Hệ thống Quản lý An toàn Thông Tin (ISMS) theo ISO 27001:2005

Cách tiếp cận & áp dụng thực tế

Trịnh Tuấn Dũng
GĐ Chứng nhận
Bureau Veritas Certification VN

Hà Nội, Security World – 24 & 25 tháng 3 năm 2009

Nội dung

1. **Nhu cầu thực tế & giới thiệu về bộ tiêu chuẩn Quốc tế về Hệ thống Quản lý An toàn Thông tin (ISMS)**

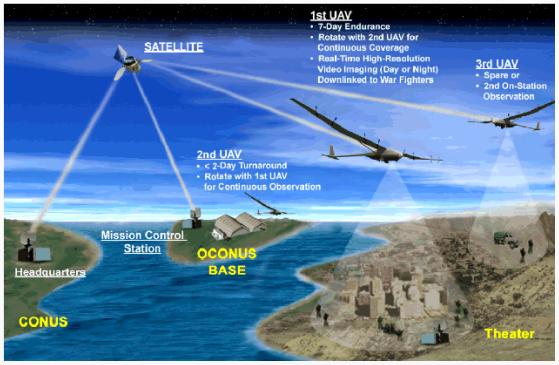
2. **Các bước thực hiện ISO 27001:2005 – Cách tiếp cận áp dụng thực tế.**

3. **Ích lợi**

NHU CẦU CẦN CÓ CỦA HT AN TOÀN THÔNG TIN

Nhu cầu cần có của tiêu chuẩn

- Trước những năm 1970, công nghệ ATTT => Chính phủ, Quân sự, hay Ngân hàng
- Internet và kinh doanh trên mạng “on-line”, ATTT => nhận dạng, chứng thực, và quản lý người sử dụng…
- Pháp luật về Chữ ký điện tử tạo điều kiện cho việc phát triển e-business, e-commerce
- Mọi người cần niềm tin và thực hiện có hiệu lực => HTQL ATTT

