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

Chương 4
Khuôn khổ quản lý rủi ro
(Risk management framework)

Nội dung

01 Khái quát (General)

02 Sự lãnh đạo và cam kết (Leadership and commitment)

03 Tích hợp (Intergration)

04 Thiết kế (Design)

05 Áp dụng (Implementation)

06 Xem xét, đánh giá (Evaluation)

07 Cải tiến (Improvement)

01

Khái quát (General)

Figure 3 — Framework

1. Khái quát (General) (1)

1.1 Mục đích:

Mục đích của khuôn khổ quản lý rủi ro (Risk Management Framework) là hỗ trợ doanh nghiệp/tổ chức **tích hợp** quản lý rủi ro (QLRR) vào các hoạt động và các chức năng quan trọng của doanh nghiệp/tổ chức.

1. Khái quát (General) (2)

1.2 Định nghĩa

a) Khuôn khổ (Framework)

- Là cấu trúc hỗ trợ hoặc cấu trúc cơ bản thiết yếu (essential supporting or underlying structure) [ISO 9001];
- Khuôn khổ phục vụ như một nền tảng (it serves as a foundation).

1. Khái quát (General) (3)

b) Khuôn khổ quản lý rủi ro (QLRR)

- Khuôn khổ quản lý rủi ro là nền tảng của quản lý rủi ro.
- Tiêu chuẩn ISO31000:2018 chính là một khuôn khổ của quản lý rủi ro.

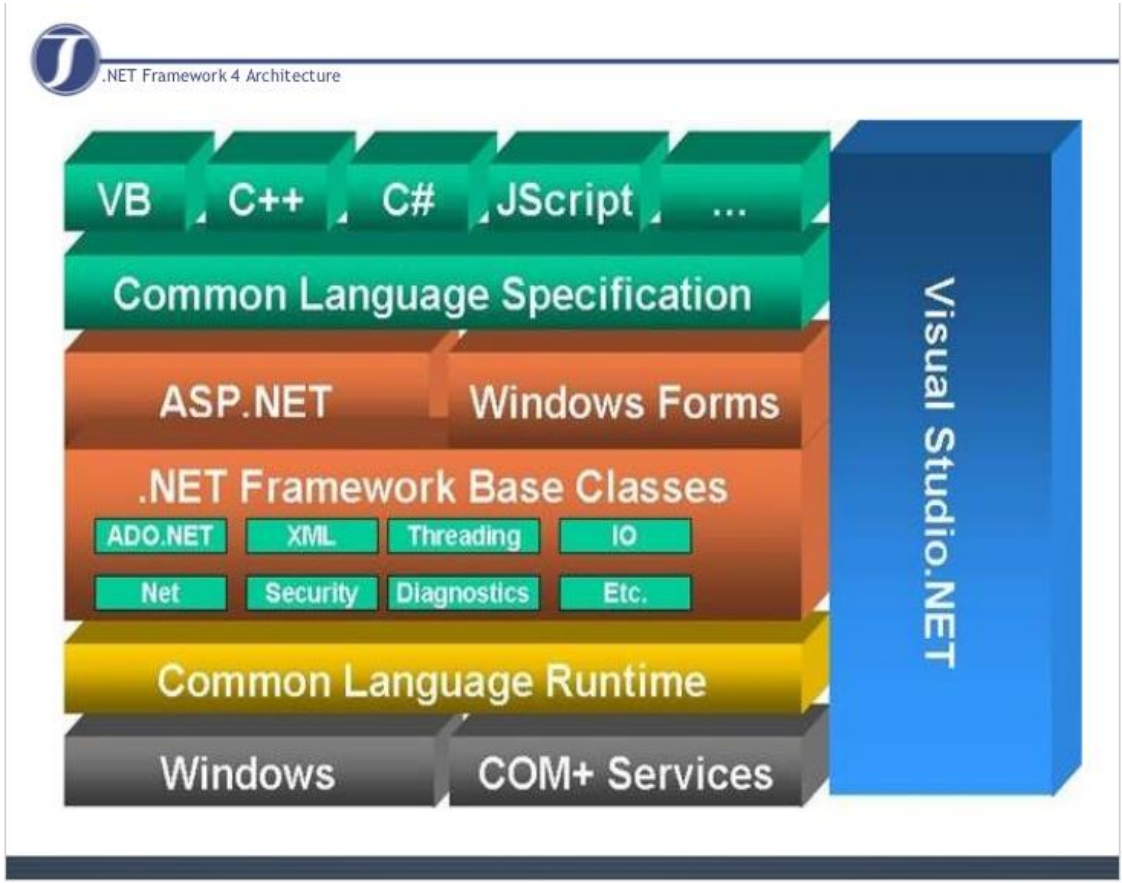


Image source: https://www.slideshare.net/diyaots/net-framework-40-changes-benefits

1. Khái quát (General) (4)

c) **Mục đích của khuôn khổ QLRR:**

- Có được hỗ trợ từ ban quản lý cấp cao và các bên liên quan.
- Giúp cho tổ chức tích hợp quản lý rủi ro vào các hoạt động và chức năng quan trọng của tổ chức.

1. Khái quát (General) (5)

d) **Khuôn khổ ATTT (Framework in cybersecurity)**

➢ Khuôn khổ ATTT là gì?

