TCVN **TIÊU CHUẨN QUỐC GIA**

TCVN 13723-1:2023
ISO/IEC 19896-1:2018

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 1: GIỚI THIỆU,KHÁI NIỆM VÀ YÊU CẦU CHUNG

IT security techniques — Competence requirements for information security testers and evaluators — Part 1: Introduction, concepts and general requirements

HÀ NỘI – 2023

Mục lục

Lời nói đầu

TCVN 13723-1:2023 hoàn toàn tương đương với ISO/IEC 19896-1:2018.

TCVN 13723-1:2023 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

Mục tiêu của bộ tiêu chuẩn này là cung cấp các khái niệm cơ bản liên quan đến các chủ đề về năng lực của các cá nhân chịu trách nhiệm thực hiện đánh giá sản phẩm an toàn thông tin mạng và kiểm thử sự phù hợp. Bộ tiêu chuẩn này cung cấp khuôn khổ và các yêu cầu chuyên môn xác định năng lực tối thiểu của các cá nhân thực hiện đánh giá sản phẩm an toàn thông tin mạng và kiểm thử sự phù hợp bằng cách sử dụng các tiêu chuẩn đã được thiết lập.

Để đạt được mục tiêu này, bộ tiêu chuẩn này bao gồm các nội dung sau:

a) Các thuật ngữ và định nghĩa liên quan đến chủ đề năng lực trong đánh giá và kiểm thử sản phẩm an toàn thông tin mạng;

b) Các khái niệm cơ bản liên quan đến năng lực trong đánh giá sản phẩm an toàn thông tin mạng và kiểm thử sự phù hợp;

c) Yêu cầu năng lực tối thiểu đối với đánh giá viên và kiểm thử viên thực hiện kiểm thử/đánh giá sản phẩm an toàn thông tin mạng.

Bộ tiêu chuẩn này liên quan đến:

a) Chuyên gia đánh giá an toàn thông tin và kiểm thử sự phù hợp;

b) Cơ quan có thẩm quyền phê duyệt đánh giá an toàn thông tin và kiểm thử sự phù hợp;

c) Phòng thử nghiệm đánh giá và kiểm thử sự phù hợp an toàn thông tin.

d) Các nhà cung cấp hoặc nhà cung cấp công nghệ có sản phẩm an toàn thông tin mạng có thể là đối tượng của các cuộc đánh giá đảm bảo an toàn thông tin hoặc kiểm thử sự phù hợp;

e) Các tổ chức cấp chứng nhận hoặc thừa nhận.

Bộ tiêu chuẩn này được chia thành ba phần, nội dung các phần đề cập đến năng lực của kiểm thử viên và đánh giá viên được trình bày ở phần sau.

Trong tiêu chuẩn này, phần giới thiệu và các khái niệm, cung cấp một cái nhìn tổng quan về các định nghĩa, khái niệm cơ bản và mô tả chung được sử dụng để truyền đạt các yêu cầu năng lực về chuyên môn cho một số lĩnh vực. Tiêu chuẩn này nhằm cung cấp kiến thức cơ bản cần thiết để sử dụng làm khuôn mẫu được trình bày trong các phần khác của bộ tiêu chuẩn này một cách thích hợp.

Phần 2 của bộ tiêu chuẩn này mô tả yêu cầu về năng lực tối thiểu theo từng mức năng lực đối với Kiểm thử viên sự phù hợp áp dụng TCVN 11295:2016 (ISO 19790:2012) và các tiêu chuẩn liên quan.

Phần 3 của bộ tiêu chuẩn này mô tả yêu cầu năng lực tối thiểu theo từng mức năng lực đối với đánh giá viên bảo mật thông tin áp dụng TCVN 8709 (ISO/IEC 15408) và các tiêu chuẩn liên quan.

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.