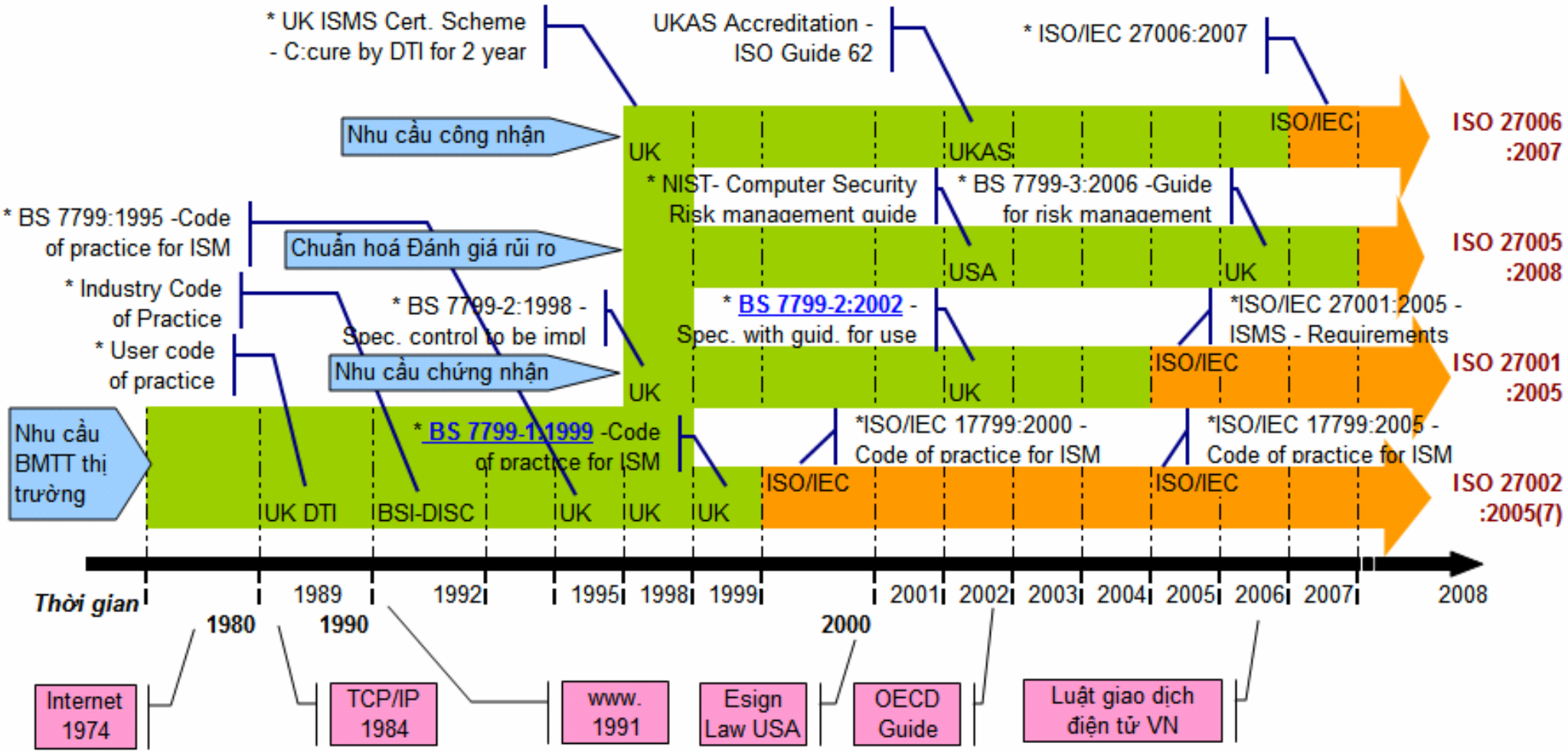


Các HTQL nhằm cải tiến & cung cấp lòng tin

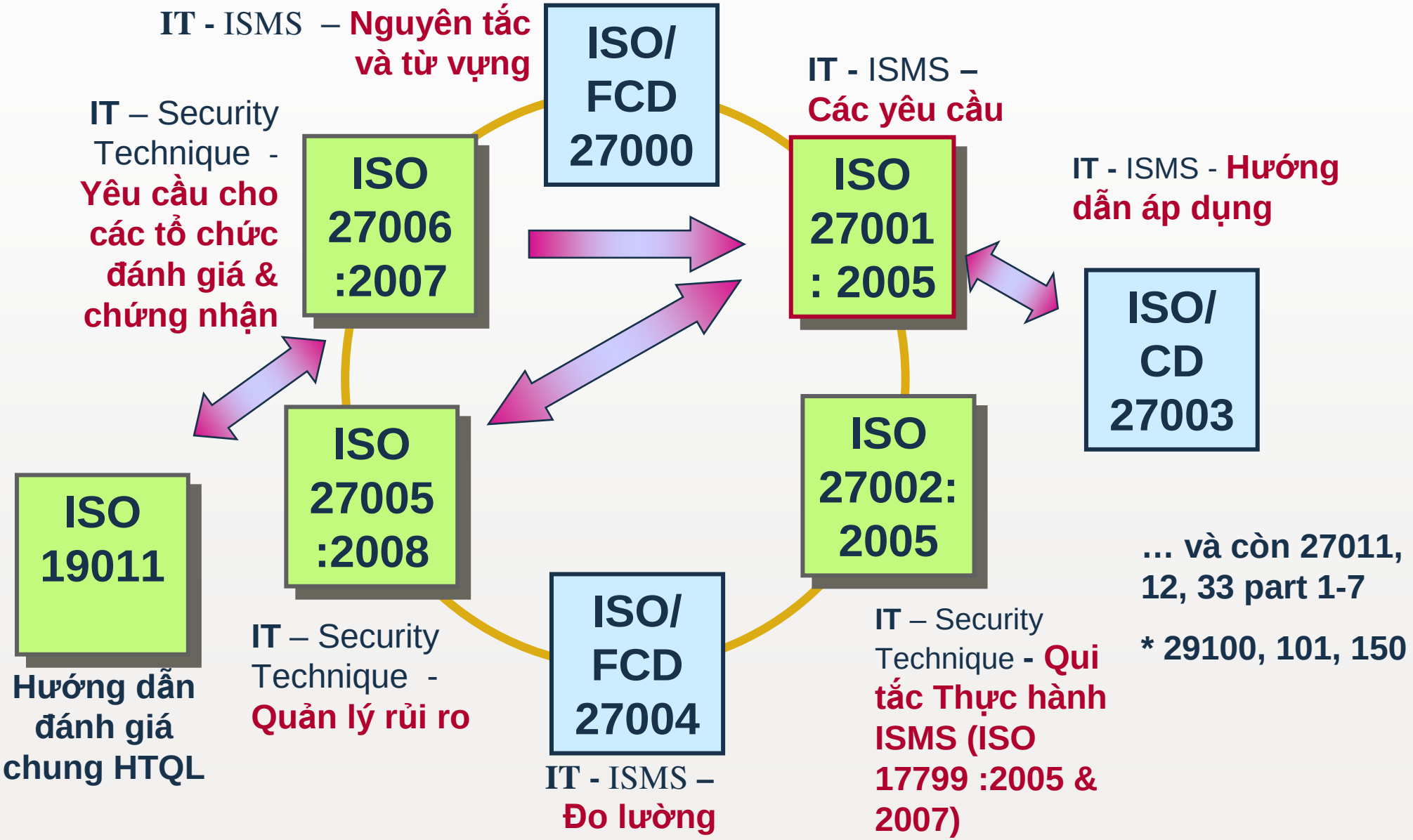
- Đảm bảo chất lượng sản phẩm & thoả mãn khách hàng => ISO 9001
- Bảo vệ môi trường sống cho cộng đồng => ISO 14001 …
- Đảm bảo Sức khoẻ, an toàn người lao động => OHSAS 18001
- Đảm bảo vệ sinh thực phẩm => ISO 22000
- Bảo mật thông tin liên lạc – là một loại tài sản đặc thù => ???
- HTQL ATTT

