Công nhận năng lực các tổ chức chứng nhận hệ thống quản lý an toàn thông tin: GÓP PHẦN TẠO MÔI TRƯỜNG SỐ AN TOÀN

Hồ Minh Trang
Văn phòng Công nhận Chất lượng, Bộ Khoa học và Công nghệ

Hiện nay, việc công nhận năng lực các tổ chức chứng nhận hệ thống quản lý an toàn thông tin theo tiêu chuẩn quốc tế được đánh giá là một trong những yếu tố quan trọng đảm bảo an toàn thông tin cho các tổ chức/doanh nghiệp, góp phần tạo nên môi trường số an toàn. Sự công nhận này còn giúp tăng tính minh bạch, tin cậy và uy tín của các tổ chức/doanh nghiệp trong mắt khách hàng và đối tác.

Vai trò của an toàn thông tin và sự cần thiết của ISO 27001

An toàn thông tin được hiểu là bảo vệ thông tin, tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, bảo mật và khả dụng của thông tin. Bên cạnh đó, an toàn thông tin còn là việc bảo đảm thông tin trên mạng không gây phương hại đến an ninh quốc gia, trật tự an toàn xã hội, bí mật nhà nước, quyền và lợi ích hợp pháp của tổ chức, cá nhân. Trong thời đại công nghệ thông tin phát triển mạnh mẽ như hiện nay, thông tin là tài sản quý giá không thể thiếu của bất kỳ tổ chức nào. Việc xây dựng một hệ thống an toàn thông tin là điều cần thiết để bảo đảm an ninh thông tin và ngăn chặn các cuộc tấn công từ bên ngoài hay bên trong tổ chức.

Việt Nam đang chuyển mình theo lộ trình chính phủ số, xã hội số và kinh tế số. An toàn an ninh mạng được coi là một trong những vấn đề ưu tiên hàng đầu để tạo nền tảng vững chắc cho công cuộc chuyển đổi số quốc gia. Việc chuyển đổi số mở ra nhiều cơ hội cho Việt Nam, bao gồm tiếp cận chính sách nhà nước và tương tác với các cơ quan quản lý thông qua các nền tảng công nghệ, giúp tiết kiệm được thời gian và chi phí. Trong bối cảnh đó, rất nhiều tổ chức phụ thuộc một phần hoặc toàn phần vào hệ thống mạng, máy tính và cơ sở dữ liệu. Để đảm bảo an ninh thông tin cho các tổ chức này, việc áp dụng ISO 27001 - hệ thống quản lý an ninh thông tin là rất cần thiết và hữu ích.

Có chứng chỉ ISO 27001 đồng nghĩa với việc doanh nghiệp có khả năng vận hành và kiểm soát tốt hơn hệ thống quản lý an toàn thông tin của mình.

Bộ tiêu chuẩn ISO 27001 ra đời từ năm 1992, do Phòng Thương mại và Công nghiệp Anh ban hành. Ban đầu đó là bộ quy phạm thực hành về hệ thống an toàn thông tin dựa trên các hệ thống đảm bảo an toàn thông tin nội bộ của các công ty dầu khí. Sau đó, năm 1995, Viện Tiêu chuẩn hoá Anh đã ban hành tài liệu này với mã hiệu BS 7799-1. Đến năm 2000, Tổ chức Tiêu chuẩn hoá Quốc tế (ISO) đã chính thức chấp nhận và ban hành tiêu chuẩn này dưới mã hiệu ISO/IEC 17799:2000 - tiền thân của bộ tiêu chuẩn ISO 27001 ngày nay.

Việc triển khai và áp dụng tiêu chuẩn ISO 27001 mang ý nghĩa quan trọng trong việc hỗ trợ các tổ chức/doanh nghiệp xây dựng hệ thống quản lý an toàn thông tin, đảm bảo tính toàn vẹn, bảo mật và sẵn sàng cho các dữ liệu và thông tin quan trọng. Với việc sử dụng rộng rãi trên toàn cầu, tiêu chuẩn này không chỉ giúp tăng cường khả năng phát hiện sớm các vấn đề liên

quan đến an ninh thông tin và niềm tin của khách hàng, đối tác kinh doanh, mà còn đáp ứng các yêu cầu pháp lý và chuẩn mực trong việc bảo vệ an toàn thông tin.

Việc sử dụng các quy trình chuẩn hóa theo ISO 27001 giúp đảm bảo thông tin và dữ liệu được lưu thông, cập nhật liên tục, mà không ảnh hưởng tiêu cực đến hoạt động kinh doanh của doanh nghiệp. Cụ thể ISO 27001 mang lại những lợi ích sau: i) Đảm bảo thông tin chính xác và kịp thời, giúp các tổ chức/doanh nghiệp quản lý thông tin hiệu quả hơn; ii) Giảm chi phí hoạt động, tránh các hoạt động trùng lặp và giảm dữ liệu đầu vào; iii) Quản lý và định vị rủi ro liên quan đến thông tin, tăng tính bảo mật, tính toàn vẹn và sẵn dùng của thông tin; iv) Mở rộng phạm vi áp dụng tiêu chuẩn cho tất cả các tổ chức/doanh nghiệp, giúp tăng khả năng trúng thầu và cơ hội ký kết hợp đồng; v) Tăng khả năng tin tưởng của khách hàng đối với tổ chức/doanh nghiệp; vi) Giảm thiểu tổn thất về thời gian và tiền bạc khi phát sinh sự cố hoặc rủi ro liên quan đến thông tin; vii) Liên tục cải tiến và cập nhật để phù hợp với sự thay đổi của môi trường kinh doanh.

