TCVN **T I Ê U C H U Ẩ N Q U Ố C G I A**

TCVN ISO/PAS 17002 : 2009

Xuất bản lần 1

ĐÁNH GIÁ SỰ PHÙ HỢP – TÍNH BẢO MẬT – NGUYÊN TẮC VÀ YÊU CẦU

Conformity assessment – Confidentiality – Principles and requirements

HÀ NỘI - 2009

Mục lục

Lời nói đầu

TCVN ISO/PAS 17002 : 2009 hoàn toàn tương đương với ISO/PAS 17002 : 2004;

TCVN ISO/PAS 17002 : 2009 do Ban kỹ thuật tiêu chuẩn quốc gia TCVN/TC 176 Quản lý chất lượng và đảm bảo chất lượng biên soạn, Tổng cục Tiêu chuẩn Đo lường Chất lượng đề nghị, Bộ Khoa học và Công nghệ công bố.

Lời giới thiệu

Tiêu chuẩn này được biên soạn dựa trên cơ sở chấp nhận Qui định phổ biến rộng rãi (Publicly Available Specification – PAS) của Tổ chức Tiêu chuẩn hóa quốc tế (ISO).

Tiêu chuẩn này đề cập đến "tính bảo mật", yếu tố được nhắc đến trong nhiều hướng dẫn của ISO/IEC và các tiêu chuẩn quốc tế về đánh giá sự phù hợp.

Tiêu chuẩn này bao gồm các nguyên tắc thống nhất về bản chất của yếu tố "tính bảo mật" đồng thời cũng đưa ra các điều khoản yêu cầu dự kiến sẽ đưa vào các tiêu chuẩn quốc tế của ISO/IEC về đánh giá sự phù hợp.

Điều 4 (Các nguyên tắc) nêu các nội dung nhằm định hướng cho các nhóm biên soạn trong việc đưa ra các yêu cầu liên quan đến tính bảo mật trong các tài liệu về đánh giá sự phù hợp.

Các yêu cầu sẽ được đưa vào các tài liệu chính thức của nhóm biên soạn tài liệu về đánh giá sự phù hợp bao gồm yếu tố chung của "tính bảo mật" nêu trong điều 5. Các yêu cầu này được trình bày theo một cấu trúc chung thống nhất và được phân nhóm theo một hay nhiều tiêu đề dưới đây:

a) Yêu cầu chung;

b) Yêu cầu về cơ cấu;

c) Yêu cầu về nguồn lực;

d) Yêu cầu về quá trình;

e) Yêu cầu về hệ thống quản lý.

Theo đó, mỗi yếu tố chung sẽ gồm các yêu cầu liên quan đến yếu tố đó được phân nhóm theo một hay nhiều tiêu đề được nêu ở trên.

Xuất bản lần 1

Đánh giá sự phù hợp – Tính bảo mật – Nguyên tắc và yêu cầu

Conformity assessment – Confidentiality – Principles and requirements

1 Phạm vi áp dụng

Tiêu chuẩn này nêu các nguyên tắc và yêu cầu đối với yếu tố bảo mật vì yếu tố này có liên quan đến hoạt động đánh giá sự phù hợp.

Tiêu chuẩn này là công cụ sử dụng trong quá trình xây dựng các tiêu chuẩn đề cập đến yếu tố bảo mật.

Tiêu chuẩn này không phải là tài liệu quy định để sử dụng độc lập trực tiếp trong hoạt động đánh giá sự phù hợp.

2 Tài liệu viện dẫn

Tài liệu viện dẫn dưới đây rất cần thiết cho việc áp dụng tiêu chuẩn. Đối với các tài liệu có ghi năm công bố thì áp dụng bản được nêu. Đối với các tài liệu không ghi năm công bố thì áp dụng phiên bản mới nhất, bao gồm cả các sửa đổi.

TCVN ISO 17000, Đánh giá sự phù hợp – Từ vựng và nguyên tắc chung

3 Thuật ngữ và định nghĩa

Tiêu chuẩn này áp dụng các thuật ngữ và định nghĩa trong TCVN ISO 17000.

CHÚ THÍCH: Thuật ngữ "tổ chức" được sử dụng trong tiêu chuẩn này có nghĩa là tổ chức công nhận hoặc tổ chức đánh giá sự phù hợp như định nghĩa trong TCVN ISO 17000.