Lịch sử của bộ tiêu chuẩn

LỊCH SỬ PHÁT TRIỂN CỦA BỘ TIÊU CHUẨN ISO 27000:2005



Bộ tiêu chuẩn ISO 27000 của JTC1 – SC 27



Xu hướng phát triển của Bộ tiêu chuẩn ISO 27000

- Phát triển và hoàn thiện những tiêu chuẩn cơ bản: 27000 - Cơ sở, từ vựng, 27004 – Đo lường
- Phát triển và hoàn thiện những tiêu chuẩn Hướng dẫn (chung và đặc thù): 27003 – Áp dụng, 27007 – Đánh giá, 27011 – Telecomunication, 27012 – E Government, 27032 - Cybersecurity
- Đưa ra kỹ thuật bảo mật cho mạng – IT network: Bộ tiêu chuẩn 27033-1 cho tới 27033-7

JTC 1/SC 27- IT Security techniques

Standards and projects under the direct responsibility of JTC 1/SC 27 Secretariat

Sort Standard and/or project.	Sort Current stage	Sort ICS
ISO/IEC FDIS 27011 Information technology -- Information security management guidelines for telecommunications organizations based on ISO/IEC 27002	50.60	35.040
ISO/IEC NP 27012 Information technology - Security techniques -- ISM guidelines for e-government services	10.99	35.040
ISO/IEC NP 27032 Guidelines for cybersecurity	10.99	35.040
ISO/IEC NP 27033 Information technology -- IT Network security	10.99	35.040
ISO/IEC CD 27033-1 Information technology -- Security techniques -- IT network security -- Part 1: Guidelines for network security	30.60	35.040
ISO/IEC WD 27033-2 Information technology -- Security techniques -- IT network security -- Part 2: Guidelines for the design and implementation of network security	20.60	35.040
ISO/IEC WD 27033-3 Information technology -- Security techniques -- IT network security -- Part 3: Reference networking scenarios -- Risks, design techniques and control issues	20.60	35.040

Nguồn: ISO/JTC1/SC27

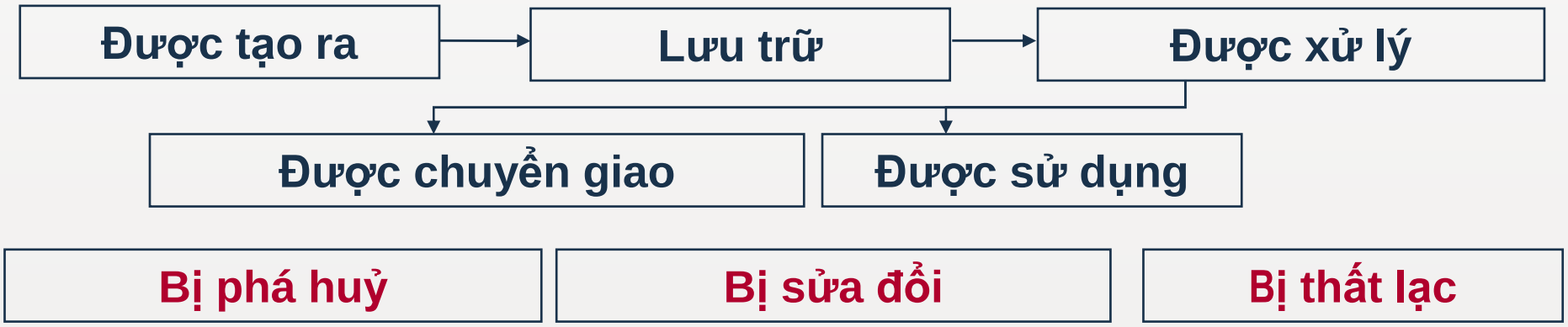
GIỚI THIỆU ISO 27001:2005
& CÁC BƯỚC ÁP DỤNG THỰC TẾ

Thông tin là gì?

Định nghĩa:

- *THÔNG TIN là một loại tài sản, giống như những tài sản kinh doanh quan trọng khác, thông tin có giá trị đối với một tổ chức và do đó cần được BẢO VỆ một cách hợp lý. (ISO/IEC 17799:2000)*

Thông tin có thể:



