



Trung tâm đào tạo DAS (DAS Training) tổ chức khóa I - Đào tạo chuyên gia đánh giá hệ thống ANTT theo tiêu chuẩn ISO/IEC 27000 cho các thành viên tham gia

MỤC ĐÍCH KHÓA ĐÀO TẠO ANTT THEO ISO/IEC 27000

- Đào tạo cho học viên những kiến thức về hệ thống tiêu chuẩn hóa, hiểu từng yêu cầu của tiêu chuẩn cùng với 11 mục tiêu cần xác định và việc lập sổ tay ANTT, mục tiêu ANTT, kiểm soát mục tiêu ANTT, kiểm soát tài liệu, hồ sơ, các yêu cầu về các báo cáo sự kiện bảo mật, họp diễn đàn bảo mật, các hành động giải quyết các vấn đề liên quan đến bảo mật để đảm bảo học viên nắm bắt và triển khai được trên thực tế./.
 - Các vấn đề liên quan đến đánh giá rủi ro, xử lý rủi ro
- a) ***Xác định cách thức đánh giá rủi ro của tổ chức***
- 1) Nhận biết phương pháp đánh giá rủi ro phù hợp với ISMS, và các yêu cầu đã xác định về an ninh bảo mật thông tin kinh doanh, qui chế, luật định.
 - 2) Xây dựng các tiêu chí chấp nhận rủi ro và nhận biết các mức rủi ro có thể chấp nhận được
- b) ***Nhận biết rủi ro***
- 1) Nhận biết tài sản trong phạm vi của ISMS, và người sở hữu của các tài sản đó.
 - 2) Nhận biết các mối đe dọa với các tài sản đó.
 - 3) Nhận biết các điểm yếu có thể bị các mối đe dọa khai thác.
 - 4) Nhận biết các tác động làm mất độ tin cậy, tính toàn vẹn và tính sẵn sàng có thể xảy ra với các tài sản.
- c) ***Phân tích và định lượng rủi ro.***
- 1) Đánh giá các tác động kinh doanh đến tổ chức mà có thể là kết quả từ các sai lỗi về an ninh bảo mật, tính đến hậu quả của việc mất độ tin cậy, tính toàn vẹn và tính sẵn có của các tài sản.
 - 2) Đánh giá khả năng có thể xảy ra trên thực tế của các sai lỗi về an ninh bảo mật diễn ra trong các mối đe dọa phổ biến và các điểm yếu, và các tác động liên quan tới các tài sản này, các phương pháp kiểm soát được thực hiện gần đây
 - 3) Ước lượng mức độ rủi ro.
 - 4) Xác định rõ các rủi ro có thể chấp nhận hoặc yêu cầu xử lý theo các tiêu chí chấp nhận rủi ro đã thiết lập
- d) ***Nhận biết và đánh giá các phương án lựa chọn để xử lý rủi ro.***
Các hành động có thể thực hiện bao gồm:
- 1) Áp dụng các kiểm soát thích hợp
 - 2) Chấp nhận rủi ro một cách có nhận thức và mục đích, thể hiện chúng thoả mãn các chính sách của tổ chức và cá tiêu chí để chấp nhận rủi ro;
 - 3) Tránh rủi ro; và
 - 4) chuyển những rủi ro công việc liên quan sang tổ chức khác, ví dụ nhà bảo hiểm, nhà cung cấp.
- e) ***Lựa chọn các mục tiêu kiểm soát và phương pháp kiểm soát để xử lý rủi ro***
Các mục tiêu kiểm soát và phương pháp kiểm soát phải được lựa chọn và thực hiện nhằm đáp ứng các yêu cầu đã được xác định thông qua quá trình đánh giá rủi ro và xử lý rủi ro. Sự lựa



chọn này phải tính đến các tiêu chí chấp nhận rủi ro cũng như các yêu cầu về qui chế và luật định.

Các mục tiêu kiểm soát và phương pháp kiểm soát trong phụ lục A sẽ được lựa chọn như một phần của quá trình này phù hợp với các yêu cầu đã được xác định.

Các mục tiêu kiểm soát và phương pháp kiểm soát trong phụ lục A không đề cập hết được mọi khía cạnh và các mục tiêu kiểm soát và phương pháp kiểm soát khác nữa có thể được lựa chọn.