IT security techniques - Competence requirements for information security testers and evaluators - Part 1: Introduction, concepts and general requirements

1 Phạm vi áp dụng

Tiêu chuẩn này xác định các thuật ngữ và thiết lập có tổ chức tập hợp các khái niệm cùng mối quan hệ để hiểu các yêu cầu năng lực đối với các kiểm thử viên và đánh giá viên sự phù hợp, đảm bảo an toàn thông tin. Từ đó, là cơ sở để hiểu được về các khái niệm và nguyên tắc trọng tâm của bộ tiêu chuẩn này thống qua cộng đồng người dùng. Phần này cung cấp thông tin cơ bản cho người sử dụng bộ tiêu chuẩn này.

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 ISO/IEC 17000:2007 (ISO/IEC 17000:2004), Đánh giá sự phù hợp - Từ vựng và các nguyên tắc chung.
- TCVN ISO/IEC 17025:2017 (ISO/IEC 17025:2017), Yêu cầu chung về năng lực của phòng thử nghiệm và hiệu chuẩn.

3 Thuật ngữ và định nghĩa

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

3.1

Năng lực (competence)

Khả năng áp dụng kiến thức, sự hiểu biết và kỹ năng để đạt được kết quả như dự định.

[Nguồn: 3.6, TCVN ISO/IEC 17024:2012 (ISO/IEC 17024:2012)]

3.2

Kiểm thử viên sự phù hợp (conformance-tester)

Kiểm thử viên (tester)

Cá nhân được giao thực hiện các hoạt động kiểm thử theo một tiêu chuẩn kiểm thử sự phù hợp nhất định và phương pháp kiểm thử liên quan.

CHÚ THÍCH 1: Ví dụ một tiêu chuẩn như vậy là TCVN 11295:2016 (ISO 19790:2012) và phương pháp kiểm thử được quy định trong TCVN 12211:2018 (ISO/IEC 24759:2017).

3.3

Đào tạo (education)

Quá trình tiếp nhận hoặc đưa ra hướng dẫn có hệ thống, điển hình là ở trường học hoặc trường đại học.

3.4

Tính hiệu quả (effectiveness)

Khả năng áp dụng kiến thức và kỹ năng một cách hiệu quả, được đặc trưng bởi các thuộc tính của hành vi như năng khiếu, sáng kiến, sự nhiệt tình, sự chủ động, kỹ năng giao tiếp, làm việc nhóm và lãnh đạo.

3.5

Đánh giá viên (evaluator)

Cá nhân được giao thực hiện đánh giá theo một tiêu chuẩn đánh giá nhất định và phương pháp đánh giá liên quan.

CHÚ THÍCH 1: Ví dụ về một tiêu chuẩn đánh giá là TCVN 8709 (ISO/IEC 15408) với phương pháp đánh giá liên quan được đưa ra trong TCVN 11386:2016 (ISO/IEC 18045:2008).

3.6

Kinh nghiệm (experience)

Sự tham gia ở mức thực tế với các dự án liên quan đến lĩnh vực năng lực.

3.7

Kiến thức, sự hiểu biết (knowledge)

Cơ sở lập luận, trao đổi thông tin, sự chính xác, các nguyên tắc hoặc kiến thức, sự hiểu biết có được thông qua kinh nghiệm hoặc qua đào tạo.

CHÚ THÍCH 1: Ví dụ về kiến thức là khả năng mô tả các phần khác nhau của tiêu chuẩn đảm bảo thông tin.

[NGUỒN: 2.56, TCVN ISO/IEC TS 17027:2015 (ISO/IEC TS 17027:2014)]

3.8

Phòng thử nghiệm (laboratory)

Tổ chức có hệ thống quản lý cung cấp công việc đánh giá hoặc kiểm thử phù hợp với một bộ chính sách, thủ tục xác định và sử dụng một phương pháp luận đã xác định để kiểm thử hoặc đánh giá chức năng của các sản phẩm an toàn thông tin mạng.

CHÚ THÍCH 1: Các tổ chức này thường được đặt các tên thay thế bởi các cơ quan phê duyệt khác nhau. Ví dụ, Cơ sở đánh giá An ninh CNTT (ITSEF), Phòng thử nghiệm kiểm tra Tiêu chí chung (CCTL), Cơ sở đánh giá Thương mại (CLEF).