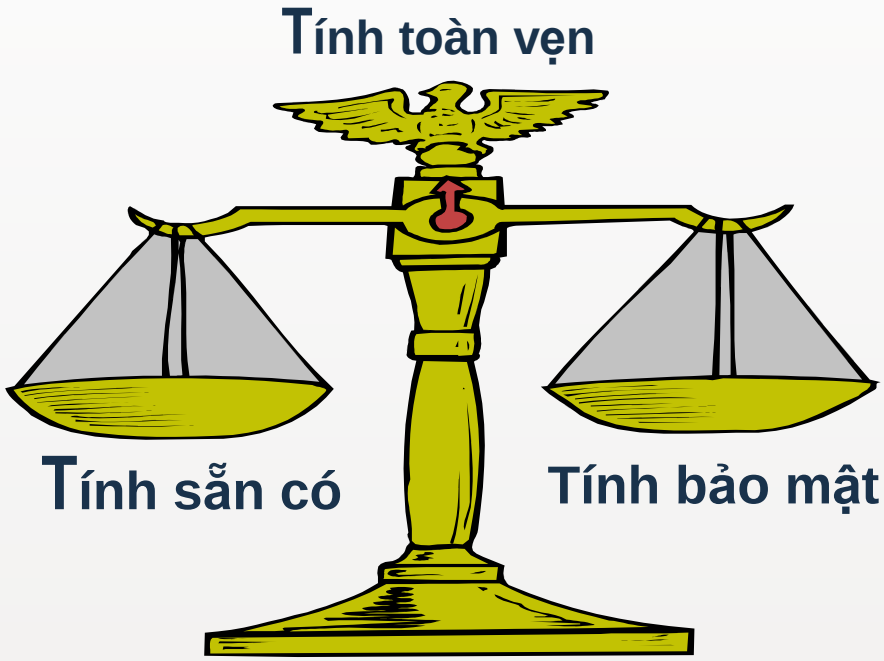
An toàn thông tin là gì?

*CIA (**C**onfidential-**I**ntegrity-**A**vailability):*

- TÍNH BẢO MẬT: Thông tin không sẵn có hoặc không nên để lộ cho cá nhân, tổ chức, đối tượng chưa được uỷ quyền
- TÍNH TOÀN VẸN: Thông tin được bảo vệ và được giữ gìn trọn vẹn
- TÍNH SẴN CÓ: Luôn sẵn sàng và sẵn có sử dụng khi cần cho đối tượng đã được uỷ quyền

(ISO/IEC 27001:2005 – Các yêu cầu)

Các tổ chức cần đạt được sự <u>cân bằng</u>...



"Sự duy trì các thuộc tính: tính bảo mật, tính toàn vẹn và tính sẵn có của thông tin; ngoài ra, các thuộc tính khác như tính xác thực, trách nhiệm giải trình, tính thừa nhận và tính đáng tin cậy cũng có thể liên quan"

Hệ thống quản lý An toàn thông tin - ISMS là gì?

Định nghĩa:

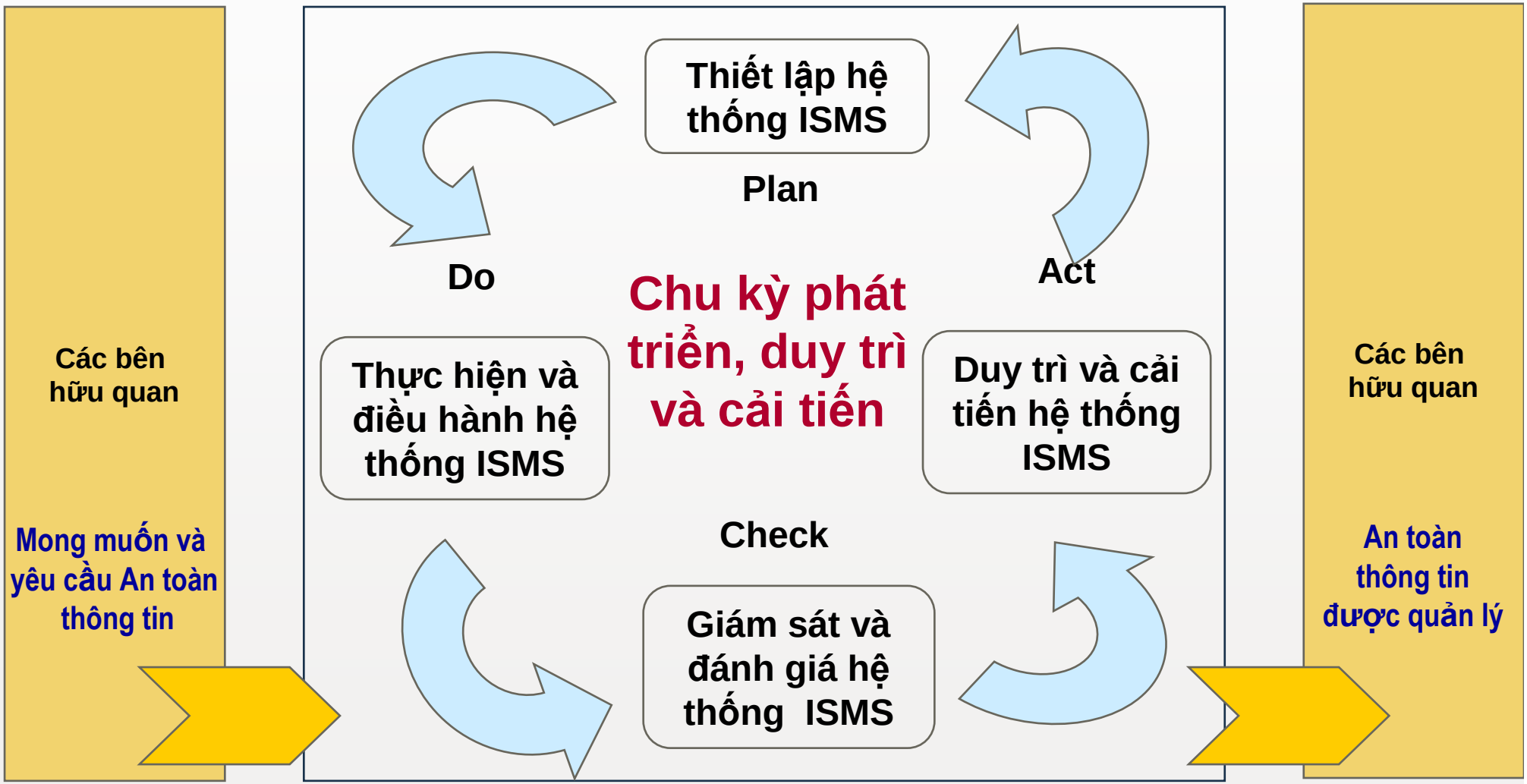
"Hệ thống quản lý an toàn thông tin (ISMS) là một phần của hệ thống quản lý tổng thể, dựa trên cách tiếp cận theo rủi ro của kinh doanh, để thiết lập, thực hiện, điều hành, giám sát, xem xét, duy trì và cải tiến việc bảo mật thông tin"