Về cơ bản, khuôn khổ ATTT là một hệ thống các tiêu chuẩn, hướng dẫn và phương pháp tốt nhất *(a system of standards, guidelines, and best practices)* để quản lý rủi ro phát sinh trong thế giới kỹ thuật số.

1. Khái quát (General) (6)

Khuôn khổ ATTT (Framework in cybersecurity) (tiếp)

- Nhóm tiêu chuẩn quản lý ATTT ISO 27000 *(The ISO family of information security management standards)* là một loạt các tiêu chuẩn bảo mật thông tin *(ISO 27001, ISO 27002…)* hỗ trợ lẫn nhau có thể được kết hợp để cung cấp một **khuôn khổ ATTT** *(framework in cybersecurity)* được công nhận trên toàn cầu cho việc quản lý bảo mật thông tin theo phương pháp tốt nhất:

1. Khái quát (General)[7]

Khuôn khổ ATTT (Framework in cybersecurity) (tiếp)

- Tiêu chuẩn ISO 27001:2013 và ISO 27002:2013 thuộc nhóm tiêu chuẩn quản lý ATTT ISO 27000 chính là các khuôn khổ ATTT.
- Tiêu chuẩn ISO 27001:2013 chính là khuôn khổ ATTT với 14 Nhóm (“domains” / “categories”), 35 Yêu cầu kèm theo mục tiêu (“Objective”) và 114 Điều kèm theo biện pháp kiểm soát (“Control”).

1. Khái quát (General)[8]

- Tiêu chuẩn ISO/IEC 27002:2013 đưa ra hướng dẫn (Guidances) về bảo mật thông tin và các thông lệ thực hành tốt nhất (Best Practices) quản lý bảo mật thông tin, bao gồm việc lựa chọn, triển khai và quản lý các biện pháp kiểm soát (Controls) có tính đến (các) môi trường rủi ro bảo mật thông tin của tổ chức.

1. Khái quát (General)(9)

e) Một số khuôn khổ (“framework”) khác:

- Khuôn khổ của mạng máy tính là mô hình OSI (Open Systems Interconnection), mô hình này chia kiến trúc mạng thành bảy lớp riêng biệt (Physical Layer, Data Link Layer, Network layer, Transport Layer, Session Layer, Presentation Layer and Application Layer)

1. Khái quát (General)(10)

Một số khuôn khổ ("framework") khác: (tiếp)

- .NET là một khuôn khổ phát triển phần mềm do Microsoft tạo ra. Nó cung cấp một nền tảng để xây dựng và chạy các ứng dụng trên Windows, Linux và macOS và hỗ trợ nhiều ngôn ngữ, bao gồm C#, F# và VB.NET.

1. Khái quát (General)[11]

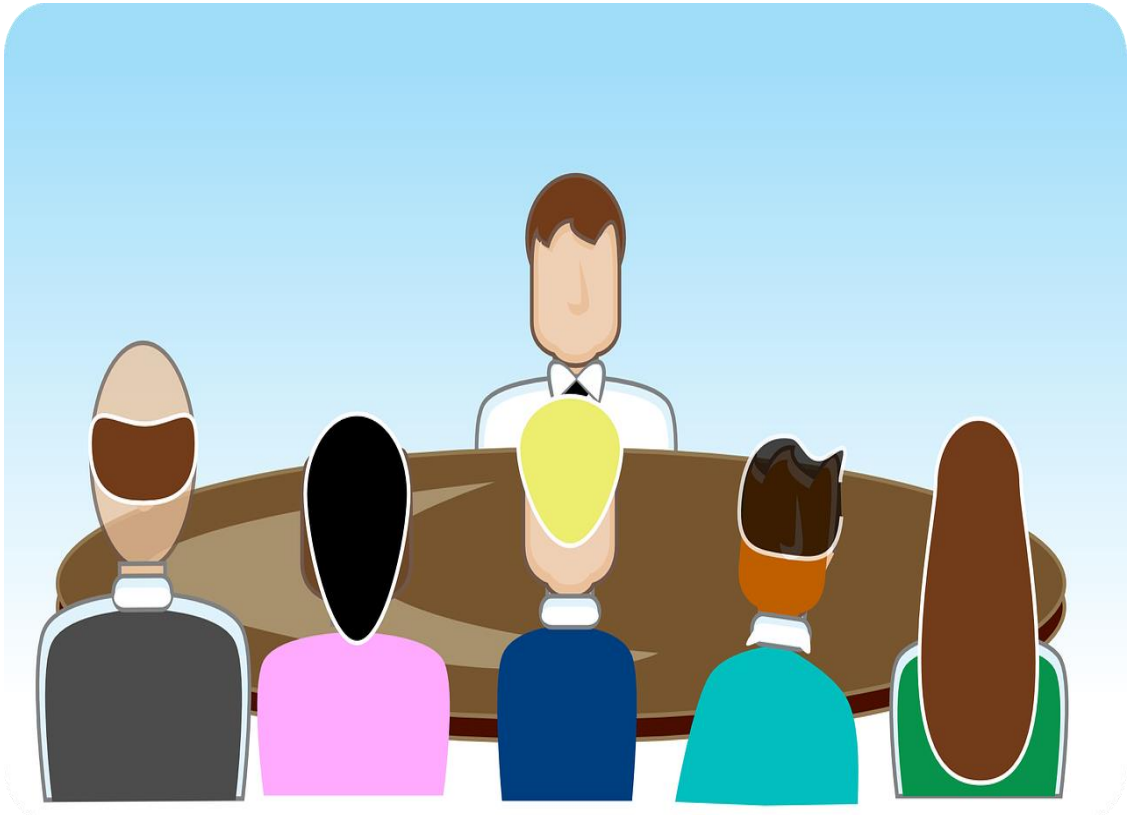
f) Quản trị (“Governance”)

Là **cách thức một tổ chức được quản lý ở cấp cao nhất** (theo các quy tắc, chuẩn mực và hành động được cấu trúc, duy trì, giám sát, điều chỉnh, ra quyết định và chịu trách nhiệm giải trình) và là **các hệ thống** dùng cho việc duy trì cách thức này: Hội đồng quản trị (Board of Directors – BoD).

