140.

Các mục liên quan đến các lớp yêu cầu chức năng an toàn

Các hạng mục liên quan đến Lớp FAU (Kiểm thử an toàn)

[22] TCVN 7818 (ISO/IEC 18014), Công nghệ thông tin - Kỹ thuật an toàn - Dịch vụ tem thời gian.

Các mục liên quan đến Lớp FCS (Hỗ trợ mật mã)

[23] TCVN 7817-2:2010 (ISO/IEC 11770-2:2008), Công nghệ thông tin - Kỹ thuật an toàn - Quản lý khóa.
[24] TCVN 11367:2016 (ISO/IEC 18033:2010), Công nghệ thông tin - Các kỹ thuật an toàn - Thuật toán mật mã.
[25] ISO/IEC 18032, Information technology - Security techniques - Prime number generation.
[26] ISO/IEC 19592, Information technology - Security techniques - Secret sharing.
[27] TCVN 12197:2018 (ISO/IEC 19772:2009), Công nghệ thông tin - Các kỹ thuật an toàn - Mã hóa có sử dụng xác thực.
[28] TCVN 13461:2022 (ISO/IEC 20008:2013), Công nghệ thông tin – Các kỹ thuật an toàn – Chữ ký số ẩn danh.
[29] Schneier Bruce Applied Cryptography. Wiley.
[30] Schneier Bruce Practical Cryptography. Wiley.
[31] Ristic Ivan Bulletproof SSL and TLS. Feisty Duck.

Các mục liên quan đến Lớp FPR (Quyền riêng tư)

[32] ISO/IEC PDTS 19608, Information technology - Security techniques - Guidance for developing security and privacy functional requirements based on ISO/IEC 15408.
[33] ISO/IEC 29101, Information technology - Security techniques - Privacy framework Items related to specific technology area Access control devices and systems.
[34] Ferraiolo David F. Kuhn, D. Richard and Chandramouli, Ramaswamy: Role Based Access Control. Artech House Inc.
[35] EUROPEAN COMMISSION INFORMATION. Document ID - System Security Policy C (2006) 3602: Standard on Access Control and Authentication: Available at https://www.eba.europa.eu/documents/10180/1449046/Annex+7+Standard+on+Access+Control+and+Authentication.pdf/cba4e74d-f54d-4797-9204-6dae43560e65.
[36] Hu, Vincent C.; Ferraiolo, David F. and Kuhn, D. Rick: NIST IR 7316: Assessment of Access Control Systems: Available at https://csrc.nist.gov/publications/nistir/7316/NISTIR-7316.pdf

Hệ thống và thiết bị sinh trắc học

[37] TCVN 11385:2016 (ISO/IEC 19792:2009), Công nghệ thông tin - Các kỹ thuật an toàn - Đánh giá an toàn sinh trắc học.
[38] ISO/IEC 19795 (all parts), Information technology - Biometric performance testing and reporting.
[39] ISO/IEC 24745, Information technology - Security techniques - Biometric information protection.
[40] ISO/IEC 29164, Information technology - Biometrics - Embedded BioAPI.
[41] Phillips P.J., Martin A, Wilson C.L., Przybocki M. An introduction to evaluating biometric systems. Computer, Vol 33: Issue 2, Feb 2000. IEEE.
[42] Wayman James, Jain Anil, Maltoni Davide, Maio Dario (Editors). Biometric Systems: Technology, Design and Performance evaluation: Springer Verlag Databases.
[43] Elmars Ramez, & Navathe Shamkant B. Fundamentals of Database Systems: Pearson ICs, smart cards and smart card-related devices and systems.
[44] ISO/IEC 24727 (all parts), Identification cards - Integrated circuit card programming interfaces.
[45] Senior Officials Group Information Systems Security (SOGIS). Supporting documents for smart card evaluations: Available at http://www.sogis.eu/uk/supporting_doc_en.html.
[46] Rankl Wolfgang, & Effing Wolfgang Smart Card Handbook: Wiley Hardware devices.

[47] ISO/IEC/TS 30104, Information Technology - Security Techniques - Physical Security Attacks, Mitigation Techniques and Security Requirements Key management systems.
[48] NIST SP 800-130: A Framework for Designing Cryptographic Key Management Systems. Available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-130.pdf.

Hệ thống và thiết bị di động

[49] ISO/IEC/TR 30125, Information technology - Biometrics used with mobile devices.
[50] Fernandez-Saavedra B., Sanchez-Reillo R., Sanchez-Redondo C., Blanco-Gonzalo R.
[51] Testing of biometric systems integrated in mobile devices. International Carnahan Conference on Security Technology (ICCST), 2015. IEEE.

Thiết bị đa chức năng

[52] TCVN 9801:2013 (ISO/IEC 27033:2009), Công nghệ thông tin - Kỹ thuật an toàn - An ninh mạng.
[53] IEEE Standard 2600-2008, Hardcopy Device and System Security Network and network-related devices and systems.
[54] Stallings William Cryptography and Network Security: Principles and Practice: Pearson.
[55] Tanenbaum Andrew, & Wetheral David J. Computer Networks: Pearson Operating systems.
[56] Tanenbaum Andrew S, & Woodhull Albert S. Operating Systems: Design and Implementation. Pierson/Prentice Hall.

Sản phẩm dành cho chữ ký điện tử

[57] TCVN 12214:2018 (ISO/IEC 14888:2008), Công nghệ thông tin - Các kỹ thuật an toàn - Chữ ký số kèm phụ lục.
[58] TCVN 13460:2022 (ISO/IEC 18370:2016), Công nghệ thông tin – Các kỹ thuật an toàn – Chữ ký số mù.

Máy tính tin cậy

[59] ISO/IEC 11889 (all parts), Information technology - Trusted platform module library.
[60] Challenger David A Practical Guide to Trusted Computing (For TPM 1.2). IBM Press.
[61] Challenger David, & Arthur Will A Practical Guide to TPM 2.0. Apress Open.
[62] Various resources from Trusted Computing Group available at https://www.trustedcomputinggroup.org/resource-directory/.

Các mục liên quan đến các chủ đề cụ thể theo lĩnh vực

[63] ISO/TR 11568 (all parts), Financial services - Key management (retail).
[64] ISO/IEC 14441, Health informatics - Security and privacy requirements of EHR systems for use in conformity assessment.
[65] ISO/TR 14742, Financial services - Recommendations on cryptographic algorithms and their use.
[66] ISO 15764, Road vehicles - Extended data link security.
[67] ISO/TS 17574, Electronic fee collection - Guidelines for security protection profiles.