3.9

Kỹ năng (skill)

Khả năng thực hiện một nhiệm vụ hoặc hoạt động với một kết quả dự định cụ thể có được thông qua giáo dục, đào tạo, kinh nghiệm hoặc các phương tiện khác

CHÚ THÍCH 1: Ví dụ về kỹ năng là khả năng xác định và phân loại rủi ro liên quan đến một dự án.

[NGUỒN: 2.74, TCVN ISO/IEC TS 17027:2015 (ISO/IEC TS 17027:2014)]

4 Các khái niệm

Để hỗ trợ sự phù hợp trong việc đánh giá hoặc kiểm thử sự phù hợp của các sản phẩm an toàn thông tin mạng, có xem xét đến yếu tố năng lực của các cá nhân thực hiện công việc đánh giá hoặc kiểm thử sự phù hợp. Bất kể việc cung cấp các phương pháp đánh giá hoặc kiểm thử sự phù hợp đã được tiêu chuẩn hóa, năng lực tối thiểu trong việc thực hiện các hoạt động này là cần thiết để hỗ trợ việc đạt được sự phù hợp và tính lặp lại của các kết quả thử nghiệm. Điều này sẽ hỗ trợ trong việc thừa nhận lẫn nhau giữa các chứng nhận và phê duyệt sản phẩm an toàn thông tin mạng.

TCVN ISO/IEC 17025:2017 đề cập đến các yêu cầu chung về năng lực của các phòng thử nghiệm và hiệu chuẩn và thường được quy định làm cơ sở cho sự phù hợp giữa các phòng thử nghiệm và đánh giá sự phù hợp về đảm bảo an toàn.

TCVN ISO/IEC 17025:2017 xác định một số yêu cầu liên quan đến năng lực mà phòng thử nghiệm cần phải đáp ứng. Bao gồm:

- Đảm bảo năng lực của tất cả nhân sự có thể ảnh hưởng đến hoạt động của phòng thử nghiệm;

- Xác định và lập thành văn bản các yêu cầu về năng lực đối với từng chức năng liên quan đến các hoạt động của phòng thử nghiệm;

- Đảm bảo nhân sự phòng thử nghiệm có đủ năng lực để thực hiện các hoạt động mà họ chịu trách nhiệm và hiểu được tầm quan trọng cũng như ứng phó, khắc phục với các sai lệch liên quan đến các hoạt động của phòng thử nghiệm;

- Lập thành văn bản các quy trình để giám sát liên tục các nhân sự tham gia vào các hoạt động của phòng thử nghiệm;

- Duy trì hồ sơ về năng lực như: giáo dục, đào tạo, kiến thức kỹ thuật, kỹ năng, kinh nghiệm, ủy quyền và giám sát tất cả nhân sự tham gia vào các hoạt động của phòng thử nghiệm.

CHÚ THÍCH: TCVN ISO/IEC 17025:2017 được đưa ra nhằm mục đích bao phủ một loạt các phòng thử nghiệm hiệu chuẩn và không chỉ được sử dụng trong lĩnh vực thử nghiệm và đánh giá sản phẩm an toàn thông tin mạng.

5 Các yếu tố của năng lực

5.1 Năng lực

Để thành thạo trong cung cấp các kết quả kiểm thử, đánh giá sự phù hợp sao cho nhất quán và hỗ trợ mục tiêu về sự phù hợp trong các kết quả do từng nhân sự thực hiện và phòng thử nghiệm khác nhau cung cấp. Kiểm thử viên và đánh giá viên sự phù hợp cần phải đạt được những kiến thức, kỹ năng, kinh nghiệm và trình độ tối thiểu cần có, nhằm đảm bảo mục tiêu sản phẩm an toàn thông tin mạng phù hợp với tiêu chuẩn và để có thể thực hiện các nhiệm vụ của mình một cách hiệu quả.

Điều khoản này xác định các yếu tố năng lực tối thiểu cần có trong áp dụng bộ tiêu chuẩn này trong khi xem xét các yêu cầu về năng lực đối với kiểm thử viên hoặc đánh giá viên sự phù hợp sản phẩm an toàn thông tin mạng đối với các tiêu chuẩn cụ thể.