1. Khái quát (General)[12]

g) Quản lý (“Management”)

Là sự kiểm soát và tổ chức vận hành một tổ chức (ví dụ doanh nghiệp); cấp nguồn lực, hướng dẫn và giám sát hoạt động hàng ngày của nhân viên làm việc trong tổ chức: Ban Tổng Giám đốc/Ban Giám đốc (Board of Management - BoM)



1. Khái quát (General)[13]

h) Phân biệt giữa “Governance” và “Management”:

- BoD (Hội đồng quản trị), với tư cách là cơ quan quản lý ở **cấp cao nhất**, có trách nhiệm thiết lập mục tiêu, định hướng, chiến lược, nguyên tắc (luật lệ), giới hạn và khuôn khổ giải trình của tổ chức.
- BoM (Ban Giám đốc) có trách nhiệm phân bổ nguồn lực và giám sát các hoạt động hàng ngày của tổ chức.
- BoD chịu trách nhiệm xác định cái gì (“What”) phải làm và BoM chịu trách nhiệm về cách thức (“How”) thực hiện.

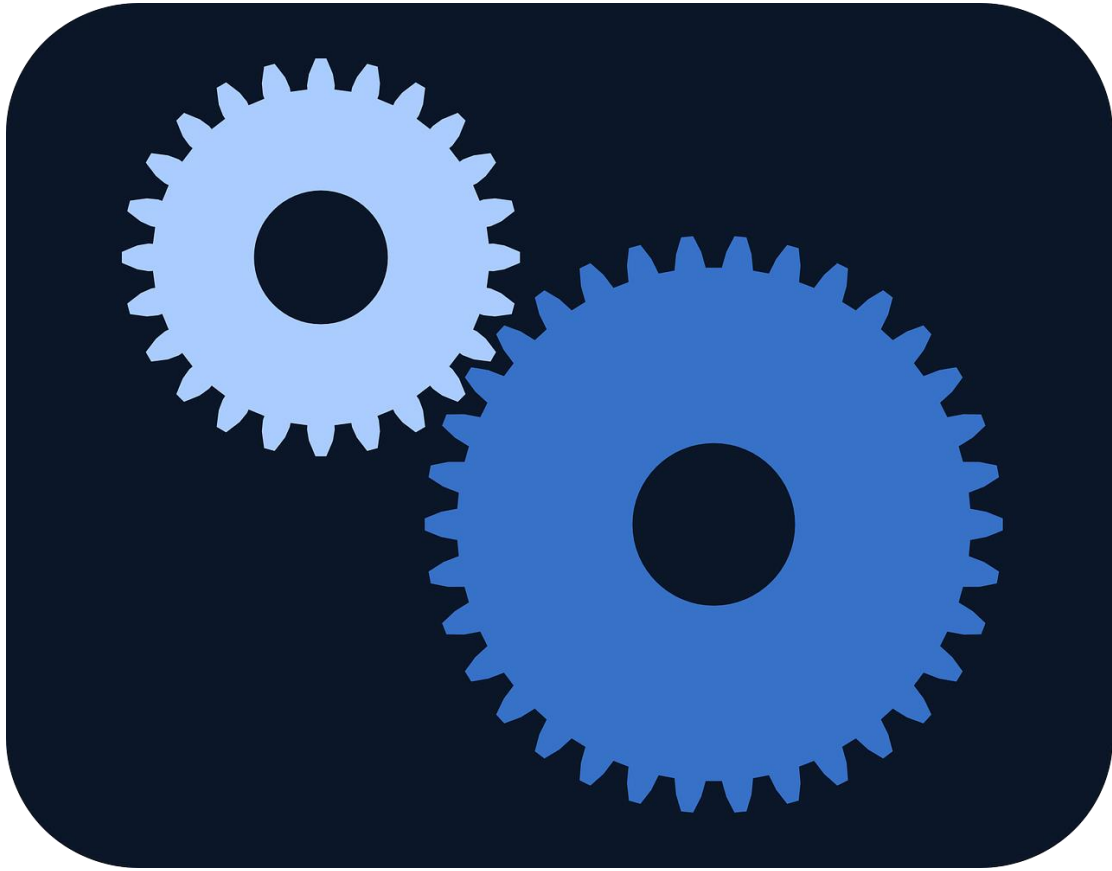
1. Khái quát (General)[14]

i) Sự phù hợp (Conformity)

Sự hoàn thành một yêu cầu [ISO 27000];

hoặc sự tuân thủ các tiêu chuẩn, quy tắc

hoặc pháp luật.