Ghi chú: hệ thống quản lý bao gồm: cấu trúc của tổ chức, chính sách, các hoạt động hoạch định, trách nhiệm, việc thực hành, thủ tục, qui trình và nguồn lực."

(ISO 27001:2005 cl 3.7)

Nhưng những lợi ích có được là gì?

Giới thiệu ISO 27001:2005



Giới thiệu ISO 27001:2005

- 4 Hệ thống quản lý an toàn thông tin
  - 4.1 Các yêu cầu tổng quát
  - 4.2 Thiết lập và quản lý hệ thống ISMS
  - 4.3 Những yêu cầu về tài liệu
- 5 Trách nhiệm lãnh đạo
  - 5.1 Cam kết của lãnh đạo
  - 5.2 Quản lý các nguồn lực
- 6 Đánh giá nội bộ hệ thống ISMS
- 7 Xem xét lãnh đạo hệ thống ISMS
- 8 Việc cải tiến ISMS
  - 8.1 Cải tiến thường xuyên
  - 8.2 Hành động sửa chữa
  - 8.3 Hành động phòng ngừa

Phụ lục A bao gồm :

- 11 phần:

5. Chính sách ISMS
6. Cơ cấu tổ chức ISMS
7. Quản lý tài sản
8. Bảo mật nguồn nhân lực
9. Bảo mật môi trường vật lý
10. Quản lý hoạt động và truyền thông
11. Kiểm soát truy cập
12. Thu nạp, duy trì và phát triển hệ thống thông tin
13. Quản lý sự cố ISMS
14. Duy trì liên tục hoạt động kinh doanh
15. Tính tuân thủ

- 39 mục tiêu kiểm soát
- 132 mục kiểm soát

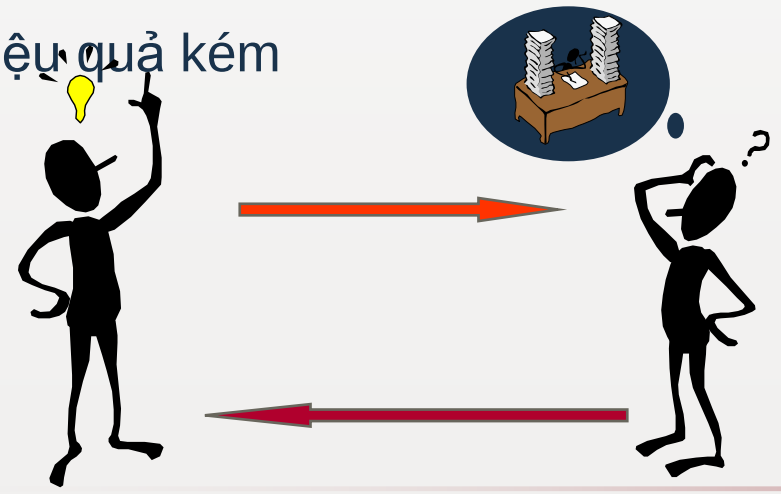

INTERNATIONAL STANDARD
ISO/IEC 27001

Information technology — Security techniques — Information security management systems — Requirements

ISMS theo ISO 27001:2005

Một số "vấn đề" có thể tồn tại của các HTQL vận hành theo tiêu chuẩn quốc tế ISO (9001, 14001, 22000…):

