QUẢN LÝ RỦI RO AN TOÀN THÔNG TIN TRONG DOANH NGHIỆP

Chương 3
Các nguyên tắc quản lý rủi ro

Nội dung

01 **Mục đích quản lý rủi ro (QLRR)**

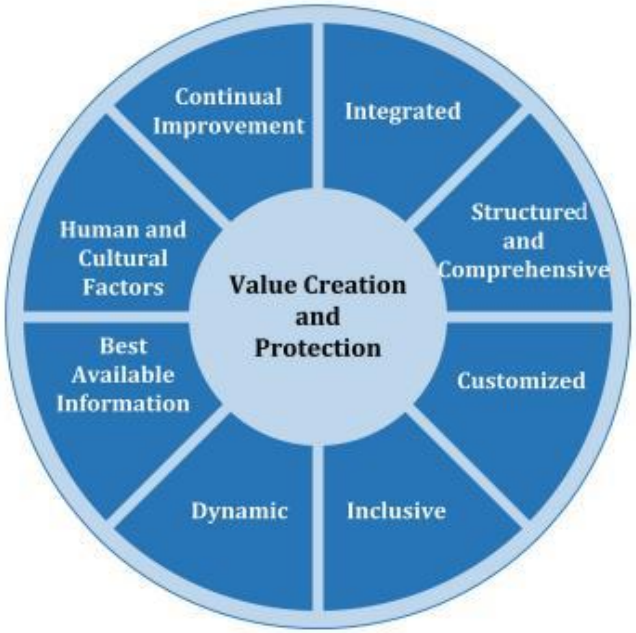
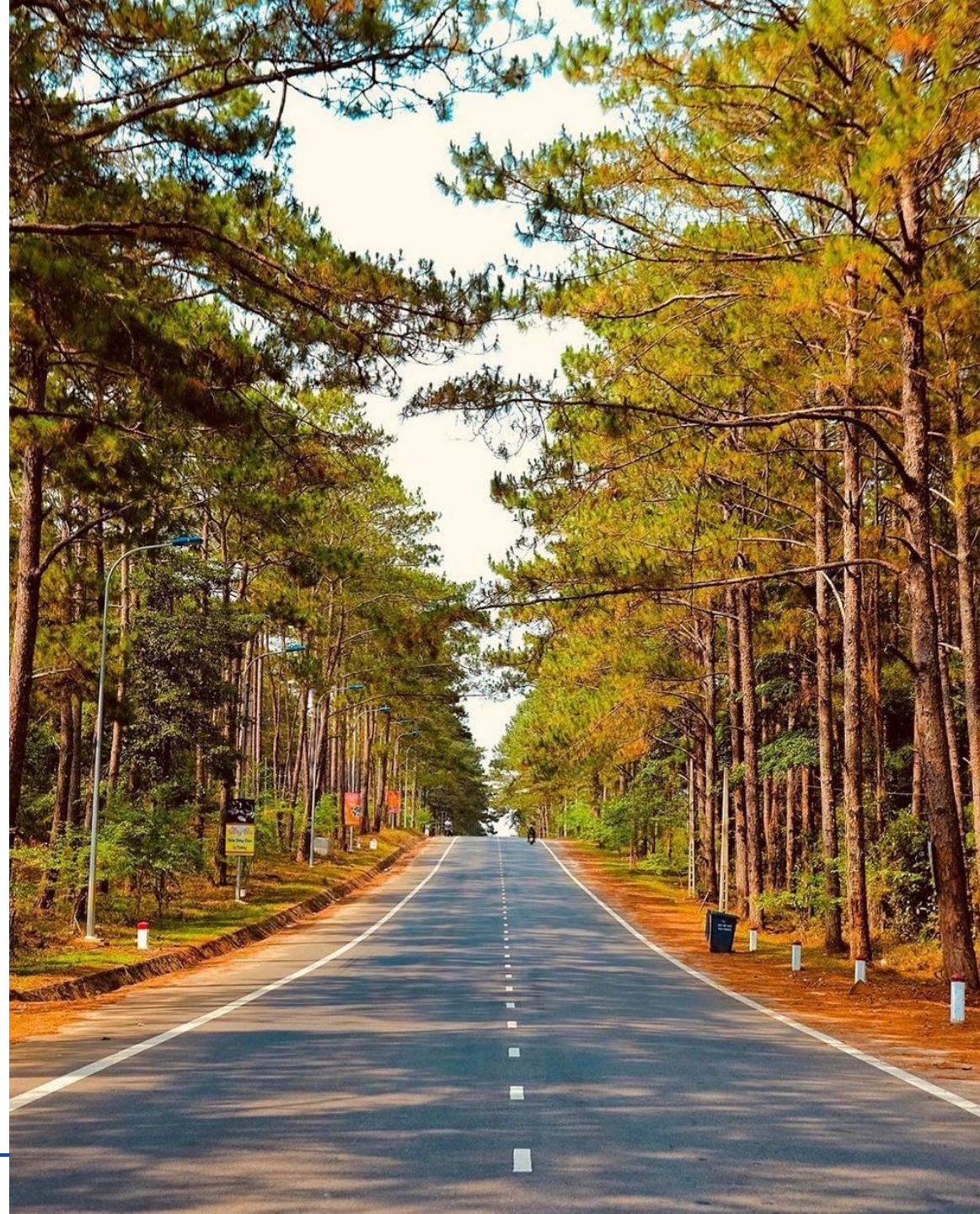