- Lập và quản lý các chương trình, kế hoạch đánh giá ANTT hoặc đánh giá chứng nhận.
- Tổ chức thực hiện các cuộc đánh giá và báo cáo lên diễn đàn an ninh hoặc bên ngoài theo các chuẩn mực quốc tế.
- Xác định nhu cầu và tổ chức các hoạt động cải tiến hệ thống quản lý chất lượng. Và

Việc xác định 11 Mục tiêu ISMS và 134 quy định ISMS bao gồm

- A.5 Security policy - Chính sách An ninh
- A.6 security policy - Tổ chức An ninh thông tin
- A.7 Asset management - Quản lý tài sản
- A.8 Human resources security – An ninh về nguồn nhân lực
- A.9 Physical and environmental security - An ninh về vật chất và môi trường
- A.10 Communications and operations management - Quản lý trao đổi thông tin và vận hành
- A.11 Access control - Kiểm soát truy cập
- A.12 Information systems acquisition, development and maintenance
- A.13 Information security incident management - Quản lý sự cố An ninh thông tin
- A.14 Business continuity management - Quản lý tính liên tục của quá trình kinh doanh
- A.15 Compliance - Sự phù hợp

Áp dụng mô hình PDCA để triển khai hệ thống ISMS

1. Plan (Thiết lập ISMS)
2. Do (Thi hành và điều hành ISMS)
3. Check (Kiểm soát và xem xét ISMS)
4. Act (duy trì và cải tiến ISMS)

NỘI DUNG

- Giới thiệu chung về chất lượng và các tiêu chuẩn hệ thống quản lý ANTT;
- Các nguyên tắc quản lý ANTT;
- Giới thiệu 8 nguyên tắc quản lý **(P-D-C-A)**;
- Tiêu chuẩn ISO/IEC 27001:2005
- DAS sẽ đào tạo học viên triển khai các văn bản của hệ thống an ninh thông tin ISMS như: Sổ tay, chính sách an ninh, kiểm soát tài liệu hồ sơ trên bản cứng, bản mềm, chính sách sử dụng máy tính, báo cáo diễn đàn bảo mật, họp diễn đàn bảo mật..... và **11 mục tiêu kiểm soát** với **134 quy định** về an ninh thông tin ISMS như



Việc xác định 11 Mục tiêu ISMS và 134 quy định ISMS bao gồm

- **A.5 Security policy - Chính sách An ninh**
- Cung cấp các chỉ dẫn quản lý và hỗ trợ an ninh thông tin
- **A.6 security policy - Tổ chức An ninh thông tin**
- Quản lý an ninh thông tin trong tổ chức, duy trì an ninh của các quá trình hỗ trợ thông tin của tổ chức và những tài sản thông tin được truy cập bởi các thành phần thứ ba và duy trì an ninh thông tin khi trách nhiệm việc xử lý thông tin đã được khoán ngoài cho tổ chức khác.
- **A.7 Asset management - Quản lý tài sản**
- Duy trì và đảm bảo các tài sản của tổ chức được bảo vệ ở các cấp độ thích hợp.
- **A.8 Human resources security – An ninh về nguồn nhân lực**
- Để giảm rủi ro về lỗi của con người, sự ăn cắp, gian lận hoặc lạm dụng. Đảm bảo người dùng nhận thức các mối đe dọa an ninh thông tin liên quan và được trang bị để hỗ trợ chính sách an ninh của tổ chức trong phạm vi công việc bình thường của họ, giảm thiểu từ những bất thường và sai chức năng an ninh và để kiểm soát cũng như học hỏi từ các bất thường như vậy.
- **A.9 Physical and environmental security - An ninh về vật chất và môi trường**
- Ngăn cản truy cập vật lý không được phép, phá hủy và can thiệp đến những thông tin và cơ ngơi Đơn vị. Ngăn cản sự mất mát, phá hủy hoặc tấn công những tài sản và cắt đứt các hoạt động kinh doanh. Ngăn cản sự tấn công hoặc ăn cắp thông tin và qui trình hỗ trợ xử lý thông tin.
- **A.10 Communications and operations management - Quản lý trao đổi thông tin và vận hành**
- Đảm bảo tác nghiệp bảo mật và đúng hỗ trợ xử lý thông tin, giảm thiểu rủi ro lỗi của các hệ thống, bảo vệ sự nguyên vẹn của phần mềm và những thông tin từ việc phá hủy của phần mềm đã tâm. Duy trì sự nguyên vẹn và sẵn sàng của quá trình xử lý thông tin và các dịch vụ truyền thông, đảm bảo sự an toàn của thông tin trong mạng và bảo vệ cơ sở hạ tầng hỗ trợ, ngăn cản phá hủy tài sản và làm gián đoạn các hoạt động kinh doanh, ngăn cản sự mất mát, sửa đổi và lạm dụng thông tin trao đổi giữa các tổ chức.
- **A.11 Access control - Kiểm soát truy cập**
- Kiểm soát truy cập đến thông tin, đảm bảo các quyền truy cập đến các hệ thống thông tin được cấp quyền, cấp phát tài nguyên và duy trì một cách phù hợp. Ngăn cản truy cập trái phép, phát hiện các hoạt động trái phép, bảo vệ các dịch vụ mạng, đảm bảo an ninh thông tin khi dùng máy tính di động và phương tiện điện thoại.
- **A.12 Information systems acquisition, development and maintenance**
- Đảm bảo an ninh được xây dựng bên trong các hệ thống thông tin. Ngăn cản, điều chỉnh, và lạm dụng dữ liệu của người dùng trong các hệ thống ứng dụng, bảo vệ tính tin cậy, tính xác thực hoặc nguyên vẹn của thông tin. Đảm bảo các dự án CNTT và các hoạt động hỗ trợ được điều hành trong một thể thức an ninh. Duy trì an ninh của phần mềm hệ thống ứng dụng và thông tin.
- **A.13 Information security incident management - Quản lý sự cố An ninh thông tin**
-
- **A.14 Business continuity management - Quản lý tính liên tục của quá trình kinh doanh**
- Chống lại sự ngưng trệ của các hoạt động kinh doanh và bảo vệ các quá trình kinh doanh quan trọng từ hậu quả của lỗi lớn hoặc hiểm họa.
- **A.15 Compliance - Sự phù hợp**



