**ISO 27001 LÀ GÌ?**

Trước đây tiêu chuẩn này có tên gọi là BS 7799 và ISO 17799.

**ISO 27001 là tiêu chuẩn của Anh về hệ thống quản lý an ninh thông tin (viết tắt là ISMS).**

Thông tin là một phần quan trọng của mỗi tổ chức và tiêu chuẩn này đưa ra các phưong pháp đánh giá việc theo dõi, bảo vệ và quản lý hệ thống thông tin và dữ liệu.

Việc mất dữ liệu và thông tin trong bất cứ trường hợp nào ít nhất cũng gây ra sự bất tiện cho tổ chức, và trầm trọng hơn có thể khiến tổ chức sụp đổ.

**ISO 27001 sẽ giúp tổ chức của tôi bằng cách nào?**

**ISO 27001**phù hợp với mọi tổ chức lớn nhỏ và áp dụng được với mọi lĩnh vực kinh tế trên toàn thế giới.

Thông qua việc triển khai một hệ thống vững chắc để quản lý thông tin trong tổ chức, bạn có thể bảo vệ được tài sản thông tin, đảm bảo được sự liên tục trong kinh doanh nếu có xảy ra sự phá hoại hoặc mất mát nào.

Mất mát hoặc phá hoại có thể do rất nhiều nguyên nhân; thiên tai như hoả hạn hoặc lũ lụt, sự mất mát ngẫu nhiên hoặc do quản lý kém, bị mua chuộc hoặc bị đánh cắp, những mất mát này  có thể gây ra những hậu quả khôn lường cho tổ chức.

Thông tin có thể là dữ liệu mà tổ chức sở hữu và nó có thể là những dữ liệu được lưu lại dưới dạng điện tử, thông tin được chuyển qua bưu điện hay email, các dữ liệu hoặc thông tin được in ra mà từng người trong tổ chức của bạn lưu giữ.

Thông qua việc triển khai **ISO 27001** tổ chức sẽ xác định được loại thông tin trong tổ chức và xác định các mối nguy và mối đe doạ. Sau đó bạn có thể thiết lập hệ thống, thiết lập sự kiểm soát và các quy trình để giảm thiểu các mối nguy.

**ISO 27001** tạo ra một hệ thống theo dõi và duy trì:

* Tính bảo mật thông tin
* Tính sẵn có của thông tin
* Tính chính xác của thông tin

Tổ chức xử lý thông tin thay cho các tổ chức khác có thể có được lợi ích rất lớn từ việc được công nhận do họ có thể chứng minh được rằng họ có một quá trình tại chỗ trong việc theo dõi liên tục và bảo vệ dữ liệu của bên thứ ba.

**Các lợi ích mà ISO 27001 đem lại cho tổ chức bao gồm:**

* Sự liên tục trong kinh doanh
* Đánh giá được mối nguy và triển khai được các phương pháp để giảm bớt ảnh hưởng
* An ninh được cải thiện
* Kiếm soát việc truy cập
* Tiết kiệm chi phí
* Tạo ra một quá trình quản lý nội bộ
* Tuyên truyền cam kết của bạn để bảo vệ dữ liệu của khách hàng.
* Chứng minh được rằng bạn tuân thủ các quy định pháp luật
* Xác định được rằng các lãnh đạo cấp cao thực sự nghiêm túc trong việc bảo mật dữ liệu.
* Đánh giá thường xuyên để duy trì hiệu quả bảo mật
* Cung cấp chứng nhận độc lập

**Xem thêm**[**Top 10 lý do để chứng nhận ISO 27001**](http://www.acsregistrars.vn/top-10-ly-do-de-chung-nhan-iso-27001)

**Đánh giá liên tục giành lợi thế cạnh tranh**

Nếu tổ chức bạn đạt được chứng nhận ISO 27001, khách hàng của bạn tin tưởng khi biết rằng những mối rủi ro về an ninh đều được đánh giá và giảm thiểu và tổ chức của bạn cũng có sẵn những hệ thống để bảo vệ và khôi phục thông tin nhanh chóng trong trường hợp mất dữ liệu.

Một quá trình cải tiến liên tục sẽ đem lại cho tổ chức của bạn những công cụ quản lý cần thiết để giám sát và cải tiến vấn đề an ninh của những thông tin giá trị của tổ chức bạn.

