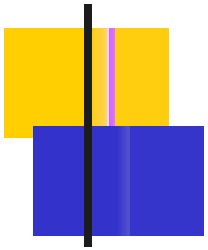
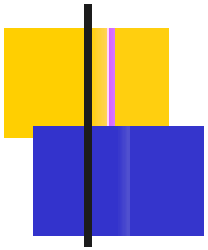
TIÊU CHUẨN AN TOÀN MẠNG

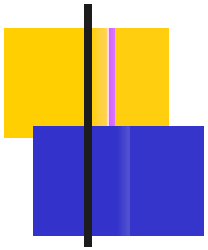
- An toàn thông tin là các biện pháp nhằm đảm bảo tính bí mật (confidentiality), tính toàn vẹn (integrity) và tính sẵn sàng (availability) của thông tin.
- **ISO 17799**: Mục tiêu của BS7799 / ISO 17799 là "tạo nền móng cho sự phát triển các tiêu chuẩn về ATTT và các biện pháp quản lý ATTT hiệu quả trong một tổ chức , đồng thời tạo ra sự tin cậy trong các giao dịch liên tổ chức"



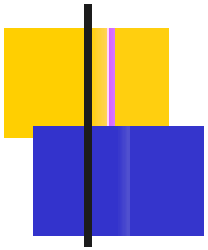
- ISO 17799 nhằm để thiết lập hệ thống quản lý bảo mật thông tin, gồm các bước như sau:
  - a) Xác định phạm vi và ranh giới của hệ thống ISMS phù hợp với đặc điểm của hoạt động kinh doanh, việc tổ chức, vị trí địa lý, tài sản và công nghệ, và bao gồm các chi tiết của chúng và các minh chứng cho các loại trừ trong phạm vi áp dụng.



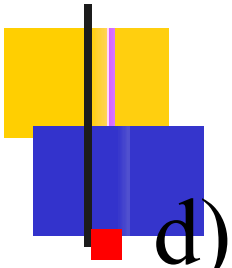
- b) Xác định một chính sách của hệ thống bảo mật phù hợp với đặc điểm của hoạt động kinh doanh, việc tổ chức, vị trí địa lý, tài sản và công nghệ mà:
  - 1) Bao gồm cơ cấu cho việc thiết lập các mục tiêu và xây dựng ý thức chung trong định hướng và các nguyên tắc hành động về bảo mật thông tin.



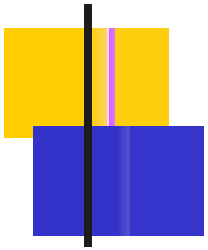
- 2) Quan tâm đến các hoạt động kinh doanh và các yêu cầu của luật hoặc pháp lý, và các bổn phận bảo mật thõa thuận.
- 3) Sắp xếp thực hiện việc thiết lập và duy trì hệ thống ISMS trong chiến lược của tổ chức về việc quản lý các rủi ro.
- 4) Thiết lập tiêu chuẩn để đánh giá các rủi ro
- 5) Được duyệt bởi lãnh đạo



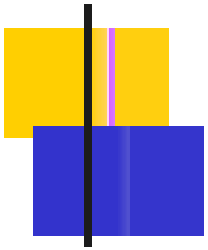
- c) Xác định cách thức đánh giá rủi ro của tổ chức
  - 1) Xác định phương pháp đánh giá rủi ro phù hợp với hệ thống mạng, và những thông tin của hoạt động kinh doanh đã xác định, các yêu cầu của luật và pháp chế
  - 2) Xây dựng tiêu chuẩn chấp nhận các rủi ro và xác định các mức độ chấp nhận



- d) Xác định các rủi ro
  - 1) Xác định các tài sản thuộc phạm vi của hệ thống mạng và các chủ nhân của những tài sản này
  - 2) Xác định các rủi ro cho các tài sản đó
  - 3) Xác định các yếu điểm mà có thể bị khai thác hoặc lợi dụng bởi các mối đe dọa
  - 4) Xác định các ảnh hưởng hoặc tác động làm mất tính bí mật, toàn vẹn và sẵn có mà có thể có ở các tài sản này