Figure 2 — Principles

02 **Các nguyên tắc quản lý rủi ro (QLRR)**

01

Mục đích quản lý rủi ro (QLRR)



GIÁ TRỊ - TẠO RA GIÁ TRỊ

- **Focus on Value**: The process involves identifying what truly adds **value** to the product or service and discarding what doesn't. [Elon Musk]
- The foundation of any successful business lies in delivering exceptional **value**…[Elon Musk]
- ***'Tạo ra giá trị…'*** **-** KhanTQ_TaoGiaTri-khi-XinViecLam.mp4

Mục đích quản lý rủi ro (QLRR)(1)

- **The purpose of risk management is <u>the creation and protection of value</u>.**
- **It improves performance, encourages innovation and supports the achievement of objectives.**

  [ISO 31000:2018]

Mục đích quản lý rủi ro (QLRR)(2)

- **<u>Mục đích</u> của quản lý rủi ro là:**
- **tạo ra giá trị; và**
- **bảo vệ giá trị (‘value’) -** [ISO 31000]
- **Quản lý rủi ro giúp cải thiện hiệu suất (‘performance’), khuyến khích sự đổi mới (‘innovation’) và hỗ trợ việc đạt được các mục tiêu (‘objectives’).**

Mục đích quản lý rủi ro (QLRR)(3)

Ví dụ: Nhà sản xuất quản lý rủi ro để tạo ra giá trị cho hiệu suất vận hành

PC và Laptop có thể gặp rủi ro vận hành (ngưng làm việc) trong quá trình sử dụng. Để quản lý rủi ro này cho người bán và khách hàng (người mua), nhà sản xuất thông báo với cả hai như sau:

- Bảo hành sản phẩm 2 năm (TẠO GIÁ TRỊ 2 năm);

- Dự trữ phụ tùng, linh kiện đủ để bảo hành sản phẩm (BẢO VỆ GIÁ TRỊ 2 năm)

→ nhà sản xuất QLRR với mục đích tạo ra giá trị bảo hành 2 năm cho sản phẩm (PC và Laptop) để khách hàng yên tâm mua hàng.

→ "2 năm bảo hành" tạo động lực cho nhà sản xuất cải thiện hiệu suất, khuyến khích đổi mới và hỗ trợ việc đạt được các mục tiêu.