Hoạt động chứng nhận ISO 27001 tại Việt Nam

Kể từ khi ban hành ISO 27001 đến nay, việc áp dụng tiêu chuẩn này đã phổ biến ở hầu hết các quốc gia trên thế giới, đặc biệt là trong lĩnh vực tài chính và ngân hàng. Tại Việt Nam, một số công ty lớn đã có chứng nhận ISO 27001 như CSC Việt Nam, FPT-IS, FPT Soft, GHP FarEast, ISB Corporation Vietnam... Hầu hết các doanh nghiệp này đều có vốn đầu tư hoặc có đối tác nước ngoài. Các doanh nghiệp thực hiện và áp dụng tiêu chuẩn này chủ yếu do yêu cầu từ các công ty góp vốn hoặc khách hàng nước ngoài… những nơi đang áp dụng ISO 27001.

Phòng Nghiệp vụ chứng nhận (VICAS) tham gia khóa đào tạo trực tuyến ISO/IEC 27001 do Cơ quan Công nhận Hàn Quốc (KAB) tổ chức.

Kết quả thống kê tại Việt Nam cho thấy, nhìn chung việc áp dụng ISO 27001 của các tổ chức/doanh nghiệp vẫn còn hạn chế. Một trong những nguyên nhân của tình trạng này là chi phí để được cấp chứng nhận ISO 27001 khá cao, bao gồm các chi phí: tư vấn, xây dựng hệ thống, đánh giá và đặc biệt là chi phí về việc thực hiện các biện pháp kiểm soát rủi ro. Việc áp dụng ISO 27001 thường tốn kém gấp 2-3 lần so với việc áp dụng ISO 9001. Thêm vào đó, trình độ về công nghệ thông tin và nhận thức về an ninh thông tin của người lao động chưa cao cũng là một trở ngại lớn khi triển khai ISO 27001. Tuy nhiên, các doanh nghiệp có nguồn lực tài chính hạn chế vẫn có thể triển khai ISO 27001 từng bước, với lộ trình hợp lý. Ngoài ra, để giảm chi phí, các doanh nghiệp có thể tự triển khai áp dụng ISO 27001 mà không yêu cầu đánh giá cấp chứng nhận.

Hiện nay, trong số các tổ chức chứng nhận ISO 27001 tại Việt Nam, chỉ có SGS và BVC Việt Nam được công nhận bởi UKAS, Quacert được công nhận bởi JAS-ANZ và TUV NORD được công nhận bởi Dakks. Các tổ chức chứng nhận còn lại khác vẫn chưa được công nhận. Qua khảo sát của Văn phòng Công nhận Chất lượng (BoA), tất cả các tổ chức chứng nhận trong nước đều mong muốn được công nhận đủ điều kiện/năng lực cấp chứng nhận ISO 27001. Hơn nữa các tổ chức chứng nhận trong nước cũng có lợi thế về sự thấu hiểu sâu sắc tình hình thực tế và thực trạng chứng nhận, nên việc đánh giá sẽ sâu sát và thực chất hơn. Bên cạnh đó, bản thân các doanh nghiệp trong nước có nhu cầu được cấp chứng nhận ISO 27001 cũng mong muốn được làm việc với các tổ chức cấp chứng nhận trong nước, vì như vậy giúp họ tiết kiệm được thời gian và chi phí.

Tại Việt Nam hiện có 3 tổ chức cung cấp dịch vụ công nhận, nhưng chỉ có BoA cung cấp dịch vụ công nhận cho các tổ chức chứng nhận và là thành viên Thỏa ước Công nhận lẫn nhau (MLA) duy nhất của Diễn đàn Công nhận Quốc tế (IAF) trong một số lĩnh vực. Hiện nay, BoA đã triển khai xây dựng hệ thống tài liệu ISO 27001 nhằm đáp ứng nhu cầu của xã hội và dự kiến sẽ cấp chứng chỉ này cho các tổ chức chứng nhận trong năm 2023. Có thể nói, việc triển khai xây dựng hệ thống tài liệu và công nhận cho các tổ chức chứng nhận ISO 27001 là cần thiết và phù hợp với xu thế hiện nay. Trong thời gian tới, BoA mong muốn trở thành thành viên MLA của IAF trong lĩnh vực công nhận cho các tổ chức chứng nhận ISO 27001, góp phần tạo nên một môi trường số tin cậy và an toàn ✍