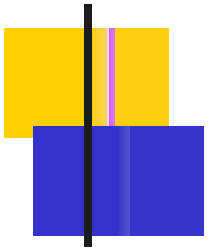


- e) Phân tích và đánh giá các rủi ro
  - 1) Đánh giá các tác động ảnh hưởng đến hoạt động của tổ chức có thể có do lỗi bảo mật, Quan tâm xem xét các hậu quả của việc mất tính bảo mật, toàn vẹn hoặc sẵn có của các tài sản
  - 2) Đánh giá khả năng thực tế có thể xãy ra các lỗi bảo mật do khinh suất các mối đe dọa và yếu điểm phổ biến hoặc thường gặp,

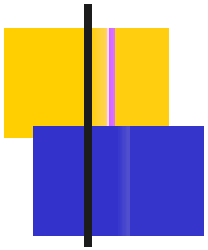


và do các ảnh hưởng liên quan đến các tài sản này, và do việc áp dụng các biện pháp kiểm soát hiện hành.

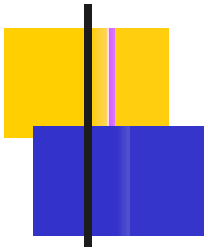
- 3) Ước lượng các mức độ rủi ro
- 4) Định rõ xem coi các rủi ro có thể chấp nhận được hay cần thiết phải có xử lý bằng cách sử dụng các tiêu chuẩn chấp nhận rủi ro đã được lập trong mục c – 2



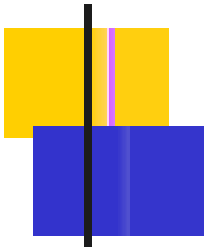
- f) Xác định và đánh giá các phương án xử lý các rủi ro
  - 1) Áp dụng các biện pháp kiểm soát thích hợp
  - 2) Chủ tâm và một cách khách quan chấp nhận các rủi ro, với điều kiện chúng thõa mãn một cách rõ ràng các chính sách của tổ chức và các chuẩn mực chấp nhận rủi ro.



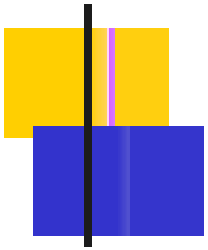
- 3) Tránh các rủi ro
- 4) Chuyển các công việc rủi ro liên đới cho các tổ chức/cá nhân khác như nhà bảo hiểm, nhà cung cấp



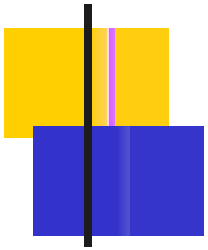
- g) Chọn các mục tiêu kiểm soát và các biện pháp kiểm soát để xử lý các rủi ro
- h) Thông qua lãnh đạo các đề suất về các rủi ro còn lại sau xử lý
- i) Được phép của lãnh đạo để áp dụng và vận hành hệ thống quản lý bảo mật thông tin



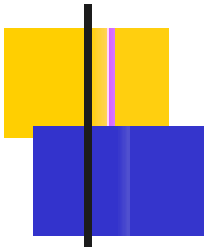
- j) Chuẩn bị bản tuyên bố áp dụng
  - 1) Các mục tiêu kiểm soát và các biện pháp kiểm soát được và các lý do chọn chúng
  - 2) Các mục tiêu kiểm soát và các biện pháp kiểm soát hiện đang được áp dụng
  - 3) Các ngoại lệ của bất kỳ các mục tiêu kiểm soát và các biện pháp kiểm soát và minh chứng cho chúng.



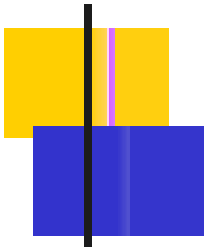
- Áp dụng và vận hành hệ thống mạng theo ISO 17799 gồm các bước như sau:
  - a) Trình bày một kế hoạch xử lý rủi ro rõ ràng để xác định sự phù hợp của các hành động của lãnh đạo, các nguồn lực, trách nhiệm và ưu tiên của việc quản lý các rủi ro bảo mật thông tin