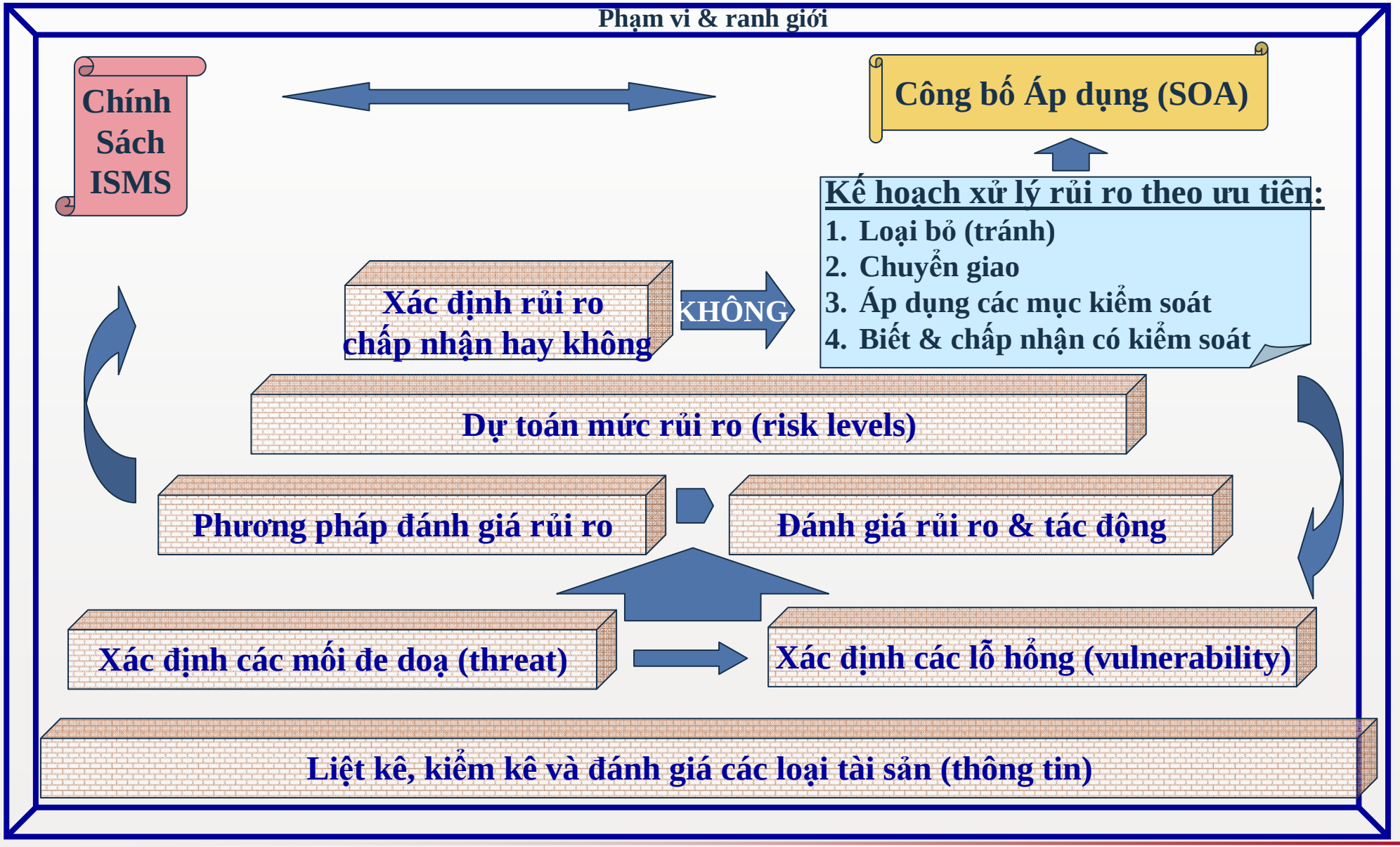
- Phức tạp nhiều hệ thống
- Tốn giấy, tốn công
- Hình thức, không thực tế
- Hiệu quả kém



Tiêu chuẩn này chỉ rõ:

- Mục 0.1 Tổng quan *"Áp dụng ISMS với mức độ tuỳ thuộc vào nhu cầu của tổ chức, nghĩa là **tình huống đơn giản chỉ yêu cầu ISMS đơn giản**"*
- Mục 0.3 Tương thích với các HTQL khác: *"Tiêu chuẩn quốc tế này hoàn toàn tương thích với ISO 9001:2000 và ISO 14001:2004 để hỗ trợ cho việc áp dụng và vận hành tích hợp. **Một HTQL được thiết kế thích hợp có thể thoả mãn tất cả các tiêu chuẩn này**"*
- Mục 1.2 Áp dụng / Chú thích: *"**Dùng HTQL hiện có** để thoả mãn các yêu cầu của tiêu chuẩn này sẽ tốt hơn trong đa số các trường hợp"*