(*)Read more at Onbai_Ch.03_TomTat_NhieuViduMinhHoa-cho-TaoGiaTri.pptx)

Phân biệt mục đích và mục tiêu(1)

- Mục đích (Purpose) và mục tiêu (Objective):
  - Mục đích cung cấp lý do để làm điều gì đó hay cụ thể hơn là để chứng minh kết quả là điều mong muốn trong dài hạn.
- Mục đích của doanh nghiệp gần với tầm nhìn, sứ mệnh và có:
  - Tính chung chung hoặc trừu tượng;
  - Tính dài hạn (thời gian thực hiện công việc);
  - Thiếu rõ ràng, không cụ thể (về công việc gì phải làm).

Phân biệt mục đích và mục tiêu(2)

- Mục đích (Purpose) và mục tiêu (Objective): *(tiếp)*
  - Mục tiêu mô tả một cách cụ thể kết quả mong muốn theo tiêu chí S.M.A.R.T.
  - Mục tiêu thể hiện những hành động cụ thể, cần thiết để đạt được kết quả mong muốn hoặc các bước cần thiết để đạt được kết quả đã định trước trong ngắn hạn.

Mục tiêu phải đáp ứng tiêu chí S.M.A.R.T

Tiêu chí S.M.A.R.T là gì?

- Tính cụ thể, rõ ràng, chi tiết (**S**pecific);
- Tính đo lường được (**M**easurable);
- Khả năng thực hiện được (**A**ttainable);
- Tính thực tế (**R**elevant); và
- Giới hạn thời gian (**T**ime-based)

Các phát biểu về mục tiêu(1)

- Mục tiêu kinh doanh của doanh nghiệp là các giá trị (doanh số, lợi nhuận, thu nhập bình quân, tỷ lệ khách hàng hài lòng với dịch vụ….).

Ví dụ: Năm 2024, ngân hàng MB đặt mục tiêu lợi nhuận trước ***thu****ế là* ***27884*** *tỷ đồng, tăng* ***6%*** *so với năm 2023.*

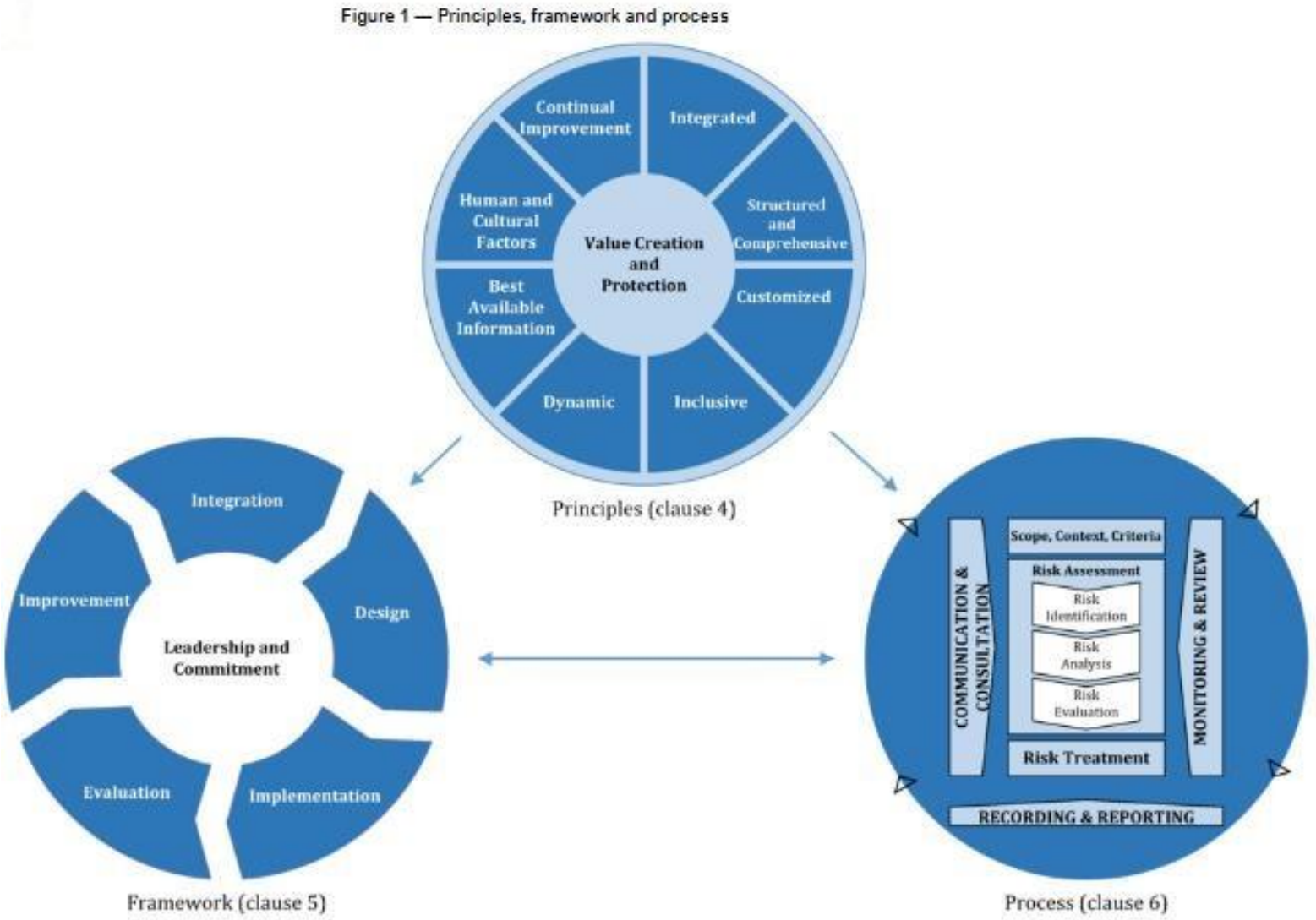
Các phát biểu về mục tiêu(2)

