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 5
Quy trình quản lý rủi ro (Process)

Nội dung

01 Khái quát (General)

02 Trao đổi thông tin và tham vấn (Establishing communication and consultation)

03 Phạm vi, bối cảnh và tiêu chí (Scope, context and criteria)

04 Đánh giá rủi ro (Risk Assessment)

05 Xử lý rủi ro (Risk Treatment)

06 Theo dõi và Xem xét (Monitoring and review)

07 Lập hồ sơ và báo cáo (Recording and reporting)

01

Khái quát (General)

1. Khái quát (General) (1)

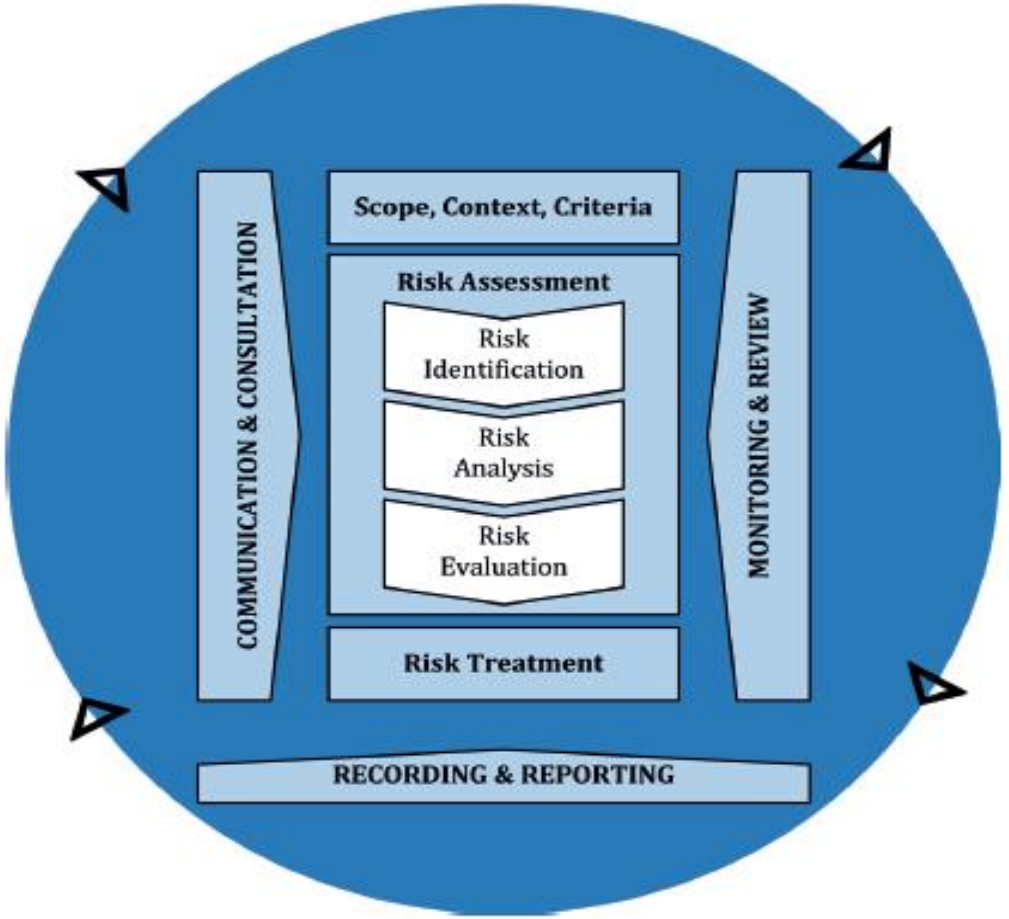


Figure 4 — Process

1. Khái quát (General) (2)

- **Biện pháp kiểm soát (‘Control’) trong ISO/IEC 27001:**
  - **An toàn thông tin đạt được bằng cách triển khai một bộ các biện pháp kiểm soát phù hợp;**
  - **Biện pháp kiểm soát là biện pháp bảo vệ hoặc biện pháp đối phó được sử dụng để quản lý rủi ro liên quan đến bảo mật thông tin.**