- Tránh sự vi phạm của mọi luật công dân và hình sự, tuân thủ pháp luật, qui định hoặc nghĩa vụ của hợp đồng và mọi yêu cầu về an ninh. Đảm bảo sự tuân thủ của các hệ thống với các chính sách an ninh và các chuẩn. Tăng tối đa hiệu quả và giảm thiểu trở ngại đến quá trình đánh giá hệ thống.
- **V. Áp dụng mô hình PDCA để triển khai hệ thống ISMS**
 - **1. Plan (Thiết lập ISMS)**
 - Thiết lập chính sách an ninh, mục tiêu, mục đích, các quá trình và thủ tục phù hợp với việc quản lý rủi ro và cải tiến an ninh thông tin để phân phối các kết quả theo các mục tiêu và chính sách tổng thể của tổ chức.
 - **2. Do (Thi hành và điều hành ISMS)**
 - Thi hành và điều hành chính sách an ninh, các dấu hiệu kiểm soát, các quá trình và các thủ tục.
 - **3. Check (Kiểm soát và xem xét ISMS)**
 - Đánh giá, tìm kiếm sự phù hợp, đo lường hiệu năng của quá trình so với chính sách an ninh, mục tiêu, kinh nghiệm thực tế và báo cáo kết quả cho lãnh đạo xem xét.
 - **4. Act (duy trì và cải tiến ISMS)**
 - Đưa ra các hành động khắc phục phòng ngừa trên cơ sở các kết quả xem xét để cải tiến liên tục hệ thống ISMS
- Các khái niệm về đánh giá; và nguyên tắc trong đánh giá
- 2 giai đoạn của quá trình đánh giá;
- Hoạt động chứng nhận và công nhận các tổ chức chứng nhận;
- Vai trò và trách nhiệm của trưởng đoàn và các chuyên gia đánh giá;
- Diễn giải yêu cầu của tiêu chuẩn ISO/IEC 27001:2005 và các nội dung cần xem xét, đánh giá;
- Xác định phạm vi và các quá trình cần đánh giá;
- Triển khai và quản lý chương trình đánh giá thông qua cách tiếp cận theo quá trình;
- Lập kế hoạch đánh giá;
- Đánh giá hệ thống tài liệu;
- Tiến hành các hoạt động đánh giá tại chỗ (gồm cả điều khiển cuộc họp khai mạc và họp kết thúc);
- Thu thập và trao đổi thông tin trong quá trình đánh giá;
- Tổng hợp các phát hiện trong quá trình đánh giá, viết báo cáo không phù hợp;
- Báo cáo kết quả đánh giá và xác định các cơ hội cải tiến;
- Thực hiện các hoạt động sau đánh giá;
- Các bài tập về tiêu chuẩn và các tình huống đánh giá;
- Kiểm tra đánh giá cuối khóa đào tạo để cấp chứng chỉ
- Học viên sau khi học sẽ có một cách nhìn nhận về Hệ thống quản lý ANTT một cách khoa học, hệ thống bao gồm:
 - Được đào tạo lý thuyết đan xen thực tế thông qua các mô hình đào tạo tại văn phòng của D.A.S như: Hệ thống bản cứng, bản mềm, hệ thống kiểm soát quá trình di chuyển hồ sơ từ bộ phận, đơn vị này sang đơn vị khác, hệ thống kiểm soát camera quan sát, hệ thống kiểm soát ra vào.
- Các học viên sẽ được thực hành trên thực tế với sự hướng dẫn của các chuyên gia giàu kinh nghiệm.