- Mục tiêu an toàn thông tin (ATTT) của doanh nghiệp là các giá trị như thời gian gián đoạn hệ thống CNTT không quá 2 giờ/năm, thời gian phục hồi hệ thống (Recovery Time Objective - RTO) không quá 30 phút, khôi phục vận hành hệ thống sau thảm họa không trễ hơn 1 ngày v.v.

Các phát biểu về quản lý rủi ro theo ISO 31000

1. QLRR là các hoạt động (‘*activities*’) được phối hợp để chỉ đạo và kiểm soát (‘*direct and control*’) một tổ chức liên quan đến rủi ro;
2. QLRR là hoạt động lặp đi lặp lại và hỗ trợ các tổ chức trong việc thiết lập chiến lược, đạt được mục tiêu và ra quyết định đúng;
3. QLRR là một phần của quản trị và lãnh đạo, và là nền tảng cho cách thức tổ chức được quản lý ở mọi cấp độ. Nó góp phần cải thiện các hệ thống quản lý;
4. QLRR là một phần của tất cả các hoạt động liên quan đến một tổ chức và bao gồm tương tác với các bên liên quan;
5. QLRR xem xét bối cảnh bên ngoài và bên trong của tổ chức, bao gồm hành vi của con người và các yếu tố văn hóa;
6. QLRR dựa trên các nguyên tắc, khuôn khổ và quy trình được minh họa trong Hình 1. Các thành phần này có thể đã tồn tại đầy đủ hoặc một phần trong tổ chức; và được điều chỉnh hoặc cải thiện để việc QLRR trở nên hiệu quả, hiệu suất và nhất quán.