1. Khái quát(15)

1.3 **Hiệu quả (“Effectiveness”) của QLRR tại doanh nghiệp phụ thuộc vào:**

- Việc tích hợp QLRR vào hoạt động quản trị
- Việc ra quyết định của lãnh đạo và sự hỗ trợ các bên liên quan;
- Sự đánh giá định kỳ các thông lệ và quy trình QLRR để giải quyết các khác biệt.

1. Khái quát(16)

1.4 Các thành phần của một khuôn khổ QLRR

Các thành phần của khuôn khổ	Liên hệ với chu trình PDCA (Deming Cycle)
Integrating (tích hợp)	PLAN
Designing (thiết kế)	
Implementing (triển khai)	DO
Evaluating (đánh giá)	CHECK
Improving (cải thiện)	ACT

02

Sự lãnh đạo và cam kết (Leadership and commitment)

2. Sự lãnh đạo và cam kết(1)

Sự lãnh đạo ('Leadership') và Cam kết ('Commitment'):

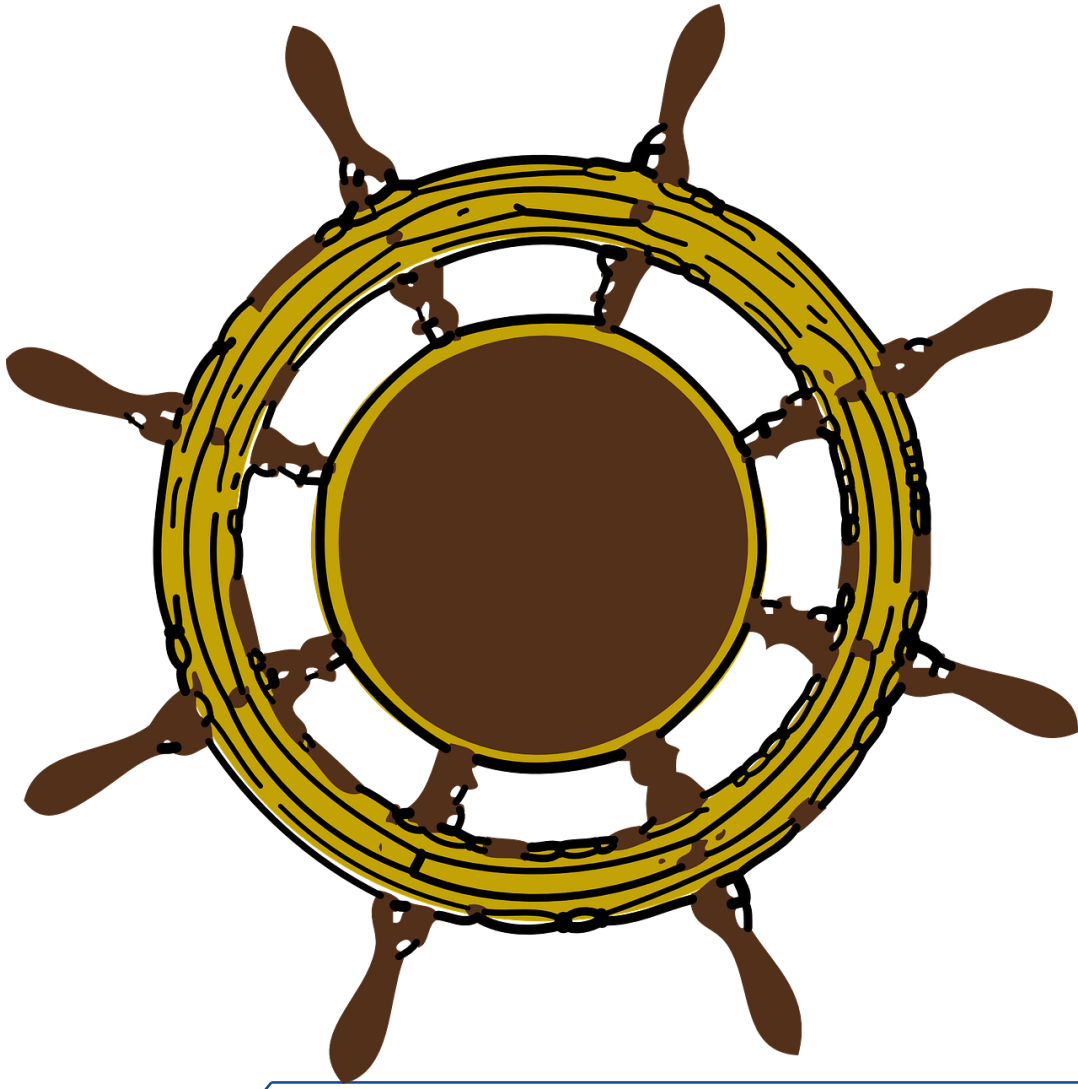
- Đặt vào vị trí trung tâm của khuôn khổ ('Framework') quản lý rủi ro;
- Luôn hiện diện trong 5 thành phần của khuôn khổ: tích hợp, thiết kế, triển khai (thực hiện), đánh giá và cải tiến QLRR.