DAS TRAINING CENTER

- Cách thức lưu trữ cơ sở dữ liệu khi gặp sự cố về thiên tai, động đất, hoả hoạn, chập điện, trộm cắp... để khi xảy ra các sự cố không làm ảnh hưởng tới hoạt động của hệ thống.
- Thiết lập khu vực an ninh cao và bố trí hệ thống camera quan sát tại những nơi có độ rủi ro cao để phòng ngừa các sự cố xảy ra như: Phòng máy chủ, kết sắt, nhà kho, văn phòng,...
- Nâng cao nhận thức và trách nhiệm của CBCNV trong việc sử dụng user và password khi đăng nhập vào hệ thống, cách thức mã hoá password và phân quyền cho người sử dụng khi đăng nhập vào các hệ thống quan trọng.
- Kiểm soát và đánh giá rủi ro an ninh thông tin.
- Cách thức lưu trữ thông tin các hồ sơ, tài liệu trên bản cứng, bản mềm, hoặc đĩa CD của những người có liên quan để tránh xảy ra tình trạng mất mát.
- Kiểm soát các thiết bị lưu trữ thông tin di động để tránh xảy ra tình trạng mất mát dữ liệu như: ổ cứng, usb, máy ảnh, máy chiếu, máy phô tô, máy ghi âm,..
- Kiểm soát CBCNV, khách hàng khi làm việc nghỉ việc tại đơn vị.
-

GIẢNG VIÊN

- Giảng viên được công nhận quốc tế được DAS-UK Vương Quốc Anh phê duyệt với nhiều kinh nghiệm đánh giá chứng nhận các hệ thống quản lý ANTT (ISMS) theo ISO/IEC 27000.

LỢI ÍCH KHÓA ĐÀO TẠO

- Tham dự khóa học, học viên được học hỏi, chia sẻ những kinh nghiệm quý báu từ các giảng viên có nhiều năm làm công tác đánh giá chứng nhận các hệ thống quản lý. Học viên được cấp Chứng chỉ chuyên gia đánh giá trưởng có khả năng vượt qua kỳ thi của DAS:
- Chứng chỉ chuyên gia đánh giá trưởng có cơ hội trở thành chuyên gia đánh giá chuyên nghiệp

PHƯƠNG PHÁP HỌC:

- Học viên được thực hành và trao đổi kinh nghiệm đối với từng nội dung khóa học. Thông qua các bài tập, làm việc theo nhóm, làm quen với các tình huống đánh giá, đánh giá giả định, trình bày kết quả đánh giá... học viên có cơ hội chia sẻ, tích lũy các kinh nghiệm đánh giá và cải tiến hệ thống quản lý ANTT.
- Học viên được tham gia thực hiện các công việc của DAS và được kiểm tra để lấy kiến thức trên thực tế
-

ĐỐI TƯỢNG THAM DỰ:

- Đại diện ANTT, cán bộ an ninh, đánh giá viên nội bộ;
- Chuyên gia tư vấn, chuyên gia đánh giá;
- Các thành viên am hiểu Công nghệ thông tin



DAS TRAINING CENTER

- Các học viên làm các công việc quản lý tại các đơn vị có mức độ rủi ro cao ANTT như: Viễn thông, chứng khoán, Ngân hàng, công nghệ thông tin
- Các cá nhân quan tâm tới chủ đề và nội dung của khóa học.

THỜI GIAN THAM DỰ:

- Khóa đào tạo được tổ chức 08 tháng
- Mỗi tuần 02 buổi;
- Số lượng học viên không quá 10 người./.

Ghi chú:

- Học viên yêu cầu phải có kiến thức cơ bản về Bộ tiêu chuẩn ISO 27000..
- Đăng ký: vui lòng đăng ký bằng điện thoại hoặc email cho DAS:
das.training@dasvietnam.com.
- Thủ tục thanh toán: Thanh toán trực tiếp bằng tiền mặt hoặc chuyển khoản tới:
Trung tâm Đào tạo DAS Việt anm (DAS Training)

ĐỊA ĐIỂM:

**Trung tâm Đào tạo DAS - Tầng 6, Tòa nhà 34JSC
Số 164 Khuất Duy Tiến, Thanh xuân, Hà Nội
Tel 844.37763177 - 844 35539 135 – Fax: 844-37763777
Hoặc click vào đây**