TRƯỜNG ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN - VNUHCM - UIT

QUẢN LÝ RỦI RO AN TOÀN THÔNG TIN TRONG DOANH NGHIỆP

Tóm tắt Chương 3
Mục đích của quản lý rủi ro…
"The purpose of risk management is the creation and protection of value"

Mục đích của quản lý rủi ro

The purpose of risk management is the creation and protection of value.

Mục đích của quản lý rủi ro là tạo ra và bảo vệ giá trị.

Minh họa Mục đích của quản lý rủi ro(1)

Ví dụ 1:

Mối đe dọa: Sao chép tập tin có dung lượng lớn

Điểm yếu: thiết bị lưu trữ (‘HDD’) còn ít dung lượng trống

Rủi ro tiềm ẩn: việc sao chép tập tin bị thất bại (‘uncompleted’)

Để tránh rủi ro này, phải làm gì?

>>> Phải quản lý rủi ro bằng cách tạo ra giá trị (‘value’) nào đó

Minh họa Mục đích của quản lý rủi ro(2)

>>> Quản lý rủi ro bằng cách tạo ra giá trị (‘value’) 8%!!

Thiết lập Biện pháp kiểm soát (‘control’) như sau:

Nếu dung lượng trống của HDD chỉ còn ~ 8% thì hệ điều hành của máy tính phải cảnh báo cho người dùng. Giá trị 8% sẽ giúp người dùng từ bỏ việc sao chép tập tin, thay vào đó, người này xóa các tập tin trên HDD để tăng dung lượng trống cho HDD trước khi sao chép. Hãng Microsoft lập giá trị 8% và bảo vệ tính toàn vẹn của dữ liệu khi sao chép để QLRR cho người dùng khi sao chép tập tin.

Minh họa Mục đích của quản lý rủi ro(3)

Ví dụ 2:

- Mối đe dọa: Nhiệt độ chip xử lý (CPU) tăng cao khi máy tính vận hành với tác vụ lớn có cường độ cao v.v.

- Điểm yếu: Chip xử lý không thể hoạt động ở mọi nhiệt độ.

- Rủi ro tiềm ẩn: Máy tính có thể ngừng hoạt động khi CPU quá nóng.

>>> Biện pháp QLRR: Intel sản xuất chip xử lý hoạt động trong điều kiện nhiệt độ ≤ 70 độ C *(:tạo giá trị)***. Để bảo vệ chip khi nhiệt độ gần đạt tới giá trị này, hãng Intel đã cải tiến kiến trúc chip, công nghệ vật liệu, quạt làm mát v.v. để làm mát cho chip xử lý.**

Minh họa Mục đích của quản lý rủi ro(4)

Ví dụ 3:

- Mối đe dọa: Sự phát sinh dữ liệu lưu vào cơ sở dữ liệu (MS Access, MS SQL, Oracle, MySQL…) gia tăng theo thời gian.
- Điểm yếu: Độ lớn tập tin (‘size’) cơ sở dữ liệu (‘database’) có giới hạn.
- Rủi ro tiềm ẩn: Tác vụ sao chép dữ liệu vào cơ sở dữ liệu có thể thất bại khi độ lớn (‘size’) tập tin cơ sở dữ liệu vượt quá một giá trị nào đó.

>>> Biện pháp QLRR: Hãng Microsoft tạo giá trị độ lớn ("size") của tập tin MS Access ≤ 2GB. Khi tập tin CSDL gần đạt giá trị này, ứng dụng MS Access sẽ thông báo / cảnh báo trước cho người dùng thay đổi nơi sao chép đến (‘destination’) để tác vụ sao chép không bị thất bại hoặc làm hỏng (corrupt) tệp dữ liệu của khách hàng bên cạnh việc nén tập tin, xóa rác trong tập tin, ...

Minh họa Mục đích của quản lý rủi ro(5)

Ví dụ 4:

- Mối đe dọa: Nguồn cung điện lưới không liên tục (ổn định) vào giờ cao điểm.
- Điểm yếu: Không có nguồn điện dự phòng và không có cơ chế ATS.
- Rủi ro tiềm ẩn: Người dùng có thể mất dữ liệu khi máy tính mất điện đột ngột.

>>> Biện pháp QLRR: Doanh nghiệp thiết lập giá trị 15 phút duy trì nguồn điện cho thiết bị xử lý thông tin ('PC, servers, POS, terminal..') nếu xảy ra mất điện lưới bằng cách trang bị UPS với thời gian duy trì điện là 15 phút. Doanh nghiệp có thể kịp sao lưu dữ liệu đầy đủ và đạt RTO (Recovery Time Object) = 0. Để bảo vệ bảo vệ giá trị thời gian duy trì điện 15 phút, doanh nghiệp không đấu nối tải vào UPS quá công suất thiết kế của UPS.