Đào tạo có thể được dùng để nâng cao một số yếu tố của năng lực ở các cá nhân. Ví dụ, đào tạo thường được thực hiện để có được hoặc nâng cao các kỹ năng hiện có, nâng cao kiến thức hoặc để tăng tính hiệu quả.

Các yếu tố bổ sung của năng lực như: năng khiếu, sự nhiệt tình, sáng kiến, khả năng lãnh đạo, tinh thần đồng đội và tính sẵn sàng có thể được các phòng thử nghiệm hoặc tổ chức công nhận quy định. Chúng cũng có thể được định nghĩa trong các phần khác của bộ tiêu chuẩn này.

5.2 Kiến thức

Kiểm thử viên và đánh giá viên có kiến thức là một trong những yếu tố của năng lực. Các mô tả sau đây là cơ sở để cung cấp một bộ kiến thức thích hợp và phần kiến thức có thể kiểm chứng đến các tiêu chuẩn có liên quan liên quan đến sản phẩm đó:

a) Hiểu biết về sản phẩm an toàn thông tin mạng phù hợp với tiêu chuẩn có liên quan;

b) Bất kỳ phương pháp kiểm thử hoặc đánh giá nào có liên quan;

c) Các chính sách và thủ tục của cơ quan có thẩm quyền phê duyệt, tổ chức công nhận và phòng thử nghiệm có liên quan;

d) Hiểu biết về cấu trúc và thiết kế sản phẩm an toàn thông tin mạng trong các lĩnh vực công nghệ có liên quan.

Khi xem xét các sản phẩm an toàn thông tin mạng, nhiều loại công nghệ có thể phù hợp với phạm vi công việc của phòng thử nghiệm và hiểu biết về các công nghệ này cần được xem xét khi xác định các mức năng lực tối thiểu. Đối với một lĩnh vực công nghệ cụ thể, sau đây là các lớp kiến thức quan trọng có liên quan:

a) Công nghệ được sử dụng trong thiết kế, phát triển và triển khai sản phẩm được kiểm thử;

b) Cách thức sử dụng hoặc dự định sử dụng sản phẩm;

c) Các lỗ hổng và điểm yếu điển hình có thể xảy ra trong công nghệ đó;

d) Lĩnh vực mà các sản phẩm được sử dụng hoặc dự định sử dụng.

Ví dụ về các lĩnh vực công nghệ bao gồm: mật mã, sinh trắc học, mạch tích hợp, hệ điều hành, thiết bị mạng, cơ sở dữ liệu, thẻ thông minh và hệ thống nhúng. Các lĩnh vực công nghệ đôi khi được xác định bởi cơ quan có thẩm quyền phê duyệt, trong số những lĩnh vực khác.

5.3 Kỹ năng

Các kỹ năng thường được yêu cầu đối với Kiểm thử viên và đánh giá các sản phẩm an toàn thông tin theo các mức năng lực được xác định trong điều khoản 6 bao gồm:

a) Hiểu biết về phạm vi và cơ sở của việc đánh giá hoặc một dự án kiểm thử sự phù hợp;

b) Hiểu về các ranh giới của việc thực hiện đang được kiểm thử hoặc mục tiêu đánh giá;

c) Có thể lựa chọn hoặc điều chỉnh phương pháp đánh giá hoặc kiểm thử thích hợp;

d) Thực hiện phân tích tài liệu;

e) Hiểu mã nguồn, sơ đồ và các thành phần cơ sở được sử dụng để xác định và triển khai sản phẩm;

f) Phát triển và thực hiện kiểm thử chức năng và phi chức năng;

g) Xác định xem các điều kiện kiểm thử có nằm trong các thông số đã nêu để cho phép kiểm thử lặp lại hay không;

h) Hiệu chuẩn và sử dụng các công cụ kiểm thử;

i) Sử dụng phương pháp lưu trữ thích hợp, bao gồm tính toàn vẹn, tính sẵn có và tính bảo mật phù hợp với bằng chứng kiểm thử, kết quả kiểm thử và hồ sơ kiểm thử (bao gồm các diễn giải và báo cáo kiểm thử);

j) Giải thích kết quả kiểm thử;

k) Có khả năng viết các báo cáo một cách dễ hiểu về chi tiết các kết quả trong công việc;

l) Có thể lặp lại quá trình kiểm thử hoặc quá trình kiểm thử đã lưu trữ và thu được kết quả tương tự;

m) Có thể xây dựng một môi trường kiểm thử để đạt được điều kiện hoạt động thích hợp cho các sản phẩm an toàn.