Các thành phần của quản lý rủi ro theo ISO 31000



Hình 1

Lợi ích của quản lý rủi ro

- Quản lý rủi ro ATTT giúp doanh nghiệp đạt được các mục tiêu (là giá trị đã nêu ra) thông qua:
  - Thiết lập các biện pháp kiểm soát (*'controls'*) *(ISO 27001:2013)* nhằm ảnh hưởng tích cực đến việc đạt được mục tiêu;
  - Cải thiện việc ra quyết định dựa trên giá trị tiêu thức rủi ro (Risk Criteria, Risk Matrix) (…/cao/trung bình/thấp/…) áp vào từng rủi ro tiềm ẩn khi thực hiện các hoạt động để đạt được mục tiêu;
  - Cải thiện các kết quả hoạt động thu về các giá trị cao hơn, và;
  - Khuyến khích đổi mới để đạt giá trị tốt hơn.

02

Các nguyên tắc quản lý rủi ro (QLRR)

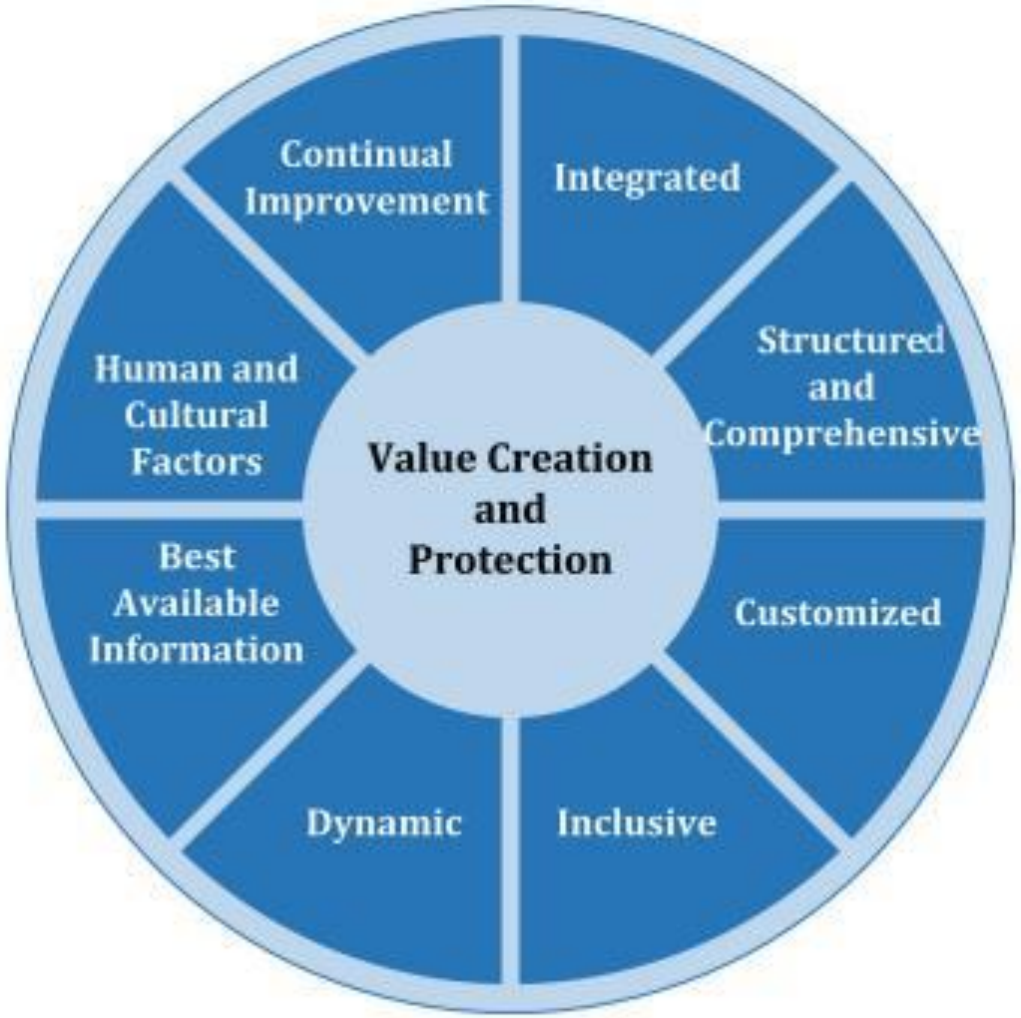


Figure 2 — Principles

Nội dung

2.1 Được tích hợp (Integrated)

