CƠ SỞ AN TOÀN THÔNG TIN

Bài 02. Hiểm họa an toàn thông tin

1. Khái niệm hiểm họa ATTT
2. Phân loại hiểm họa ATTT
3. Nguyên tắc đảm bảo an toàn thông tin
4. Phương pháp chung đảm bảo an toàn thông tin

1. Khái niệm hiểm họa ATTT
2. Phân loại hiểm họa ATTT
3. Nguyên tắc đảm bảo an toàn thông tin
4. Phương pháp chung đảm bảo an toàn thông tin

Các khái niệm khác

Hiểm họa (Threat)

Lỗ hổng (Vunerability)

Điểm yếu (Weakness, Gap)

Rủi ro (Risk)

"Đã yếu lại còn ra gió"

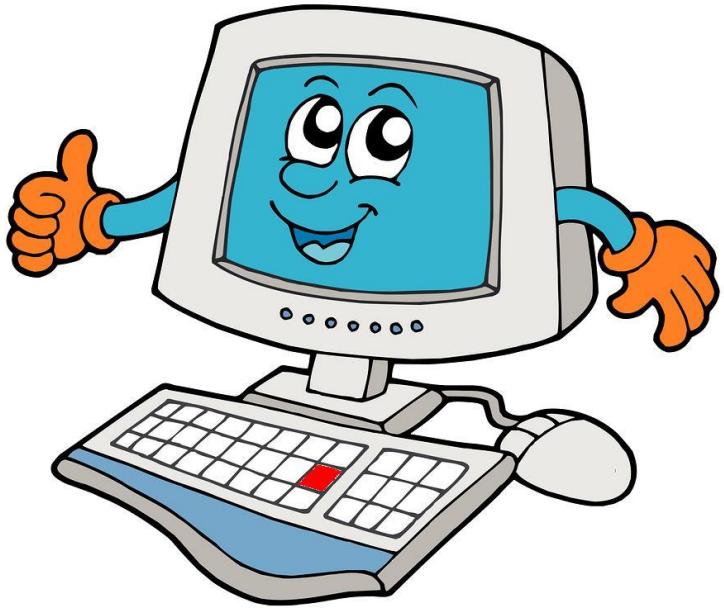
- Nếu không có gió thì không bị ốm

  ➔ Nếu hiểm họa không xảy ra thì không có rủi ro

- Nếu sức khỏe tốt thì không bị ốm

  ➔ Nếu không có điểm yếu thì không có rủi ro

Hiểm họa an toàn thông tin



- Điểm yếu: không có UPS
- Hiểm họa: mất điện
- Rủi ro: - mất dữ liệu
  - hỏng ổ cứng

Hiểm họa

- **Hiểm họa ATTT** của HTTT là những **khả năng tác động** lên TT, HTTT dẫn tới sự thay đổi, hư hại, sao chép, sự ngăn chặn tiếp cận tới TT; tới sự phá huỷ hoặc sự ngừng trệ hoạt động của vật mang TT.
- **Ví dụ**: virus, động đất, tấn công mạng

Hiểm họa an toàn thông tin

Lỗ hổng

- **Lỗ hổng** của HTTT là những **khiếm khuyết trong chức năng, thành phần**

Một lỗ hổng có thể bị khai thác bởi nhiều hiểm họa khác nhau

  - Không có UPS

Điểm yếu ≠ Lỗ hổng

❑Lỗ hổng (Vulnerability)

- thực tế đã bị khai thác
- https://cve.mitre.org/
- CVE = Common Vulnerabilities and Exposures

❑Điểm yếu (Weakness)