Ở các mức năng lực cao, các kỹ năng như khả năng giao tiếp hiệu quả và thực hiện quản lý dự án có thể ở dạng kỳ vọng.

Ở mức năng lực 1 và 2, các kỹ năng này có thể được thực hiện dưới sự giám sát.

5.4 Kinh nghiệm

Cá nhân có được kinh nghiệm thông qua thực hiện đánh giá hoặc kiểm thử sự phù hợp và có thể đã qua đào tạo hoặc cố vấn cho những người khác trong nhiều dự án đánh giá hoặc kiểm thử sự phù hợp. Các cá nhân có kinh nghiệm có hiểu biết sâu về các yêu cầu đối với các dự án đánh giá hoặc kiểm thử sự phù hợp, cũng như bất kỳ diễn giải và chính sách nào của tổ chức công nhận, cơ quan có thẩm quyền phê duyệt và phòng thử nghiệm.

5.5 Trình độ đào tạo

Các bằng cấp giáo dục cụ thể như bằng Cao đẳng, bằng Cử nhân hoặc bằng cấp cao hơn có thể giúp xác định khả năng của một cá nhân đã theo một chương trình đào tạo chính thức hoặc làm việc độc lập. Một số chương trình giáo dục đại học và bồi dưỡng có liên quan đến đánh giá và kiểm thử sự phù hợp có thể mang lại cho một cá nhân cơ hội đạt được kiến thức phù hợp với tư cách là một chuyên gia đảm bảo an toàn thông tin.

Trong một số trường hợp, có thể chấp nhận các kinh nghiệm sẵn có thay cho trình độ học vấn hoặc bằng cấp một cách thích hợp.

5.6 Tính hiệu quả

Tính hiệu quả với tư cách là kiểm thử viên hoặc đánh giá viên khác nhau tùy thuộc vào mục tiêu và tổ chức của phòng thử nghiệm cũng như của cơ quan có thẩm quyền phê duyệt. Đặc biệt, tính hiệu quả cần xem xét tính chính xác của các kết quả kiểm thử hoặc đánh giá thu được, khả năng lặp lại các phương pháp và hoạt động đánh giá hoặc kiểm thử được thực hiện bởi những kiểm thử viên và đánh giá viên khác có năng lực, thu được kết quả tương tự. Khả năng truyền đạt kết quả kiểm thử và đánh giá trong cùng một nội dung mà người nhận kết quả dự kiến dễ dàng hiểu được.

6 Các mức năng lực

6.1 Tổng quan

Đánh giá viên và kiểm thử viên có thể được phân định một mức năng lực cho từng lĩnh vực cụ thể được nêu trong các điều khoản khác của bộ tiêu chuẩn này. Chúng được mô tả trong các điều khoản từ 6.2 đến 6.5.

Các mức năng lực tổng thể có thể được sử dụng để hỗ trợ các phân định khác nhau về năng lực chuyên môn như:

a) Kỹ thuật viên;

b) Đánh giá viên/Kiểm thử viên;

c) Đánh giá viên cấp cao/Kiểm thử viên cấp cao;

d) Chuyên gia đánh giá trưởng/Kiểm thử viên trưởng.

6.2 Mức 1 (Hỗ trợ)

– Cung cấp hỗ trợ cho một số hoạt động theo yêu cầu của các phương pháp đánh giá hoặc kiểm thử sự phù hợp;

– Có khả năng thực hiện công việc kiểm thử hoặc đánh giá dưới sự giám sát.

là hợp pháp.