1. Khái quát (General) (3)

- **Biện pháp kiểm soát (‘Control’) trong ISO/IEC 27001:**
  - **Các biện pháp kiểm soát này được thiết kế để giảm lỗ hổng bảo mật và các mối đe dọa tiềm ẩn;**
  - **Các biện pháp kiểm soát đảm bảo tính bảo mật, toàn vẹn và khả dụng của tài sản thông tin.**

1. Khái quát (General) (4)

- **Biện pháp kiểm soát (‘Control’) trong ISO/IEC 27001:**
  - **Bộ các biện pháp kiểm soát bao gồm các:**
    - **Chính sách, quy trình, thủ tục;**
    - **Cơ chế kỹ thuật;**
    - **Cấu trúc tổ chức; và**
    - **Chức năng phần mềm và phần cứng.**

1. Khái quát (General) (5)

Quy trình QLRR phải:

1.1 Tuân thủ nguyên tắc QLRR (Chương 3 / ISO 31000:2018)

1.2 Đáp ứng theo khuôn khổ QLRR (Chương 4 / ISO 31000:2018)

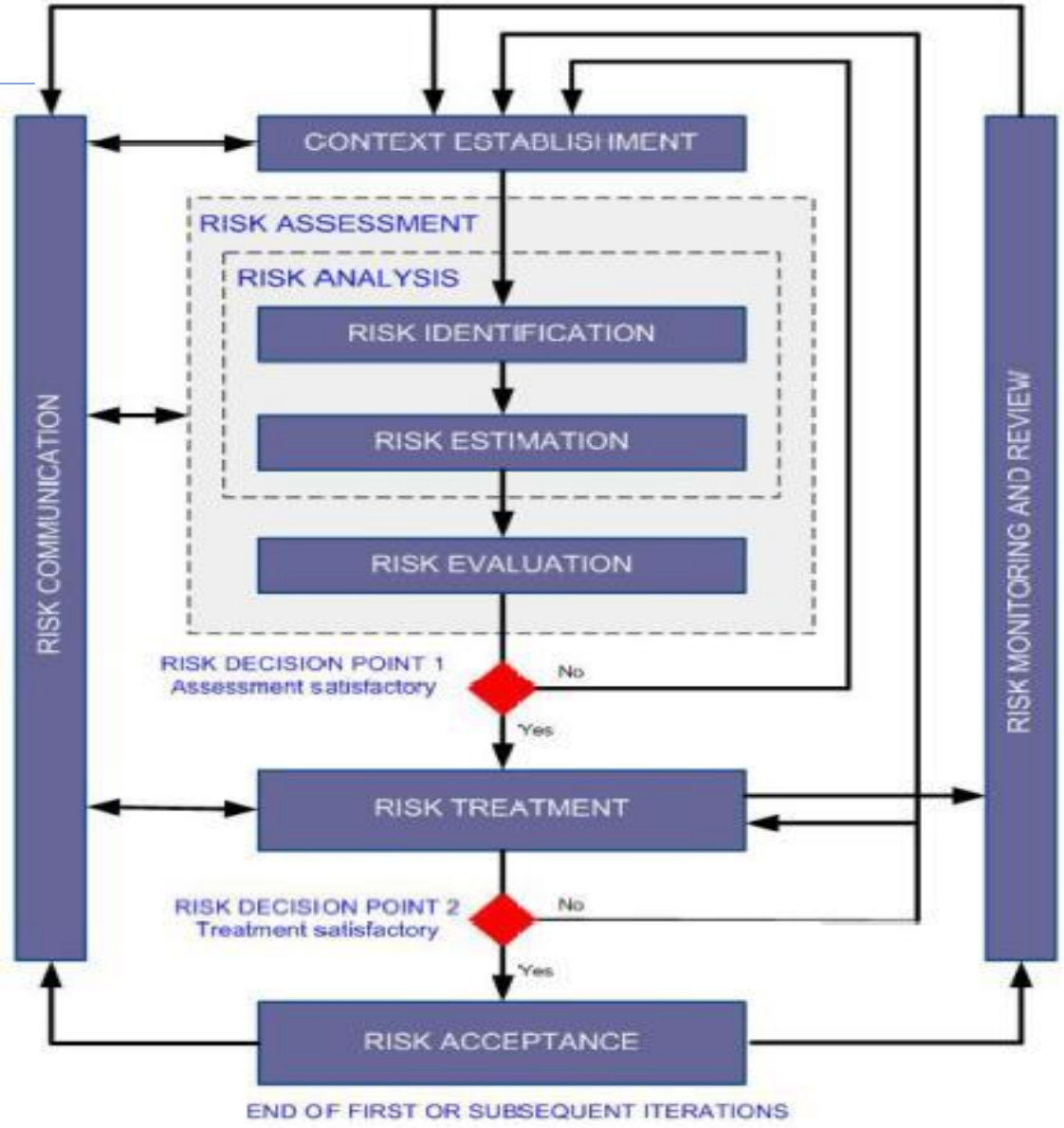
1.3 Áp dụng một cách hệ thống các chính sách, thủ tục và thực hành của tổ chức (doanh nghiệp) vào quá trình QLRR.