Xây dựng ISMS theo ISO 27001:2005

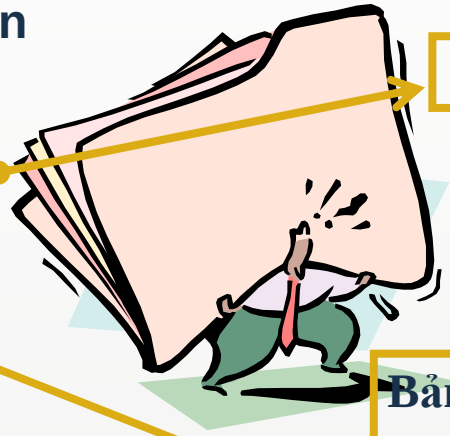


SO SÁNH VỚI HTQL HIỆN CÓ (ISO 9001:2008)

ISO 27001:2005

- 4 Hệ thống quản lý an toàn thông tin
  - 4.1 Các yêu cầu tổng quát
  - 4.2 Thiết lập và quản lý hệ thống ISMS
  - 4.3 Những yêu cầu về tài liệu
- 5 Trách nhiệm lãnh đạo
  - 5.1 Cam kết của lãnh đạo
  - 5.2 Quản lý các nguồn lực
- 6 Đánh giá nội bộ hệ thống ISMS
- 7 Xem xét lãnh đạo hệ thống ISMS
- 8 Việc cải tiến ISMS
  - 8.1 Cải tiến thường xuyên
  - 8.2 Hành động sửa chữa
  - 8.3 Hành động phòng ngừa

HTQL hiện có (hay ISO 9001:2000)



Xem trang trước

Bảng so sánh tương đồng giữa 9001/14001&27001:

4.2.3 &4.2.4
5.1 & 5.2
6.2
8.2.2
5.6
8.5.1
8.5.2
8.5.3

Giới thiệu ISO 27001:2005

Phụ lục A bao gồm :

- **11 phần:**

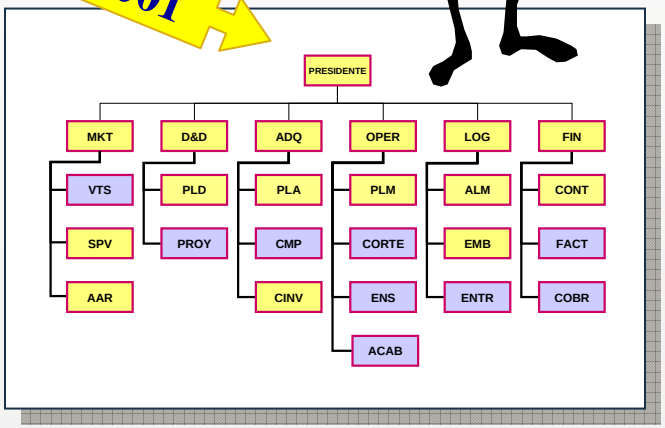
5. Chính sách ISMS
6. Cơ cấu tổ chức ISMS
7. Quản lý tài sản
8. Bảo mật nguồn nhân lực
9. Bảo mật môi trường vật lý
10. Quản lý hoạt động và truyền thông
11. Kiểm soát truy cập
12. Thu nạp, duy trì và phát triển hệ thống thông tin
13. Quản lý sự cố ISMS
14. Duy trì liên tục hoạt động kinh doanh
15. Tính tuân thủ

- **39 mục tiêu kiểm soát**
- **132 biện pháp** Kiểm soát

Giống ISO 9001

Tương tự ISO 9001

Mới so với ISO 9001 nhưng bài bản



Các tổ chức chuyên môn

Khách hàng

Các bên cung cấp thứ Ba

Kiểm kê – Có chủ - Phân loại – Nhãn - QĐ sử dụng

Giới thiệu ISO 27001:2005

Phụ lục A bao gồm :

Nhân viên/nhà thầu/bên thứ 3 – trước/trong/sauHĐ

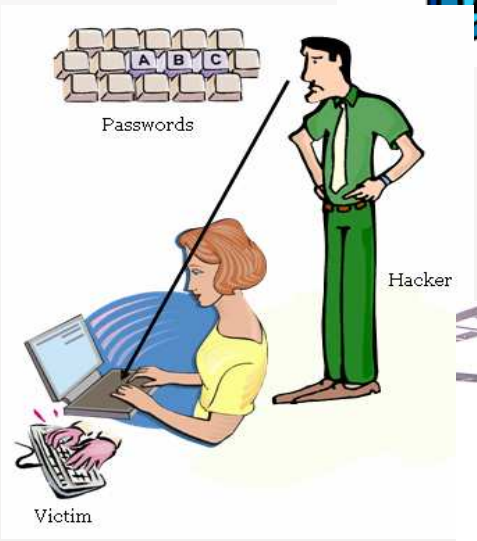
- **11 phần:**

5. Chính sách ISMS
6. Cơ cấu tổ chức ISMS
7. Quản lý tài sản
8. **Bảo mật nguồn nhân lực**
9. **Bảo mật môi trường vật lý**
10. **Quản lý hoạt động và truyền thông**
11. Kiểm soát truy cập
12. Thu nạp, duy trì và phát triển hệ thống thông tin
13. Quản lý sự cố ISMS
14. Duy trì liên tục hoạt động kinh doanh
15. Tính tuân thủ