7.5 Tính hiệu quả

Các tiêu chí đánh giá tính hiệu quả của đánh giá viên và kiểm thử viên phải do phòng thử nghiệm thiết lập. Các tiêu chí liên quan bao gồm:

– Thời gian cần thiết để lập kế hoạch kiểm thử hoặc đánh giá;

– Thời gian cần thiết để thực hiện một kế hoạch kiểm thử hoặc đánh giá và hoàn thành nó;

– Số lượng, loại và mức độ nghiêm trọng của các ý kiến nhận được trong các hoạt động đánh giá nội bộ;

– Số lượng, loại và mức độ nghiêm trọng của các nhận xét nhận được trong giai đoạn phê duyệt;

– Có khả năng lặp lại các bước trong quá trình kiểm thử từ những tài liệu do kiểm thử viên hoặc đánh giá viên khác có năng lực ghi lại;

– Khả năng hiểu công nghệ mới và sử dụng các công cụ;

– Có thể giải thích các lỗi và trạng thái kiểm thử cho các nhà cung cấp, người phê duyệt và các thành viên khác trong nhóm;

– Độ chính xác của kết quả đánh giá hoặc kiểm thử;

– Sử dụng ngôn ngữ trực tiếp và tập trung trong các báo cáo kiểm thử (hoặc "khả năng sử dụng các loại ngôn ngữ trong báo cáo kiểm thử).

7.6 Lưu giữ hồ sơ năng lực

TCVN ISO/IEC 17025:2017 yêu cầu phòng thử nghiệm lưu giữ hồ sơ năng lực. Phụ lục A và B cung cấp các biểu mẫu để ghi lại các thông tin này.

6.3 Mức 2 (Chuyên nghiệp)

– Có khả năng làm việc không cần đến giám sát trong nhiều lĩnh vực thử nghiệm hoặc đánh giá, tuy nhiên vẫn có thể cần phải giám sát trong một số lĩnh vực;

– Có khả năng hiểu được tầm quan trọng và ứng phó với những sai lệch liên quan đến các hoạt động của phòng thử nghiệm.

6.4 Mức 3 (Quản lý)

– Có khả năng làm việc mà không có giám sát trong hầu hết các phạm vi kiểm thử, đánh giá;

– Có khả năng hiểu được tầm quan trọng và ứng phó với những sai lệch được tìm thấy liên quan đến các hoạt động của phòng thử nghiệm;

– Có khả năng giám sát công việc kiểm thử hoặc đánh giá những người ở mức 1 và 2.

6.5 Mức 4 (Lãnh đạo)

– Có năng lực kiểm tra tất cả các khía cạnh của cuộc kiểm thử hoặc đánh giá theo các tiêu chuẩn và phương pháp đã xác định đối với ít nhất một lĩnh vực công nghệ;

– Có năng lực trong việc giao tiếp với các bên liên quan bao gồm cơ quan phê duyệt và nhà cung cấp và có thể thực thi công tác quản lý dự án cho một dự án đánh giá hoặc kiểm thử sự phù hợp;

– Có khả năng làm việc không giám sát trong tất cả các phương pháp kiểm thử/đánh giá được chỉ định cho dự án;

– Có khả năng hiểu được tầm quan trọng và ứng phó với những sai lệch được tìm thấy liên quan đến các hoạt động của phòng thử nghiệm;

– Có khả năng giám sát và cung cấp hướng dẫn liên quan đến công việc kiểm thử hoặc đánh giá của những người tại mức 1, 2 và 3.

7 Đánh giá các yếu tố của năng lực

7.1 Kiến thức

Lượng kiến thức cung cấp được đề cập trong phạm vi của bộ tiêu chuẩn này là có thể đo lường được. Những đánh giá về kiến thức có thể bao gồm: trình độ chuyên môn đạt được thông qua bên thứ ba hoặc thông phát triển kiểm thử và được thực hiện bởi tổ chức công nhận hoặc do chính phòng thử nghiệm thực hiện.

7.2 Kỹ năng

Các kỹ năng khác nhau được yêu cầu đối với kiểm thử viên và đánh giá viên các sản phẩm an toàn thông tin mạng được trình bày trong các phần tiếp theo của bộ tiêu chuẩn này. Tuy nhiên những kỹ năng này nên được đánh giá.