4 Nguyên tắc bảo mật

4.1 Nhằm đạt được sự tiếp cận các thông tin cần thiết để tiến hành có hiệu lực các hoạt động đánh

giá sự phù hợp, tổ chức cần đảm bảo rằng thông tin bí mật sẽ không bị tiết lộ.

4.2 Tất cả các tổ chức và cá nhân được đánh giá có quyền được bảo vệ các thông tin mà họ cung cấp.

4.3 Quản lý sự cân bằng giữa các yêu cầu liên quan đến việc bảo mật và công khai thông tin ảnh hưởng đến lòng tin của các bên liên quan và nhận thức của họ về giá trị của hoạt động đánh giá sự phù hợp được thực hiện.

5 Yêu cầu đối với tính bảo mật

5.1 Khái quát

Do mức độ đa dạng cần xem xét, các yêu cầu trong điều này được chia thành ba mức đặc trưng như dưới đây.

a) Bắt buộc:

Các yêu cầu được soạn thảo cụ thể để sử dụng phải đề cập đến yếu tố này, không được thay đổi trừ trường hợp được thay thế bằng điều khoản cụ thể hơn. Ví dụ như cụm từ: “Hoạt động đánh giá sự phù hợp phải được thực hiện một cách công bằng”, có thể được thay thế cụ thể hơn bằng “Hoạt động chứng nhận hệ thống quản lý phải được thực hiện một cách công bằng”. Không nên sử dụng các yêu cầu này khi đề cập đến yếu tố chung liên quan.

b) Khuyến nghị:

Các yêu cầu được soạn thảo để sử dụng khi muốn có mức độ quy định kỹ thuật chi tiết. Được phép thay đổi các yêu cầu loại này.

c) Gợi ý:

Các xem xét có thể tính đến trong quá trình soạn thảo các yêu cầu.

Thông qua việc cung cấp các mức đặc trưng khác nhau, tiêu chuẩn đưa ra sự trình bày thống nhất về các yếu tố chung cho tất cả các hoạt động đánh giá sự phù hợp, đồng thời duy trì được tính linh hoạt trong cách thức diễn đạt cụ thể.

5.2 Yêu cầu chung

Các yêu cầu dưới đây là bắt buộc.

a) Tổ chức phải có trách nhiệm, thông qua các cam kết thi hành về mặt pháp lý, đối với việc quản lý tất cả các thông tin thu được hoặc tạo lập được trong quá trình thực hiện các hoạt động đánh giá sự phù hợp. Tổ chức phải thông báo trước cho khách hàng các thông tin dự kiến đưa ra công khai. Ngoại trừ các thông tin mà khách hàng đã công bố, hoặc khi có thỏa thuận giữa tổ chức và khách hàng (ví dụ vì mục đích phúc đáp các khiếu nại), tất cả các thông tin khác được coi là thông tin độc

quyền và phải được coi là mật.

b) Trường hợp tổ chức được luật pháp hoặc người được ủy quyền theo thỏa thuận hợp đồng yêu cầu công khai thông tin mật, nếu pháp luật không cấm thì khách hàng hoặc cá nhân có liên quan phải được thông báo về thông tin cung cấp.

c) Thông tin về khách hàng thu được từ các nguồn không phải từ khách hàng đó (ví dụ người khiếu nại, nhà chức trách) phải được coi là thông tin mật.

5.3 Yêu cầu về nguồn lực

5.3.1 Yêu cầu bắt buộc

Nhân sự, bao gồm các thành viên của ủy ban, người đấu thầu, nhân sự của tổ chức bên ngoài, hoặc các cá nhân bất kỳ đại diện cho tổ chức đánh giá, phải giữ bí mật tất cả các thông tin thu được hoặc tạo lập được trong quá trình thực hiện các hoạt động đánh giá sự phù hợp của tổ chức, ngoại trừ khi luật pháp yêu cầu.

5.3.2 Yêu cầu khuyến nghị

Tổ chức phải có sẵn và sử dụng các phương tiện để xử lý an toàn (ví dụ: bưu chính, thư điện tử, hủy hồ sơ) các thông tin mật (ví dụ: tài liệu, hồ sơ) và các đối tượng của hoạt động đánh giá sự phù hợp (ví dụ: mẫu sản phẩm).

Thư mục tài liệu tham khảo

[1] CAN/CSA-Q830-03, Model code for the protection of personal information (Qui phạm mẫu đối với việc bảo vệ thông tin cá nhân)