- **39 mục tiêu kiểm soát**
- **132 biện pháp** Kiểm soát

Tương tự ISO 9001

Tương tự ISO 9001



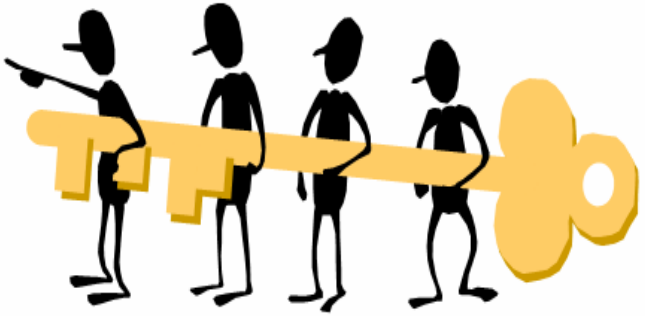
Giới thiệu ISO 27001:2005

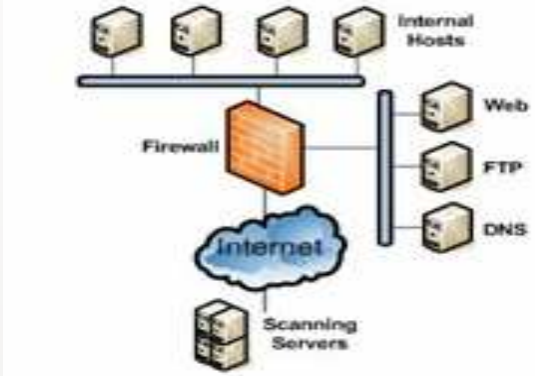
Phụ lục A bao gồm :

- **11 phần:**

5. Chính sách ISMS
6. Cơ cấu tổ chức ISMS
7. Quản lý tài sản
8. Bảo mật nguồn nhân lực
9. Bảo mật môi trường vật lý
10. Quản lý hoạt động và truyền thông
11. **Kiểm soát truy cập**
12. **Thu nạp, duy trì và phát triển hệ thống thông tin**
13. **Quản lý sự cố ISMS**
14. **Duy trì liên tục hoạt động kinh doanh**
15. **Tính tuân thủ**

- **39 mục tiêu kiểm soát**
- **132 biện pháp** Kiểm soát





ÍCH LỢI

Lợi ích của an toàn thông tin

- Bảo vệ tài sản thông tin một cách thích hợp
  - Kiểm soát dựa trên rủi ro
  - Không bị Thiếu / Thừa
- Lợi thế cạnh tranh
- Sự tuân thủ pháp luật
- Hình ảnh
- Lợi nhuận

- Thành lập nền tảng vững chắc cho chính sách bảo mật thông tin
- Là bằng chứng thấy được về những thực hành được áp dụng cho các bên quan tâm:
  - Các khách hàng thương mại
  - Khách hàng là người sử dụng cuối cùng
  - Đối với nhân viên (kiểm toán)
  - Đối với các cơ quan quản lý

BUREAU VERITAS CERTIFICATION VIETNAM

- Phát hành 2000 Giấy chứng nhận phù hợp với các tiêu chuẩn quốc tế cho các HTQL
- Phù hợp ISO 17021:2006 & được chuyển thành Trung tâm chứng nhận (ICC) từ tháng 9 năm 2008
  - Quyết định chứng nhận với công nhận của UKAS & ANAB.
  - Kịp thời hơn với nhu cầu khách hàng
- Có chuyên gia đánh giá người Việt Nam
- Khách hàng tiêu biểu tại Việt Nam ISO 27001:2005–UKAS công nhận
  - YKK.
  - BKIS


BUREAU VERITAS
Certification

Certification

Awarded to

EAST JAPAN RAILWAY COMPANY

Bureau Veritas certify that the Management System of the above organisation has been audited and found to be in accordance with the requirements of the management system standards detailed below

STANDARDS

ISO 14001:2004

SCOPE OF SUPPLY

MARKETING AND SALES, DESIGN AND ENGINEERING, MANUFACTURING, AFTER SALE AND IN SERVICE SUPPORT OF AIRCRAFT AND ALL AERONAUTIC PRODUCTS AND SERVICES.

Original Approval Date:

Subject to the continued satisfactory operation of the organisation's Management System, this certificate is valid from: 08 February 2005

To check this certificate validity please call +85 78 272 2600

Further clarifications regarding the scope of this certificate and the applicability of the management system requirements may be obtained by consulting the organisation

Certificate Number: Date:

Bureau Veritas Certification using the accreditation certificate number 008

BUREAU
VERITAS

Move Forward with Confidence