2.2 Có cấu trúc và toàn diện (Structured and Comprehensive)

2.3 Được tùy chỉnh (Customized)

2.4 Sự tham gia (Inclusive)

2.5 Có tính động (Dynamic)

2.6 Thông tin sẵn có tốt nhất (Best Available Information)

2.7 Yếu tố con người và văn hóa (Human and Cultural Factors)

2.8 Cải tiến liên tục (Continual Improvement)

Nguyên tắc quản lý rủi ro(1)

- Là một ý tưởng hoặc chân lý hoặc quy tắc cơ bản giải thích hoặc kiểm soát cách hoạt động của doanh nghiệp tập trung vào quản lý rủi ro;
- Là một quy tắc đạo đức hoặc tiêu chuẩn của quản lý rủi ro;
- Là một luật lệ, một quy tắc hoặc một lý thuyết mà quản lý rủi ro dựa vào;
- Là khái niệm cơ bản hoặc niềm tin chỉ đạo tạo thành nền tảng của việc thực hành quản lý rủi ro. Nó đóng vai trò là giá trị cốt lõi hoặc tiêu chuẩn đạo đức định hình quá trình ra quyết định, hành động và hành vi trong quá trình quản lý rủi ro.

Nguyên tắc quản lý rủi ro(2)

- Các nguyên tắc (xem Hình 2) cung cấp hướng dẫn về các đặc điểm của quản lý rủi ro (sao cho) hiệu quả và hiệu suất, truyền đạt giá trị (của nó) và giải thích ý định và mục đích của quản lý rủi ro.
- Các nguyên tắc là nền tảng để quản lý rủi ro và cần được xem xét khi thiết lập khuôn khổ và quy trình quản lý rủi ro của tổ chức.
- Các nguyên tắc này sẽ cho phép một tổ chức quản lý các tác động của sự không chắc chắn đối với các mục tiêu của mình.

Nguyên tắc QLRR(1) : Được tích hợp (Integrated)

- Quản lý rủi ro là một phần không thể tách rời trong tất cả các hoạt động của tổ chức / doanh nghiệp. *('Risk management is an integral part of all organizational activities.' – ISO 27000)*

Nguyên tắc QLRR(1): Được tích hợp (Integrated)

- Quản lý rủi ro là một phần không thể tách rời của tất cả các hoạt động tổ chức / doanh nghiệp.

  Các loại rủi ro sau đây luôn hiện diện, do đó phải được tích hợp vào quản lý:
  - Rủi ro trong hoạt động hàng ngày của doanh nghiệp (vận hành, tác nghiệp, danh tiếng, tín dụng, thanh khoản …)
  - Rủi ro khi triển khai dự án (tiến độ (T), phạm vi (S), chi phí (C), chất lượng (Q)…luôn có rủi ro khi triển khai dự án)
  - Rủi ro trong hệ thống CNTT (sự cố gây gián đoạn hệ thống, vi phạm ATTT, vi phạm tuân thủ …)

Nguyên tắc QLRR(2): Có cấu trúc và toàn diện (Structured and Comprehensive)

- Một cách tiếp cận toàn diện và có cấu trúc để quản lý rủi ro mang lại kết quả nhất quán và có thể so sánh được, cụ thể:
  - Tổ chức QLRR toàn doanh nghiệp với cơ cấu từ trên xuống dưới;
  - Có bộ phận phụ trách QLRR từng phòng ban.

Nguyên tắc QLRR(2): Có cấu trúc và toàn diện (Structured and Comprehensive)

- Tổ chức QLRR toàn doanh nghiệp với cơ cấu từ trên xuống dưới;
- Có bộ phận phụ trách QLRR từng phòng ban;
- Chỉ định vai trò, trách nhiệm, truyền đạt thông tin và báo cáo;
- Có chính sách và quy trình QLRR;
- Có công cụ và kỹ thuật để QLRR;
- Có tổ chức và duy trì hoạt động giám sát, kiểm tra và đánh giá kết quả QLRR định kỳ.