Các ví dụ về các phương pháp đánh giá kỹ năng bao gồm:

– Các mặt thành thạo trong chương trình kiểm thử của phòng thử nghiệm được thực hiện như một phần của các yêu cầu về sự phù hợp với tiêu chuẩn TCVN ISO/IEC 17025:2017;

– Trong các chi tiết về đánh giá hiệu quả đào tạo, sử dụng đến các hồ sơ đào tạo được lưu trữ phù hợp với tiêu chuẩn TCVN ISO/IEC 17025:2017, có thể chứng minh sự thành thạo của một kỹ năng;

– Chứng chỉ chuyên môn liên quan đến các kỹ năng cụ thể;

– Phản hồi/đánh giá từ những nhân sự khác đã có năng lực về cùng một kỹ năng.

7.3 Kinh nghiệm

Kinh nghiệm cần được đánh giá thông qua việc theo dõi hồ sơ về số lượng dự án đã hoàn thành và mô tả của từng dự án, bao gồm cả phạm vi kỹ thuật, mức độ phức tạp của dự án, các công nghệ và phương pháp kiểm thử được sử dụng trong các dự án.

CHÚ THÍCH: Bản thân số năm kinh nghiệm dành cho các vai trò liên quan không phải là một thước đánh giá thích hợp vì kinh nghiệm phản ánh khối lượng và sự đa dạng của các dự án đã được thực hiện trong thời gian tối thiểu bằng với thời gian của dự án.

7.4 Trình độ đào tạo

Trình độ đào tạo và bằng cấp của một nhân sự thường được chứng minh bằng việc sở hữu các chứng chỉ có tính xác thực, được cấp bởi các tổ chức đã được cơ quan có thẩm quyền công nhận

Phụ lục A

(Tham khảo)

Khung mô tả các yêu cầu về năng lực

Các Bảng A.1 đến A.4 mô tả một bộ khung mà các phòng thử nghiệm có thể sử dụng để xác định các yêu cầu năng lực cụ thể bằng cách sử dụng các tiêu chí về kiến thức, kỹ năng, kinh nghiệm và giáo dục, cho từng mức năng lực. Thông tin trong bảng là các yêu cầu tối thiểu được xác định trong điều khoản 7.

Phần 2 và Phần 3 của bộ tiêu chuẩn này cung cấp các tiêu chí năng lực cụ thể cho kiểm thử viên TCVN 11295:2016 (ISO 19790:2012) và đánh giá viên TCVN 8709 (ISO/IEC 15408) có thể được sử dụng để hoàn thành các bảng.

Bảng A.1 - Hồ sơ yêu cầu về năng lực đối với Mức 1

Mức 1 (Hỗ trợ)	
Tên lĩnh vực kiến thức	**Mô tả lĩnh vực kiến thức**
Tên kỹ năng	**Mô tả về kỹ năng**
Yêu cầu về kinh nghiệm	
Yêu cầu về đào tạo	
Tiêu chí về tính hiệu quả	

Bảng A.2 - Hồ sơ yêu cầu về năng lực đối với Mức 2

Mức 2 (Chuyên nghiệp)	
Tên lĩnh vực kiến thức	**Mô tả lĩnh vực kiến thức**
Tên kỹ năng	**Mô tả về kỹ năng**
Yêu cầu về kinh nghiệm	
Yêu cầu về đào tạo	
Tiêu chí về tính hiệu quả	

Bảng A.3 - Hồ sơ yêu cầu về năng lực đối với Mức 3 (Quản lý)

Mức 3 (Quản lý)	
Tên lĩnh vực kiến thức	**Mô tả lĩnh vực kiến thức**
Tên kỹ năng	**Mô tả về kỹ năng**
Yêu cầu về kinh nghiệm	
Yêu cầu về đào tạo	
Tiêu chí về tính hiệu quả	

Bảng A.4 - Hồ sơ yêu cầu về năng lực đối với Mức 4 (Lãnh đạo)