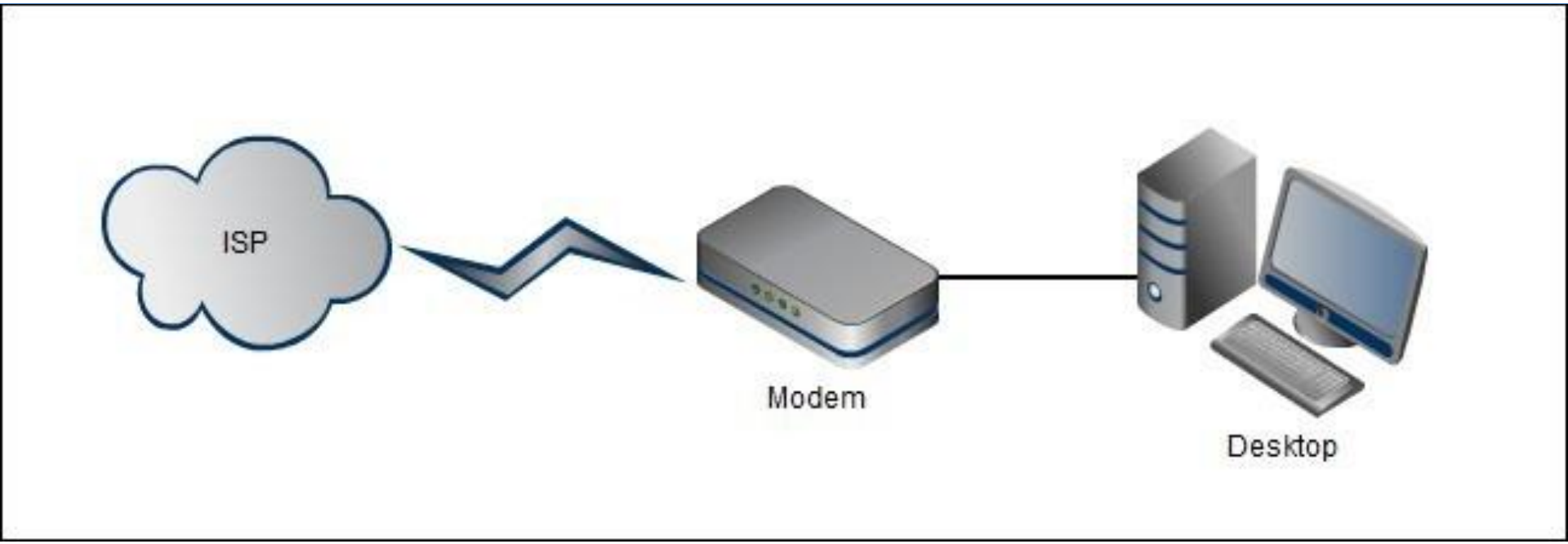
- Có thể bị khai thác
- https://cwe.mitre.org/
- CWE = Common Weakness Enumeration

Hiểm họa an toàn thông tin

Rủi ro

- **Rủi ro** của HTTT là những **khả năng xấu** có thể xảy ra đối với hệ thống.
- **Ví dụ**:
  - Rủi ro lộ bí mật
  - Rủi ro mất dữ liệu
  - Rủi ro hỏng thiết bị