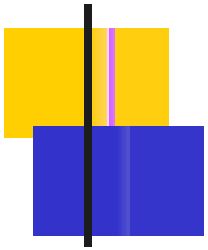
- b) Áp dụng kế hoạch xử lý rủi ro để mà đạt được các mục tiêu kiểm soát đã xác định, trong đó bao gồm việc xem xét chi phí (funding) và sự phân công vai trò và trách nhiệm
- c) Áp dụng các biện pháp kiểm soát được lựa chọn nhằm đạt được các mục tiêu kiểm soát



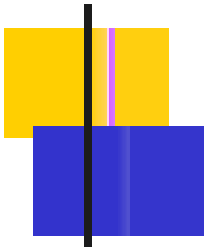
- d) Xác định cách thức đo lường hiệu quả của các biện pháp kiểm soát đã chọn hoặc nhóm các kiểm soát và xác định cách thức sử dụng các cách đo này để kiểm soát đánh giá một cách hiệu quả để cho ra các kết quả có thể so sánh và tái thực nghiệm



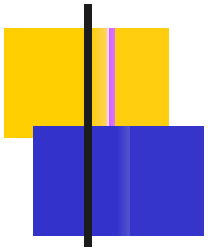
- e) Đào tạo áp dụng và các chương trình nhận thức
- f) Quản lý hoạt động của hệ thống mạng
- g) Quản lý nguồn lực cho hệ thống mạng
- h) Áp dụng các thủ tục quy trình và các biện pháp kiểm soát có thể khác để kích hoạt việc phát hiện kịp thời các sự kiện bảo mật và đối phó với các sự cố bảo mật



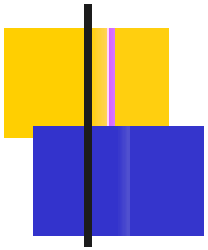
- Giám sát và tái xem xét hệ thống mạng theo ISO 17799, gồm các bước sau:
  - a) Thực hiện giám sát và xem xét các thủ tục và các biện pháp kiểm soát khác để :
    - 1) Phát hiện kịp thời sai lỗi ngay trong các kết quả của quá trình xử lý
    - 2) Nhận biết kịp thời việc thử nghiệm và đột nhập thành công các lỗ hổng và sự cố bảo mật



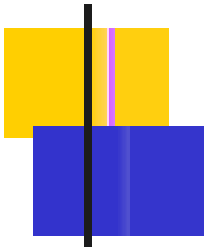
- 3) Để cho lãnh đạo xác định được hoạt động bảo mật ủy thác cho người hay vận dụng công nghệ thông tin đang hoạt động có đạt như mong đợi không
- 4) Giúp cho việc phát hiện sự kiện bảo mật và để ngăn ngừa sự cố bảo mật bằng việc sử dụng các chỉ số
- 5) Xác định các hành động giải quyết lỗ hổng bảo mật có hiệu quả không



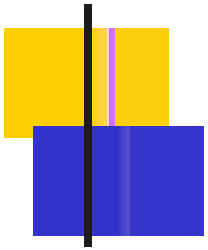
- b) Thực hiện việc xem xét định kỳ hiệu quả của hệ thống ISMS (Bao gồm việc đạt được chính sách bảo mật và các mục tiêu, và xem xét các biện pháp kiểm soát bảo mật) quan tâm đến các kết quả của việc đánh giá bảo mật, các sự cố, các kết quả đo lường hiệu quả, các kiến nghị và phản hồi từ các bên quan tâm.
- c) Đo lường hiệu quả của các biện pháp kiểm soát để xác minh là các yêu cầu bảo mật đã được thõa mãn.



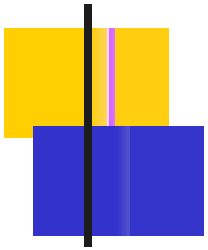
- d) Xem xét các việc đánh giá rủi ro ở các giai đoạn đã hoạch định và xem xét các rủi ro còn lại và các mức độ chấp nhận rủi ro đã xác định, quan tâm đến các thay đổi đến
  - 1) Cơ cấu tổ chức
  - 2) Công nghệ
  - 3) Mục tiêu kinh doanh và các quá trình



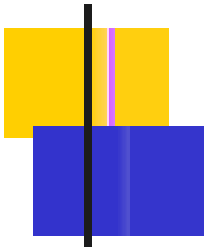
- 4) Các mối đe dọa đã xác định
- 5) Hiệu quã của việc áp dụng các kiểm soát
- 6) Các sự kiện bên ngoài, như là luật hay môi trường pháp lý thay đổi, càc bổn phận thõa thuận thay đổi, và hoàn cảnh xã hội thay đổi.