Minh họa Mục đích của quản lý rủi ro(6)

Ví dụ 5:

- **Mối đe dọa: Sức hút của trái đất vào cơ thể con người.**
- **Điểm yếu: Cơ thể người chịu va đập rất kém.**
- **Rủi ro tiềm ẩn: Người làm việc trên cao có thể bị thương tật hoặc tử vong nếu té ngã xuống đất từ trên cao.**

>>> Biện pháp QLRR: Chính phủ TQ có quy định bất kỳ công việc nào được thực hiện ở độ cao từ 2 mét trở lên *(:tạo giá trị)* **so với mặt đất đều được coi là** ***"làm việc trên cao"*****. Người "làm việc trên cao" phải có chứng chỉ hành nghề và được trang bị mũ bảo hộ, dây đai an toàn,... trong khi làm việc, nếu không sẽ bị coi là vi phạm về an toàn lao động hay vi phạm pháp luật** *(tức là bảo vệ giá trị 2 mét trên)*.

Minh họa Mục đích của quản lý rủi ro(7)

Ví dụ 6:

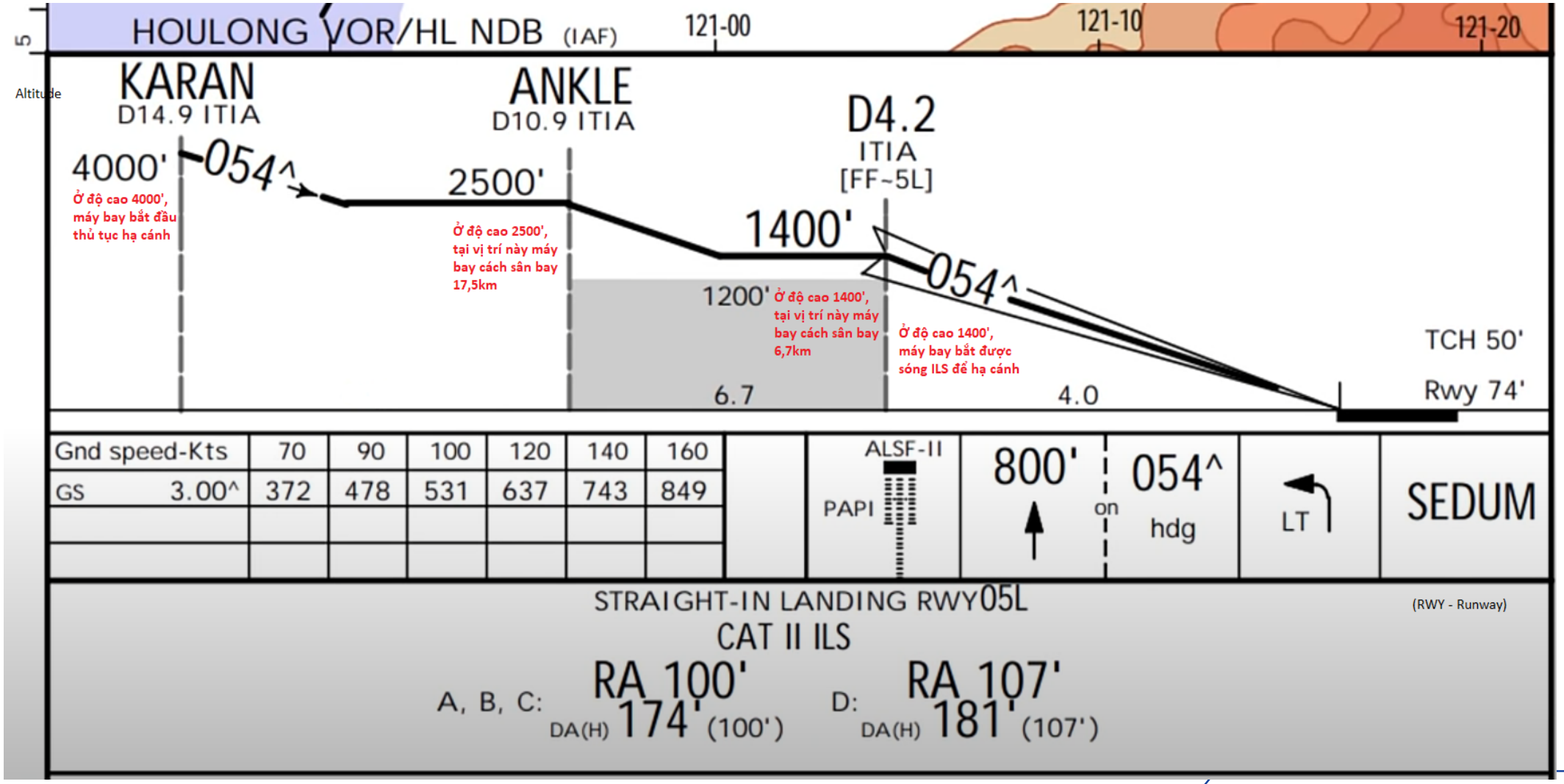
Tính huống: máy bay ở giai đoạn hạ độ cao và hạ cánh theo phương thức ILS.