Hiểm họa an toàn thông tin



Hãy chỉ ra một số bộ

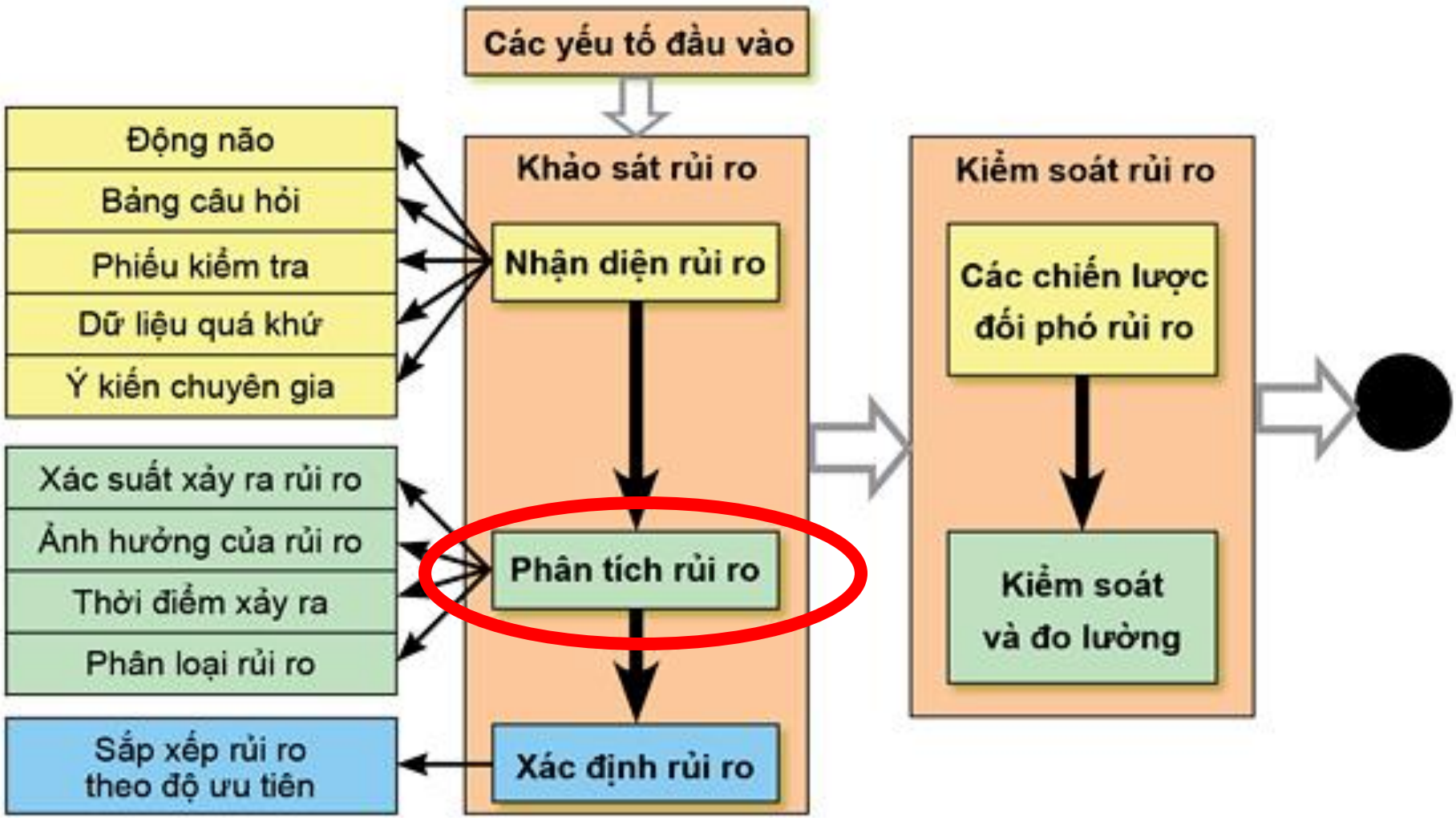
(Điểm yếu, Hiểm họa, Rủi ro)

1. Khái niệm hiểm họa ATTT
2. Phân loại hiểm họa ATTT
3. Nguyên tắc đảm bảo an toàn thông tin
4. Phương pháp chung đảm bảo an toàn thông tin

Hiểm họa

- **Hiểm họa ATTT** của HTTT là những **khả năng tác động** lên TT, HTTT dẫn tới sự thay đổi, hư hại, sao chép, sự ngăn chặn tiếp cận tới TT; tới sự phá huỷ hoặc sự ngừng trệ hoạt động của vật mang TT.
- **Ví dụ**: virus, động đất, tấn công mạng

Vai trò của phân loại hiểm họa



Phân loại hiểm họa an toàn thông tin

❑Theo bản chất xuất hiện

- Hiểm họa tự nhiên: thiên tai, mối mọt, ẩm mốc,...
- Hiểm họa nhân tạo: phá hoại, thao tác sai,...

Phân loại hiểm họa an toàn thông tin

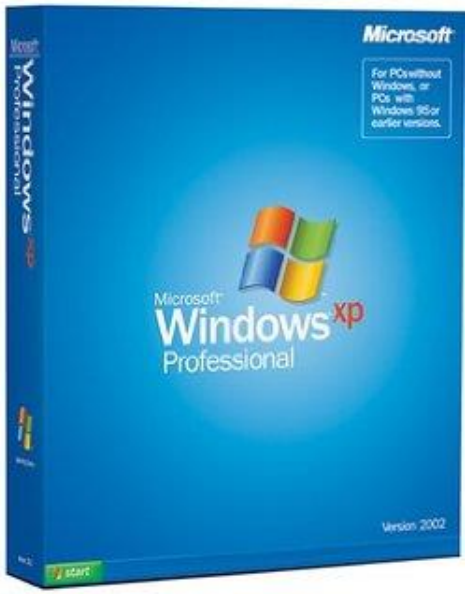
❑Theo mức độ định trước

- Hiểm họa từ hành động vô ý
- Hiểm họa từ hành động có chủ ý

Phân loại hiểm họa an toàn thông tin

❑Theo nguồn trực tiếp sinh ra

- Nguồn sinh trực tiếp là con người
- Nguồn sinh là các phần mềm hợp lệ
- Nguồn sinh là các phần mềm trái phép