Mức 4 (Lãnh đạo)	
Tên lĩnh vực kiến thức	**Mô tả lĩnh vực kiến thức**
Tên kỹ năng	**Mô tả về kỹ năng**
Yêu cầu về kinh nghiệm	
Yêu cầu về đào tạo	
Tiêu chí về tính hiệu quả	

Phụ lục B

(Tham khảo)

Mẫu hồ sơ về kinh nghiệm và năng lực

Bảng B.1 là một ví dụ về bộ khung để ghi lại kinh nghiệm mà Đánh giá viên theo TCVN 8709 (ISO/IEC 15408) hoặc Kiểm thử viên theo TCVN 11295:2016 (ISO 19790:2012) đạt được.

Trong các phần tiếp theo của tiêu chuẩn TCVN 13723 (ISO/IEC 19896) có thể sẽ đưa ra các ví dụ cụ thể hơn về hồ sơ.

Các phòng thử nghiệm nên có phương pháp để chỉ ra mức độ phức tạp của dự án dựa trên danh mục dự án.

VÍ DỤ: "đơn giản" và "phức tạp", mức đảm bảo đánh giá cho các đánh giá được thực hiện theo TCVN 11386:2016 (ISO/IEC 18045:2008) hoặc mức an toàn của mô-đun mật mã được kiểm thử bằng TCVN 12211:2018 (ISO/IEC 24759:2017).

Bảng B.1 – Ví dụ về hồ sơ kinh nghiệm

Hồ sơ kinh nghiệm					
Tên của đánh giá viên/ kiểm thử viên					
ID dự án	Thời gian của dự án	Lĩnh vực kỹ thuật	Độ phức tạp dự án	Số giờ làm việc của dự án	Các phương pháp kiểm thử/đánh giá được thực hiện

Bảng B.2 là một ví dụ về bộ khung để ghi lại năng lực đạt được bởi đánh giá viên TCVN 8709 (ISO/IEC 15408) hoặc kiểm thử viên TCVN 11295:2016 (ISO 19790:2012).

Trong các phần tiếp theo của bộ tiêu chuẩn này, có thể sẽ đưa ra các ví dụ khác về hồ sơ.

Bảng B.2 – Ví dụ về hồ sơ năng lực

Hồ sơ năng lực					
Tên của đánh giá viên/kiểm thử viên					
ID dự án	Kinh nghiệm	Kiến thức	Các kỹ năng	Tính hiệu quả	Mức năng lực

Tài liệu tham khảo

[1] TCVN 8709 (ISO/IEC 15408), Công nghệ thông tin - Các kỹ thuật an toàn - Các tiêu chí đánh giá an toàn công nghệ thông tin.
[2] TCVN 11778 (ISO/IEC TR 15443), Công nghệ thông tin - Các kỹ thuật an toàn - Khung cho đảm bảo an toàn công nghệ thông tin.
[3] TCVN ISO/IEC 17024:2012 (ISO/IEC 17024:2012), Đánh giá sự phù hợp - Yêu cầu chung đối với tổ chức chứng nhận năng lực cá nhân.
[4] TCVN ISO/IEC TS 17027:2015 (ISO/IEC TS 17027:2014), Đánh giá sự phù hợp - Từ vựng về năng lực cá nhân sử dụng trong chứng nhận năng lực cá nhân.
[5] TCVN IEC/ISO 17065:2013 (IEC/ISO 17065:2012), Đánh giá sự phù hợp - Yêu cầu đối với Tổ chức chứng nhận sản phẩm, quá trình và dịch vụ.
[6] TCVN 11386:2016 (ISO/IEC 18045:2008), Công nghệ thông tin - Các kỹ thuật an toàn - Phương pháp đánh giá an toàn công nghệ thông tin.
[7] TCVN 11295:2016 (ISO 19790:2012), Công nghệ thông tin - Các kỹ thuật an toàn - Yêu cầu an toàn cho mô-đun mật mã
[8] TCVN 12211:2018 (ISO/IEC 24759:2017), Công nghệ thông tin - Các kỹ thuật an toàn - Yêu cầu kiểm thử cho mô-đun mật mã.