- **Mối đe dọa: Sự cố xảy ra cho máy bay.**
- **Điểm yếu: Có rất ít thời gian để phi công xử lý. Nếu sự cố xảy ra khi máy bay vừa chạm mặt đất, phi công gần như không có thời gian để quyết định cũng như điều khiển sao cho máy bay (*"con quái vật"* nặng 88 tấn) dừng lại. (*)**
- **Rủi ro tiềm ẩn: sự kém năng lực của phi công / lỗi thiết bị bay / thời tiết xấu hay lỗi nghiêm trọng khác có thể làm cho sự cố nghiêm trọng hơn hay không thể khắc phục được sự cố.**

>>> Biện pháp QLRR: Trước khi bắt được sóng dẫn đường hạ cánh, phi công phải đưa máy bay vào đường hạ cánh 4000' – 2500' – 1400' - xem hình 3

Minh họa Mục đích của quản lý rủi ro(8)

Ví dụ 6: *(tiếp) Hình 3* (*)



Minh họa Mục đích của quản lý rủi ro(9)

Ví dụ 7:

Tính huống: Một khách hàng mua cà phê ở McDonald's. Khi lái xe, họ kẹp ly cà phê giữa đùi. Cà phê đổ, người mua bị bỏng do cà phê quá nóng. Họ đi kiện McDonald's và thắng kiện 2 triệu USD.

- **Mối đe dọa: Cà phê pha giao cho khách mang về đang ở nhiệt độ cao hơn nhiệt độ gây bỏng là 56^oC.**
- **Điểm yếu: Vật chứa nước (ví dụ ly, cốc, bình,…) không đủ kín**

Minh họa Mục đích của quản lý rủi ro(9)

Ví dụ 7: (…)

- **Rủi ro tiềm ẩn: Cửa hàng có thể gặp rủi ro danh tiếng và an toàn nếu có khách hàng kiện cửa hàng do họ có thể bị bỏng khi cà phê đổ vào người.**

>>> Biện pháp QLRR (cho cả cửa hàng và cho khách): Khi khách hàng mua café pha sẵn và mang đồ uống nóng có nhiệt độ >=56°C () *(:tạo giá trị)* ra khỏi cửa hàng, người bán của cửa hàng phải:

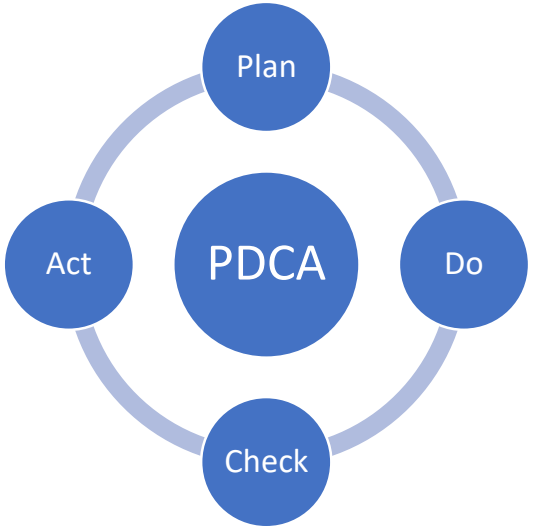
(1) đặt ly café vào các túi chứa (hay bình chứa) cách nhiệt *(:bảo vệ giá trị)* và kín để khi café bị đổ thì không chảy ra ngoài; hoặc

(2)yêu cầu khách ký giấy cam kết tự chịu trách nhiệm khi mang ly café ra khỏi cửa hàng và bị thương tích do đổ café vào người./.

Cải tiến liên tục (Continual improvement)(1)

ÁP DỤNG CHU TRÌNH PDCA (CHU TRÌNH DEMING) ĐỂ CẢI TIẾN

- (**P**LAN) – Hoạch định các bước cải tiến
- (**D**O) – Thực hiện công việc cải tiến
- (**C**HECK) – Kiểm tra kết quả cải tiến
- (**A**CT) – Thực hiện hành động khắc phục



Cải tiến liên tục (Continual improvement)(2)

- QLRR được cải tiến liên tục thông qua:

Tạo giá trị(*) > Đo lường > Phân tích > Quản lý > Kiểm soát > Cải tiến

Creat value(*) > Measure > Analyse > Manage > Control > Improve

- **K**hi nghĩ về CẢI TIẾN, phải tạo ra giá trị trước và ghi nhớ:

  If you can't measure it, you can't ***analyse*** it (*Nếu không thể đo lường thì không thể phân tích*);

  If you can't analyse it, you can't ***manage*** it (*Nếu không thể phân tích thì không thể quản lý*);

  If you can't manage it, you can't ***control*** it (*Nếu không thể quản lý thì không thể kiểm soát*);

  If you can't control it, you can't ***improve*** it (*Nếu không thể kiểm soát thì không thể cải tiến).*

(*) Giá trị ('value') là một con số ('number') nào đó có thể đo lường được mà sinh viên phải tạo ra (hay nghĩ ra) khi làm bài tập Chương 3. Có đo lường được con số này mới phân tích, quản lý, kiểm soát và cải tiến.

Hết Tóm tắt Ôn bài Chương 03

Cám ơn tất cả Anh/Chị đã theo dõi nội dung này

(*)Một số hình minh họa được tải từ trang https://www.pexels.com/ và https://pixabay.com/