Phân loại hiểm họa an toàn thông tin

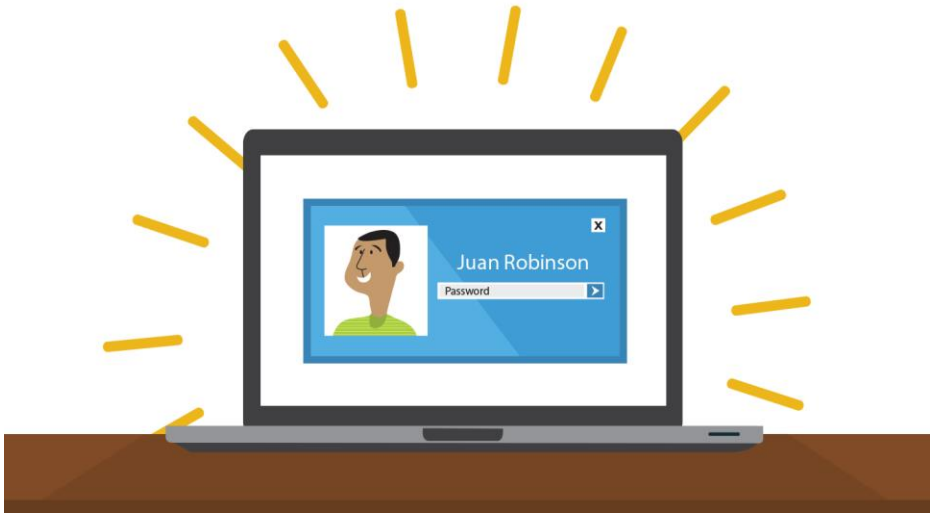
❑Theo vị trí của nguồn sinh ra

- **Vùng 1**: Phạm vi cơ quan, đơn vị, tổ chức...
- **Vùng 2**: Phạm vi tòa nhà
- **Vùng 3**: Phòng chờ, lễ tân, trực ban
- **Vùng 4**: Phòng họp, phòng làm việc của cán bộ, nhân viên...
- **Vùng 5**: Những khu vực đặc biệt quan trọng, phòng của lãnh đạo,...
- **Vùng 6**: Tủ chứa tài liệu, két sắt, cơ sở dữ liệu...

Phân loại hiểm họa an toàn thông tin

❑Theo mức độ hoạt động của HTTT

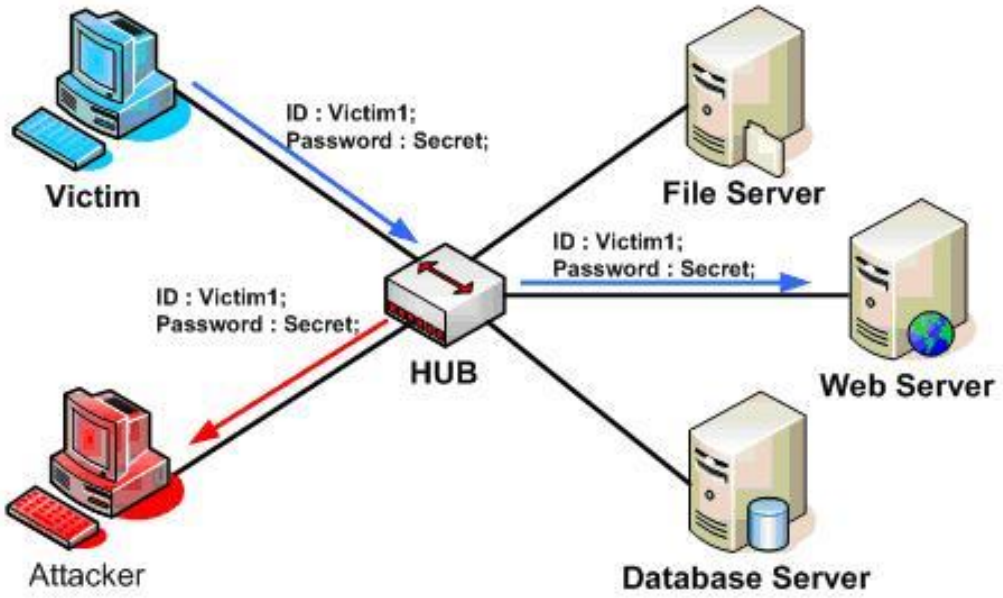
- Không phụ thuộc vào hoạt động của hệ thống
- Chỉ xuất hiện khi hệ thống hoạt động