Figure 3 — Framework

2. Sự lãnh đạo và cam kết(2)

2.1 Sự lãnh đạo (Leadership)

- Lãnh đạo là một kỹ năng liên quan đến việc gây ảnh hưởng và thúc đẩy một nhóm cá nhân làm việc hướng tới một mục tiêu chung.
- Trong môi trường doanh nghiệp, điều này liên quan đến việc lãnh đạo và hướng dẫn nhân viên cũng như đồng nghiệp về một chiến lược hoặc kế hoạch nhằm đáp ứng yêu cầu của doanh nghiệp. [ISO 9001]



2. Sự lãnh đạo và cam kết(3)

2.2 Sự cam kết (commitment)

- Việc triển khai hoạt động QLRR ATTT không thể thành công nếu không có sự cam kết của cấp quản lý cao nhất (BoM).
- Cấp quản lý cao nhất (BoM) phải đảm bảo rằng QLRR phải được (1)tích hợp vào tất cả các hoạt động của doanh nghiệp; (2)tổ chức các hoạt động giám sát, và (3)chịu trách nhiệm giải trình về QLRR với cấp quản trị (BoD).

2. Sự lãnh đạo và cam kết(4)

2.2 Sự cam kết (commitment)

- Cấp quản lý cao nhất (BoM) phải:
  - Chứng tỏ sự lãnh đạo và cam kết đối với ATTT (ban hành chính sách (như chính sách ATTT); kế hoạch thực hiện; phân công thẩm quyền, trách nhiệm và giải trình ở các cấp trong tổ chức; cung cấp nguồn lực; ban hành quy trình; thúc đẩy cải tiến liên tục v.v.)
  - Thiết lập và tổ chức công tác giám sát hoạt động QLRR phù hợp với mục tiêu, chiến lược và văn hóa của tổ chức; phù hợp với khuôn khổ QLRR và bối cảnh hoạt động..

2. Sự lãnh đạo và cam kết(5)

- Cấp quản lý cao nhất (BoM) phải:
  - Chứng tỏ và khẳng định rõ cam kết liên tục của mình đối với QLRR thông qua chính sách, tuyên bố hoặc các hình thức khác để truyền đạt rõ ràng các mục tiêu và cam kết của doanh nghiệp đối với QLRR. (*)
  - Cam kết của tổ chức đối với QLRR phải được ghi thành điều khoản trong chính sách ATTT của doanh nghiệp khi ban hành [Minh họa: một Mẫu chính sách ATTT của doanh nghiệp có cam kết QLRR]. (*)
  - Nội dung cam kết QLRR bao gồm nhưng không giới hạn theo hướng dẫn trong ISO 31000:2018 – Risk Management – Guidelines.

2. Sự lãnh đạo và cam kết(6)

- Hoạt động QLRR tại doanh nghiệp phải bao gồm hoạt động của các thực thể (bộ phận) làm công việc giám sát song song với hoạt động QLRR của cấp quản lý cao nhất.
- Thực thể (bộ phận) giám sát được yêu cầu phải đảm bảo là:
  - Các rủi ro được xem xét và thấu hiểu khi đặt mục tiêu của tổ chức;
  - Hệ thống QLRR được triển khai và hoạt động hiệu quả;
  - Các rủi ro nêu ra phù hợp với bối cảnh các mục tiêu của tổ chức;
  - Thông tin về các rủi ro và cách QLRR được truyền đạt đúng cách.

03

Tích hợp (Integration)

3. Tích hợp (Integration)

- Quản lý rủi ro là một phần không thể tách rời của tất cả các hoạt động tổ chức / doanh nghiệp.
- Tích hợp QLRR vào hoạt động của doanh nghiệp là một quá trình động, lặp lại và tùy chỉnh theo nhu cầu và văn hóa của doanh nghiệp.

04

Thiết kế (Design)

4.1 Hiểu về tổ chức và bối cảnh của tổ chức

4.2 Phân công vai trò, quyền hạn, trách nhiệm, và trách nhiệm giải trình trong tổ chức

4.3 Phân bổ nguồn lực

4.4 Thiết lập việc trao đổi thông tin và tham vấn

4.1 Thiết kế - Hiểu về tổ chức và bối cảnh của tổ chức

- Khi thiết kế khuôn khổ quản lý rủi ro, tổ chức (doanh nghiệp) cần xem xét và hiểu bối cảnh nội bộ và bên ngoài của mình.
- **Xem xét bối cảnh bên ngoài** tổ chức (các yếu tố xã hội, văn hóa, chính trị, pháp lý, tài chính, công nghệ, kinh tế và môi trường ở cấp quốc tế, khu vực, quốc gia…; các mối quan hệ, sự lệ thuộc…- *(tham khảo tài liệu ISO 31000 và các tài liệu liên quan khác))*
- **Xem xét bối cảnh bên trong** tổ chức (tầm nhìn, sứ mệnh, các giá trị của doanh nghiệp, cơ cấu điều hành, chiến lược, mục tiêu, chính sách, văn hóa, các mối quan hệ, sự phụ thuộc … *(tham khảo tài liệu ISO 31000 và các tài liệu liên quan khác))*

4.2 Thiết kế - Phân công vai trò, quyền hạn, trách nhiệm, và trách nhiệm giải trình trong tổ chức

- Cấp quản lý cao nhất đảm bảo rằng quyền hạn, trách nhiệm và trách nhiệm giải trình của những vị trí liên quan đến QLRR được phân công và trao đổi thông tin cho tất cả các cấp trong tổ chức, và cần:

  - Nhấn mạnh rằng quản lý rủi ro là trách nhiệm cốt lõi;

  - Xác định các cá nhân có trách nhiệm giải trình và quyền hạn đối với việc quản lý rủi ro (chủ sở hữu rủi ro). (*)