Nguyên tắc QLRR(3): Được tùy chỉnh (Customized)

- Quá trình và khuôn khổ quản lý rủi ro được tùy biến và tương xứng với bối cảnh bên ngoài và bối cảnh nội bộ của tổ chức có liên quan đến các mục tiêu của tổ chức.
  - Mỗi tổ chức đều khác nhau. Khuôn khổ và quy trình quản lý rủi ro phải được điều chỉnh phù hợp với từng tổ chức, bối cảnh hoạt động và mục tiêu của tổ chức.

Nguyên tắc QLRR[4]: Sự tham gia (Inclusive)[4]

- Sự tham gia thích hợp và kịp thời của các bên liên quan giúp cho kiến thức, quan điểm và cảm nhận của mọi người được suy xét thấu đáo. Điều này dẫn đến việc nâng cao nhận thức và việc quản lý rủi ro có đầy đủ thông tin.

Nguyên tắc QLRR(5): Tính động (Dynamic)

- Rủi ro có thể hình thành, thay đổi hoặc biến mất do bối cảnh nội bộ, bên ngoài của tổ chức thay đổi.
- Quản lý rủi ro dự đoán, phát hiện, ghi nhận và ứng phó một cách kịp thời, thích hợp với những thay đổi và sự kiện đó.

Nguyên tắc QLRR[6]: Thông tin sẵn có tốt nhất (Best Available Information)

- Đầu vào cho QLRR dựa trên thông tin trong quá khứ, hiện tại, cũng như dự báo trong tương lai.
- QLRR tính đến một cách rõ ràng mọi hạn chế và sự không chắc chắn gắn liền với những thông tin và dự báo đó.
- Thông tin cần kịp thời, rõ ràng và có sẵn cho các bên liên quan

Nguyên tắc QLRR(7): Yếu tố con người và văn hóa (Human and cultural factors)

- Hành vi của con người và văn hóa ảnh hưởng đáng kể đến tất cả các khía cạnh của QLRR tại mỗi cấp và giai đoạn.
  - Các cá nhân và các bên liên quan có khẩu vị rủi ro (Risk Attitude) khác nhau (Ghét rủi ro, chấp nhận rủi ro, không quan tâm rủi ro, trung tính) hoặc *"Trời kêu ai người đó dạ"*

Nguyên tắc QLRR[8]: Cải tiến liên tục (Continual improvement)

QLRR được cải tiến liên tục thông qua áp dụng chu trình PDCA (PDCA cycle) để duy trì và cải tiến liên tục hiệu quả hoạt động QLRR:

"P" là Lập Kế hoạch (**P**lan);