**Để biết thêm thông tin về chứng nhận ISO 27001, vui lòng ghé thăm trang website:[www.iso27001.com.vn](http://iso27001.com.vn/" \t "_blank)**

**1. Thông tin đúng:** Có được thông tin đúng là yếu tố sống còn của bất kỳ tổ chức hay doanh nghiệp nào. Tuy nhiên, việc nắm bắt được và kiểm soát thông tin đúng thường khó và không bền vững. Do vậy, ISO 27001 sẽ giúp các tổ chức hay doanh nghiệp quản lý thông tin của mình một cách hiệu quả hơn.

**2. Thúc đẩy quan hệ đối tác:** Các tổ chức hay doanh nghiệp ngày càng ý thức được việc thiếu kiểm soát của mình, đặc biệt là công tác thông tin tới nhà cung cấp và khách hàng của mình. Do đó, họ đang tìm kiếm các quy tắc và sự tin tưởng nhờ hệ thống đánh giá theo tiêu chuẩn ISO 27001 đem lại.

**3. Cắt giảm chi phí trong chuỗi cung ứng:** [ISO 27001](http://www.acsregistrars.vn/chung-nhan-tieu-chuan-iso-27001) được coi như sáng kiến giúp giảm thiểu các hoạt động trùng lặp của công ty hay doanh nghiệp bạn, chẳng hạn như kiểm tra lượng hàng nhập vào và xuất ra. Tiêu chuẩn này cũng được coi là sáng kiến nhằm giảm dữ liệu đầu vào cho doanh nghiệp.

**4. Không đơn thuần về an ninh thông tin:** Ngoài đảm bảo an ninh thông tin, [ISO 27001](http://www.acsregistrars.vn/chung-nhan-tieu-chuan-iso-27001) còn cung cấp các giải pháp quản lý bảo mật, tính toàn vẹn và sẵn có của thông tin. Đồng nghĩa với đó là hỗ trợ quản lý rủi ro cho các tổ chức doanh nghiệp.

**5. Hoạt động trên quy trình và hệ thống nhất quán:** ISO 27001 giúp huy động các nguồn lực then chốt nhằm đề ra các hành động cần thiết để giảm thiểu sự cố thông tin và quản lý rủi ro thông tin cho các tổ chức doanh nghiệp.

**6. Không chỉ riêng bộ phận CNTT:** Trước kia, ISO 27001 được biết đến là tiêu chuẩn đánh giá trong lĩnh vực công nghệ thông tin (CNTT). Tuy nhiên, hiện nay tiêu chuẩn này đã được mở rộng và bao quát toàn bộ tổ chức hay doanh nghiệp từ nhân viên vệ sinh đến giám đốc điều hành.

**7. Được đánh giá bởi Tổ chức chứng nhận được công nhận Quốc tế** (ví dụ như Tổ chức Công nhận Vương quốc Anh - UKAS). Điều này không chỉ đảm bảo cho công ty hay doanh nghiệp bạn duy trì và cải tiến hoạt động của mình mà còn giúp xác định năng lực và tìm kiếm các cơ hội hợp tác.

**8. Tăng khả năng trúng thầu và cơ hội ký kết hợp đồng:** Khách hàng thường bị hạn chế về nguồn lực để tìm hiểu các đối tác hay nhà cung cấp của mình. Thông thường họ sử dụng ISO 27001 và các tiêu chuẩn quản lý khác làm thước đo xác định xem tổ chức hay doanh nghiệp bạn có phải là đối tác tin cậy hay không để từ đó tiếp tục xem xét hồ sơ bỏ thầu của doanh nghiệp bạn.

**9. Cải thiện lợi nhuận:** Các sự cố và vụ việc nghiêm trọng như sự cố đều khiến tổ chức hay doanh nghiệp bạn lãng phí thời gian và tiền bạc. Do vậy, điều quan trọng là làm thể nào xác định được các sự cố và rủi ro tiềm ẩn và triển khai hành động phòng ngừa sự cố đó. Sẽ không ngạc nhiên nếu tổ chức hay doanh nghiệp bạn phải bỏ thời gian và tiền bạc để khắc phục các sự cố an ninh thông tin mà nguyên nhân là không chủ động xác định các sự cố và rủi ro tiềm ẩn. Trên cơ sở đó, ISO 27001 hướng tới giúp các doanh nghiệp đảm bảo thông tin đúng được cung cấp đúng chỗ, đúng lúc và đúng người.