4.3 Thiết kế - Phân bổ nguồn lực

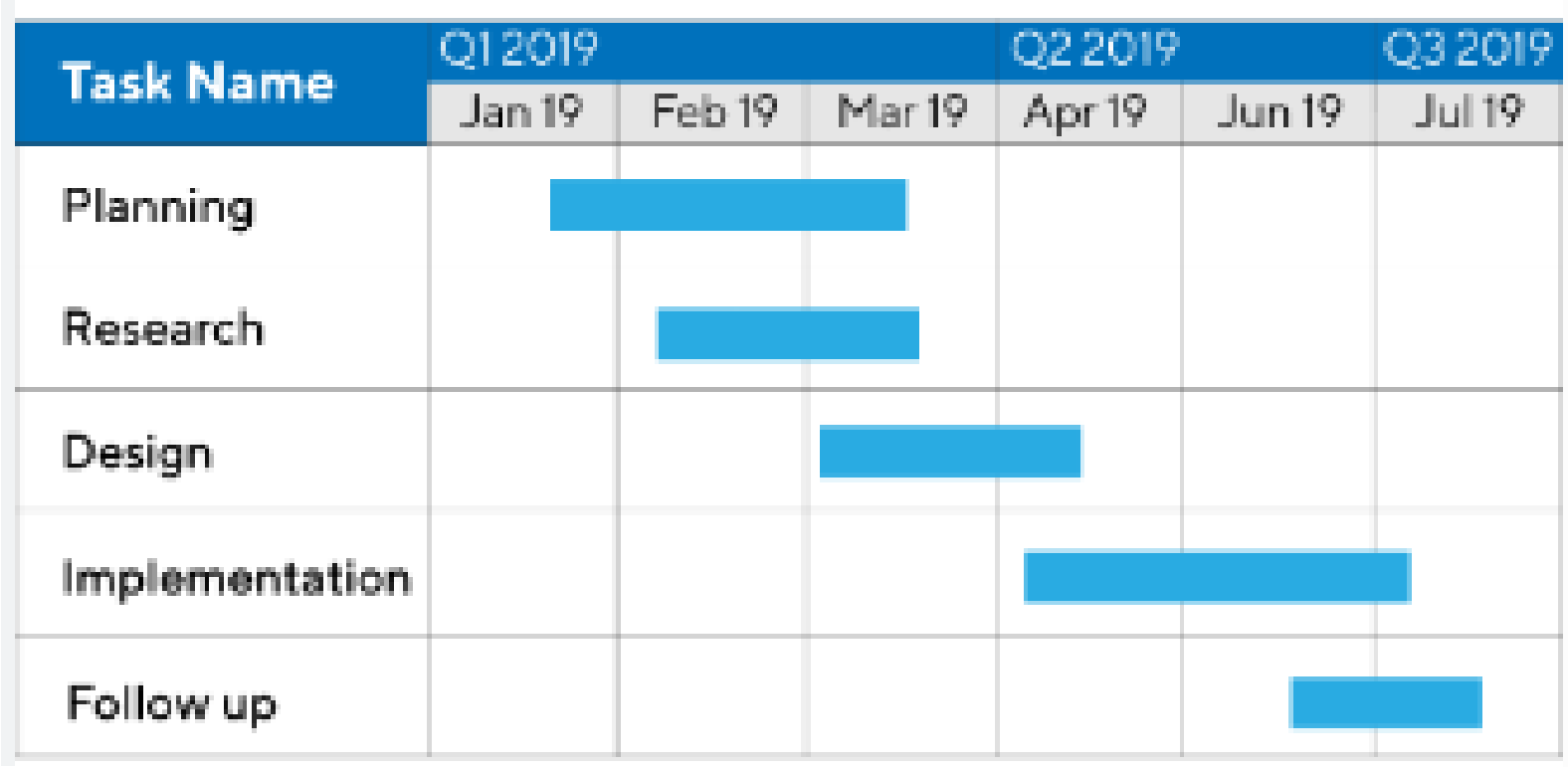
- Lãnh đạo cao nhất và bộ phận giám sát, nếu có, cần đảm bảo phân bổ các nguồn lực thích hợp *(con người, công cụ, tài liệu hướng dẫn công việc (quy trình, thủ tục), khóa đào tạo về QLRR…)* cho việc QLRR, theo hướng dẫn trong tiêu chuẩn ISO 31000:2018 – Risk Management – Guidelines và không bị giới hạn.

4.4 Thiết kế - Thiết lập việc trao đổi thông tin và tham vấn

- Trao đổi thông tin với các đối tượng mục tiêu và tham vấn nhằm hỗ trợ khuôn khổ QLRR thông qua họp mặt, gửi văn bản lấy ý kiến góp ý, gửi thư điện tử (Email) kèm tài liệu, điện thoại ….
- Ý kiến phản hồi của các đối tượng mục tiêu phải được xem xét, đối chiếu, tổng hợp, trả lời và ra quyết định thực hiện khắc phục, cải tiến.