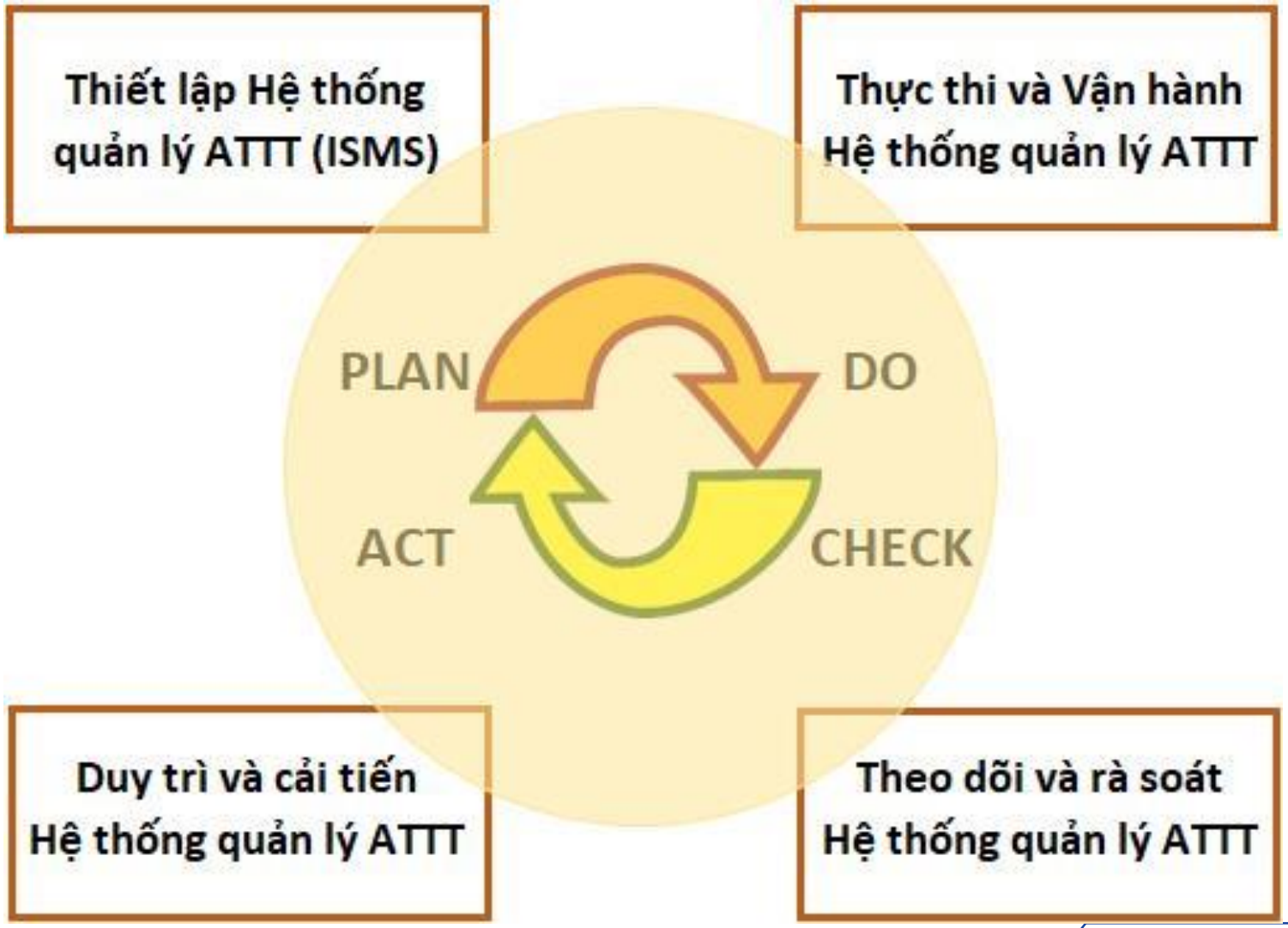
"D" là Thực hiện (**D**o);

"C" là Kiểm tra, giám sát (**C**heck); và

"A" là Duy trì và cải tiến kết quả (**A**ct)

Nguyên tắc QLRR(8): Cải tiến liên tục …

CHU TRÌNH PDCA (CHU TRÌNH DEMING)



Nguyên tắc QLRR(8): Cải tiến liên tục …

- QLRR được cải tiến liên tục thông qua tạo giá trị, học hỏi (từ khách hàng,…) và kinh nghiệm;
- Khi nghĩ về **CẢI TIẾN**, phải tạo giá trị (value) và ghi nhớ:

If you can't measure it, you can't analyse it;

If you can't analyse it, you can't manage it;

If you can't manage it, you can't control it;

If you can't control it, you can't improve it.

Nếu không thể đo lường thì không thể phân tích;
Nếu không thể phân tích thì không thể quản lý;
Nếu không thể quản lý thì không thể kiểm soát;
Nếu không thể kiểm soát thì không thể cải tiến.

Hết Chương 03

Cám ơn tất cả Anh/Chị đã theo dõi Chương này

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