Phân loại hiểm họa an toàn thông tin

❑Theo mức độ tác động lên HTTT

- Hiểm họa thụ động, không làm thay đổi cấu trúc, nội dung của hệ thống
- Hiểm họa tích cực, gây ra những thay đổi nhất định trong hệ thống



Hiểm họa an toàn thông tin

Xác định danh sách hiểm họa đối với HTTT là khâu quan trọng trong đảm bảo ATTT cho hệ thống, bởi nó cho biết cần phải áp dụng những biện pháp bảo vệ nào!

Một số hiểm họa cụ thể

- Hiểm họa ngẫu nhiên: sai sót của con người, tác động của tự nhiên
- Trộm cắp
- Mã độc
- Truy cập trái phép
- Tấn công từ chối dịch vụ
- Lừa đảo

1. Khái niệm hiểm họa ATTT
2. Phân loại hiểm họa ATTT
3. Nguyên tắc đảm bảo an toàn thông tin
4. Phương pháp chung đảm bảo an toàn thông tin

Nguyên tắc đảm bảo ATTT

1. Nguyên tắc tính hệ thống

- Các yếu tố, các điều kiện và các nhân tố có quan hệ với nhau, có tương tác với nhau và có biến đổi theo thời gian
- Chống lại cả những kênh truy cập trái phép tiềm tàng (chưa biết)