**10. Liên tục cải tiến:** Môi trường kinh doanh hiện đang không ngừng thay đổi. Do vậy, các tổ chức hay doanh nghiệp cũng cần phải cải tiến và thay đổi để phù hợp với xu thế. Để tăng tính hiệu quả cho các doanh nghiệp, [ISO 27001](http://www.acsregistrars.vn/chung-nhan-tieu-chuan-iso-27001) hỗ trợ họ giám sát các chỉ số quan trọng của mình và đưa ra quyết định và hành động phù hợp với thực tế.

# Quá trình chứng nhận ISO 27001

## ****1. Xác định lợi ích****

Nhóm quản lý xác định các lợi ích mà tổ chức có thể có thông qua việc áp dụng một hệ thống quản lý an ninh thông tin và đạt chứng nhận ISO 27001.

Sau đó, bạn cần chỉ định một chuyên gia tư vấn có kinh nghiệm với những hiểu biết cần thiết để đạt được chứng nhận ISO 27001.

## ****2. Đánh giá rủi ro****

Công việc sẽ bắt đầu từ việc xác định, sau đó đánh giá các rủi ro về an ninh trong toàn tổ chức.

Mỗi rủi ro đều được đánh giá về nguy cơ diễn ra cao hay thấp và đánh giá mức độ ảnh hưởng của từng sự cố đối với tổ chức.

## ****3. Kiểm soát thực hiện****

Từ danh sách các rủi ro an ninh đã được xác định, có thể áp dụng các biện pháp kiểm soát thích hợp để giảm rủi ro xuống mức độ chấp nhận được.

Sau đó các hệ thống quản lý sẽ được thiết lập để quản lý các rủi ro, giám sát các sự cố an ninh và liên tục giám sát các quá trình, xác định các rủi ro mới.

### ****Tiến hành chứng nhận****

Đến bước này, bạn đã sẵn sàng tiến hành lần đánh giá đầu tiên.

Trước tiên, chuyên gia đánh giá sẽ xem xét hệ thống văn bản , đảm bảo rằng chúng khớp với những gì bạn thực sự thực hiện và đưa ra kiến nghị thay đổi nếu cần.

Khi đã thực hiện những thay đổi cần thiết, bạn sẽ sẵn sàng để tiến hành một cuộc đánh giá thực sự thực hiện bởi một tổ chức chứng nhận độc lập được công nhận, tổ chức đó nên được UKAS công nhận.

### ****Quản lý hệ thống tài liệu****

Lưu giữ các hồ sơ và sử dụng hệ thống tài liệu thích hợp sẽ giúp bạn duy trì được một hệ thống hiệu quả.

### ****Biện pháp khắc phục****

Có một điều không thể tránh khỏi đó là các quá trình có thể trở nên không còn đúng và bạn sẽ cần có một quá trình đã xác định để sửa chữa vấn đề và xác định điểm sai trước khi thay đổi để ngăn không có vấn đề tái diễn.

Bạn nên giữ một hồ sơ về các hành động bạn thực hiện để điều chỉnh vấn đề. Nếu có thể, bạn nên xác định các vùng vấn đề tiềm ẩn và thiết lập một hệ thống nhằm ngăn chặn hay giảm thiểu hiệu ứng của chúng trước khi xảy ra vấn đề.

### ****Đánh giá thường xuyên****

Bạn cần phải thường xuyên Đánh giá chất lượng nội bộ hệ thống mình áp dụng. Những cá nhân trong tổ chức của bạn, những người độc lập với các chức năng được đánh giá có thể tiến hành đánh giá nội bộ.

Chuyên gia đánh giá sẽ kiểm ra xem tổ chức bạn có làm theo các quy trình hay không và xác định bất kỳ khu vực nào cần phải điều chỉnh.

Bạn sẽ phải có một quy trình cho việc lập kế hoạch, thực hiện và ghi chép các cuộc đánh giá.