05

Thực thi - Áp dụng (Implementation)



5. Áp dụng

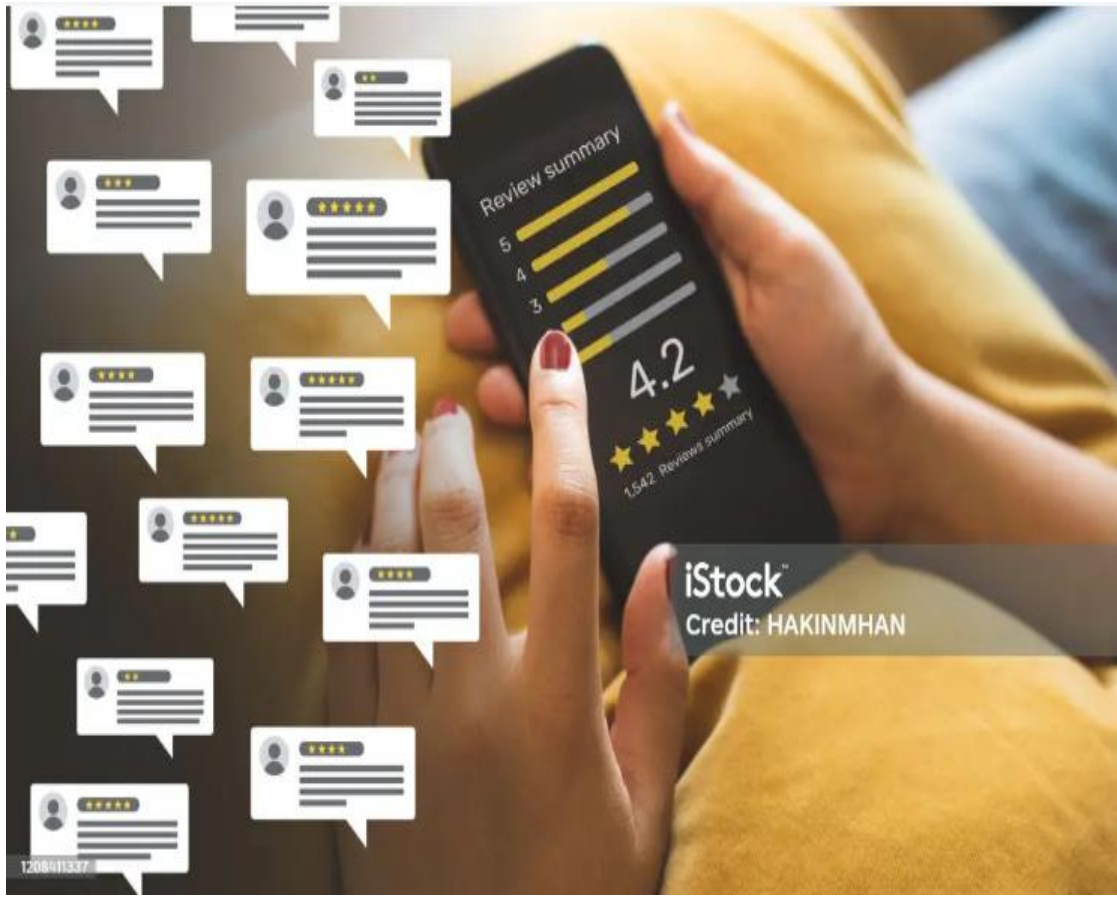
- Xây dựng và trình ban hành Quy chế hoạt động QLRR của các Phòng/Ban/Đơn vị trực thuộc bao gồm các nội dung thiết kế đã trình bày. [xem một Mẫu Quy chế đính kèm](*)
- Xây dựng và trình phê duyệt kế hoạch triển khai QLRR bao gồm nội dung phạm vi áp dụng, thời điểm triển khai, người thực hiện, thời gian, nguồn lực trang bị, cách thức ra quyết định, cập nhật định kỳ, khóa đào tạo về QLRR cho cá nhân liên quan.

06

Xem xét và đánh giá (Evaluation)