Nguyên tắc đảm bảo ATTT

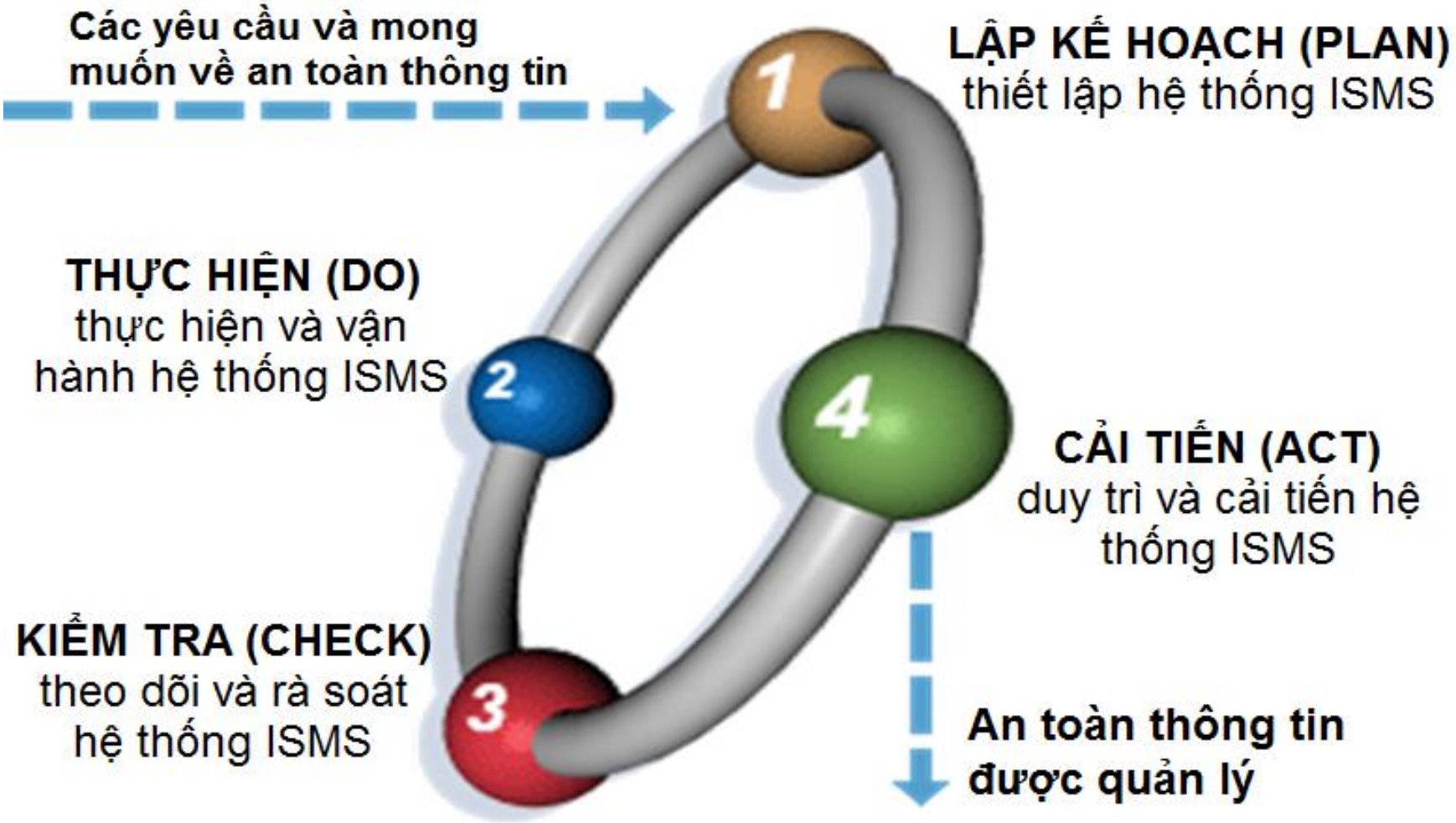
2. Nguyên tắc tổng thể

- Các biện pháp phải thống nhất, đồng bộ
- Phải tổ chức phòng ngự nhiều lớp

3. Nguyên tắc bảo vệ liên tục

- Đảm bảo ATTT là quá trình liên tục
- Xuyên suốt chu kỳ sống của hệ thống, từ thiết kế cho đến loại bỏ

Mô hình PDCA của ISO 27001



Nguyên tắc đảm bảo ATTT

4. Nguyên tắc đầy đủ hợp lý

- Không có an toàn tuyệt đối
- Biện pháp bảo vệ có ảnh hưởng ít nhiều đến hoạt động của hệ thống
- Biện pháp bảo vệ thường tốn kém
- Chi phí cho việc bảo vệ không lớn hơn giá trị của hệ thống
- Mục tiêu của bảo vệ là đưa rủi ro về mức chấp nhận được

Nguyên tắc đảm bảo ATTT

5. Nguyên tắc mềm dẻo hệ thống

- Phân hệ an toàn được thiết lập trong điều kiện có nhiều bất định
- Phải cho phép nâng cấp, cập nhật