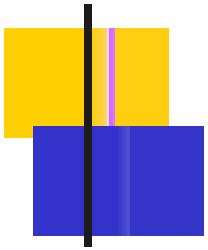
- e) Thực hiện đánh giá nội bộ hệ thống ISMS theo chu kỳ đã hoạch định
- f) Thực hiện việc xem xét lãnh đạo cho hệ thống mạng một cách định kỳ nhằm đảm bảo phạm vi áp dụng vẫn còn đầy đủ và các cải tiến trong quá trình của hệ thống mạng được nhận biết



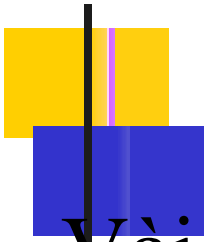
- g) Cập nhật các kế hoạch bảo mật nhằm quan tâm các phát hiện của hoạt động giám sát và xem xét
- h) Hồ sơ của các hành động và sự kiện mà có thể ảnh hưởng đến hiệu quả hoặc năng lực của hệ thống mạng



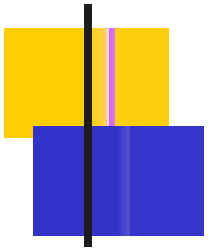
- Duy trì và cải tiến hệ thống mạng theo ISO 17799, gồm các bước sau:
  - a) Áp dụng các cải tiến đã nhận biết trong hệ thống mạng
  - b) Thực hiện các hành động khắc phục và phòng ngừa . Áp dụng các bài học kinh nghiệm từ các sự cố bảo mật của các tổ chức khác và của chính tổ chức



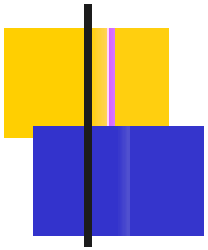
- c) Trao đổi các hành động và các cải tiến cho tất cả các bên quan tâm với mức độ chi tiết phù hợp với hoàn cảnh và, khi thích hợp, thống nhất cách thức thực hiện.
- d) Đảm bảo rằng các cải tiến đạt được mục tiêu mong muốn cho chúng



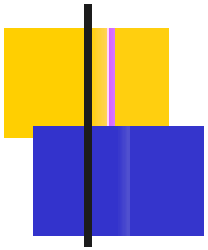
- Vài ví dụ về rủi ro mất an toàn thông tin :
  - Bị **Virus** xâm nhập: hỏng dữ liệu, ngừng hệ thống, …
  - Bị **Trojan, Spyware**: ăn cắp thông tin, cài đặt cổng hậu, …
  - Bị **đánh cắp mật khẩu**: dẫn đến bị giả mạo để truy nhập thông tin
  - Bị **Hacker** (Tin tặc) xâm nhập qua mạng: để phá hoại hệ thống, lấy cắp hay sửa đổi thông tin, …



- Bị "**nghe trộm**" (sniffer) thông tin khi truyền qua mạng: lộ bí mật kinh doanh (giá bỏ thầu, giá mua hàng…), bị sửa sai lệch thông tin,…
- Bị **thông tin giả mạo** gửi đến, dẫn đến những quyết định sai gây thiệt hại nghiêm trọng (vi phạm tính chống từ chối): **PHISHING, …**
- Bị **sửa đổi trang Web**, gây mất uy tín với KH, bạn hàng, …



- Bị **người dùng bên trong** làm lộ thông tin cho đối thủ, …(information leakage)
- Bị **người dùng bên trong** phá hoại, …
- Bị **lỗ hổng, back-door** (vô tình hay cố ý) trong các **ứng dụng thuê** công ty bên ngoài **phát triển ……**
- Bị **tấn công từ chối dịch vụ**: gây ngừng trệ hệ thống (mất tính sẵn sàng)



THANKS