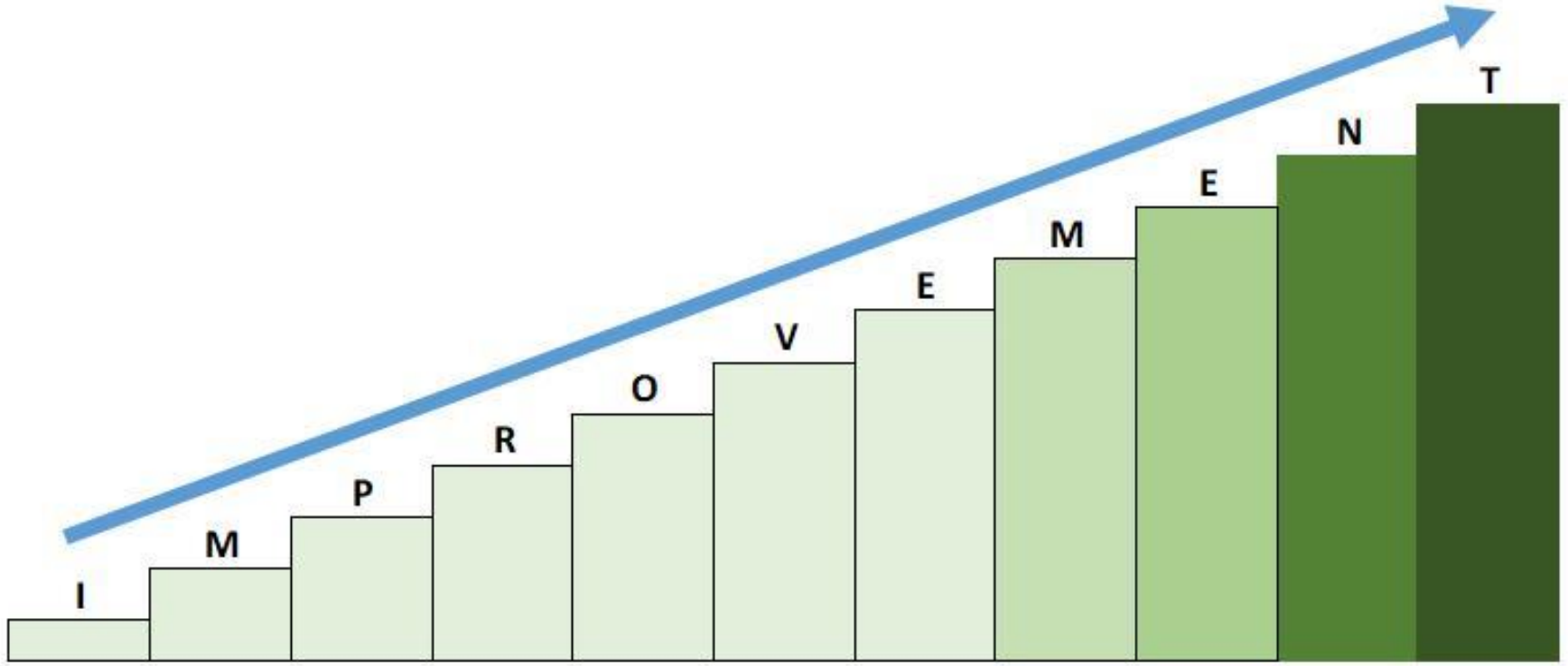
6. Xem xét và đánh giá

- Xem xét đánh giá tính hiệu lực của khuôn khổ QLRR, tổ chức cần:
  - định kỳ đo lường kết quả thực hiện khuôn khổ quản lý rủi ro theo mục đích, kế hoạch thực hiện, các chỉ số và những hành vi dự kiến;
  - xác định xem khuôn khổ QLRR có duy trì sự thích hợp để hỗ trợ đạt được các mục tiêu của tổ chức hay không



07

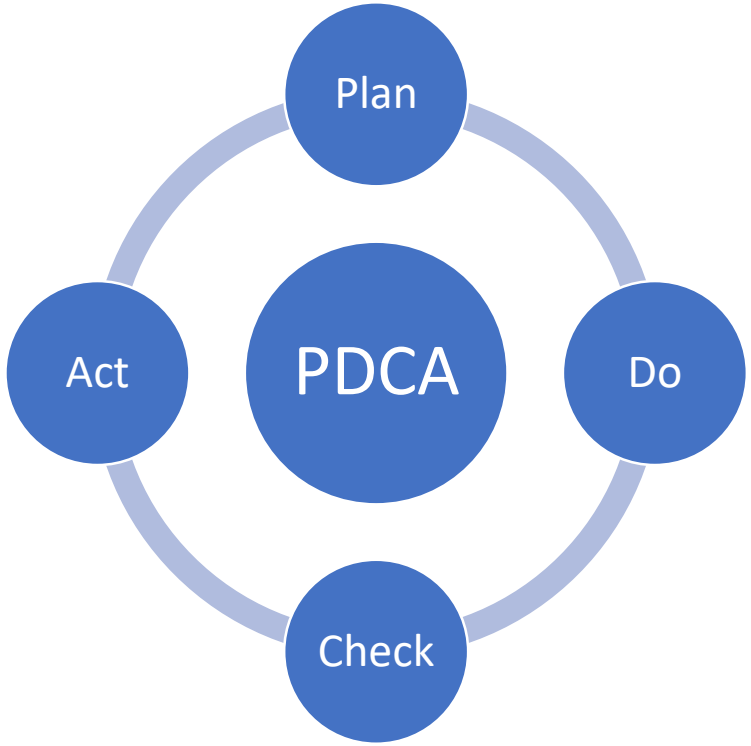
Cải tiến (Improvement)



7. Cải tiến(1)

7.1 Điều chỉnh

- Tổ chức cần liên tục theo dõi và điều chỉnh khuôn khổ QLRR để giải quyết những thay đổi nội bộ, bên ngoài và có thể nâng cao giá trị của tổ chức.
- Triển khai hoạt động cải tiến theo chu trình PDCA (chu trình Deming).



7. Cải tiến(2)

7.2 Cải tiến liên tục khuôn khổ QLRR

- Phân công trách nhiệm cụ thể cho người thi hành cải tiến.
- Cải tiến cách thức tích hợp quá trình QLRR sao cho phù hợp, đầy đủ và hiệu lực.
- Cải tiến bộ giá trị (“values”) được đo lường trong QLRR.

7. Cải tiến(3)

7.3 QLRR được cải tiến liên tục thông qua học hỏi, kinh nghiệm và để cải tiến điều gì hoặc việc gì, phải ghi nhớ:

Nếu bạn không có giá trị để đo lường, bạn không thể phân tích nó;

Nếu bạn không thể phân tích nó, bạn không thể quản lý nó;

Nếu bạn không thể quản lý nó thì bạn không thể kiểm soát nó;

Nếu bạn không thể kiểm soát nó, bạn không thể cải tiến nó.

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

Hết Chương 04

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/