6. Nguyên tắc đơn giản trong sử dụng

- Cơ chế bảo vệ không được gây khó khăn cho người dùng hợp lệ

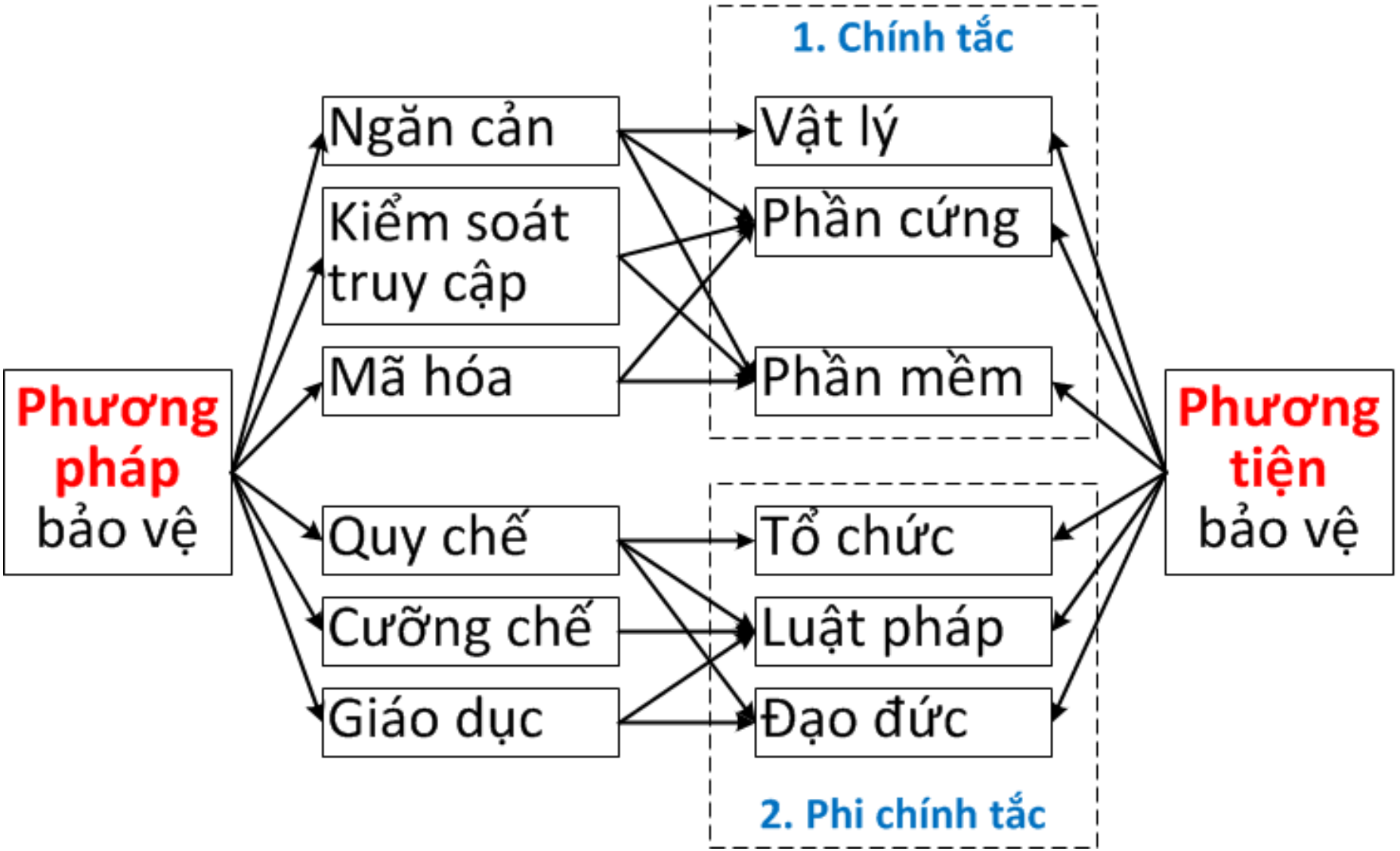
Nguyên tắc đảm bảo ATTT

7. Nguyên tắc công khai thuật toán và cơ chế bảo vệ

- Biết được thuật toán, cơ chế bảo vệ cũng không thể vượt qua được
- Chính tác giả cũng không thể vượt qua
- Không có nghĩa là phải công khai thuật toán và cơ chế bảo vệ

1. Khái niệm hiểm họa ATTT
2. Phân loại hiểm họa ATTT
3. Nguyên tắc đảm bảo an toàn thông tin
4. Phương pháp chung đảm bảo an toàn thông tin

Phương pháp bảo vệ thông tin



Phương pháp bảo vệ thông tin

- **Ngăn cản**: không cho phép tiếp cận khu vực được bảo vệ
- **Kiểm soát truy cập**: điều khiển, kiểm soát mọi thành phần của hệ thống
- **Mật mã (che giấu)**: biến đổi thông tin về dạng khác

Phương pháp bảo vệ thông tin

- **Quy chế**: đưa ra các quy tắc xác định những việc mà con người được làm, không được làm, phải làm
- **Cưỡng chế**: gắn liên với quy chế; là việc đưa vào những cơ chế mà khiến con người phải thực hiện đúng theo quy tắc đã định
- **Giáo dục**: tác động lên ý thức, đạo đức của con người

Phương tiện bảo vệ thông tin

- **Phương tiện chính tắc (formal)**: thực hiện các chức năng bảo vệ theo đúng các thủ tục được xác định trước mà không cần sự can thiệp của con người
- **Phương tiện phi chính tắc (informal)**: quy định hành vi của con người

http://f.tqn.com/y/jobsearch/1/W/J/7/1/185275200.jpg