1.4 Có bộ văn bản Quy trình QLRR tại doanh nghiệp đáp ứng 1.1, 1.2, 1.3…được ban hành (bộ văn bản gồm quy trình, thủ tục, phụ lục, biểu mẫu) và triển khai áp dụng cho QLRR ATTT của doanh nghiệp.

1. Khái quát (General)(6)

1.5 Trường hợp QLRR đối với ATTT, quy trình QLRR phải được tùy chỉnh theo yêu cầu của tiêu chuẩn ISO 27005:2008:

- Quá trình có 2 điểm kiểm soát để ra quyết định hành động trước khi chấp nhận nghiệm thu (Risk Acceptance)



1. Khái quát (General) (7)

Các BƯỚC thực hiện quy trình	Chu trình PDCA
Trao đổi thông tin và tham vấn; Xác định phạm vi QLRR, nhận thức bối cảnh hoạt động và thiết lập tiêu chí rủi ro (Scope, context and risk criteria)	PLAN
- Đánh giá rủi ro (RISK ASSESSMENT) (:Risk identification, risk analysis and risk evaluation) - Xử lý rủi ro (RISK TREATMENT) (:Selection of options and Preparing and implementing plans)	DO
Theo dõi và Xem xét (Monitoring and review)	CHECK
Cải tiến, lập hồ sơ và báo cáo (Improving, Recording and reporting)	ACT

1. Khái quát (General) [8]

Tại doanh nghiệp, Quy trình QLRR được thực hiện theo 11 bước như sau:

Bước 1. Lập kế hoạch

Bước 2. Nhận dạng rủi ro (Risk Identification);

Bước 3. Phân tích rủi ro (Risk Analysis / Risk Estimation);

Bước 4. Đánh giá rủi ro (Risk Evaluation);

Bước 5. Xử lý rủi ro (Risk Treatment);

Bước 6. Lập kế hoạch xử lý rủi ro;

Bước 7. Phê duyệt tài liệu, hồ sơ QLRR;

Bước 8. Báo cáo kết quả hoạt động QLRR;

Bước 9. Theo dõi, xem xét và đánh giá lại quá trình;

Bước 10. Cải tiến, lập hồ sơ và báo cáo định kỳ kết quả QLRR;

Bước 11. Lưu hồ sơ QLRR

02

Trao đổi thông tin và tham vấn (Establishing communication and consultation)

2. Trao đổi thông tin và tham vấn

Quá trình QLRR phải:

1.1 Đáp ứng theo khuôn khổ QLRR (Chương 4 / ISO 31000:2018) tại nội dung tương tự

1.2 Hỗ trợ các bên liên quan hiểu về rủi ro, về các cơ sở để ra quyết định và lý do tại sao cần các hành động cụ thể.

03

Phạm vi, bối cảnh và tiêu chí (Scope, context and criteria)

3.1 Khái quát (General)

3.2 Xác định phạm vi (Defining the scope)

3.3 Bối cảnh nội bộ và bên ngoài

(External and internal context)

3.4 Xác định tiêu chí rủi ro

(Defining risk criteria)

3.1 Khái quát

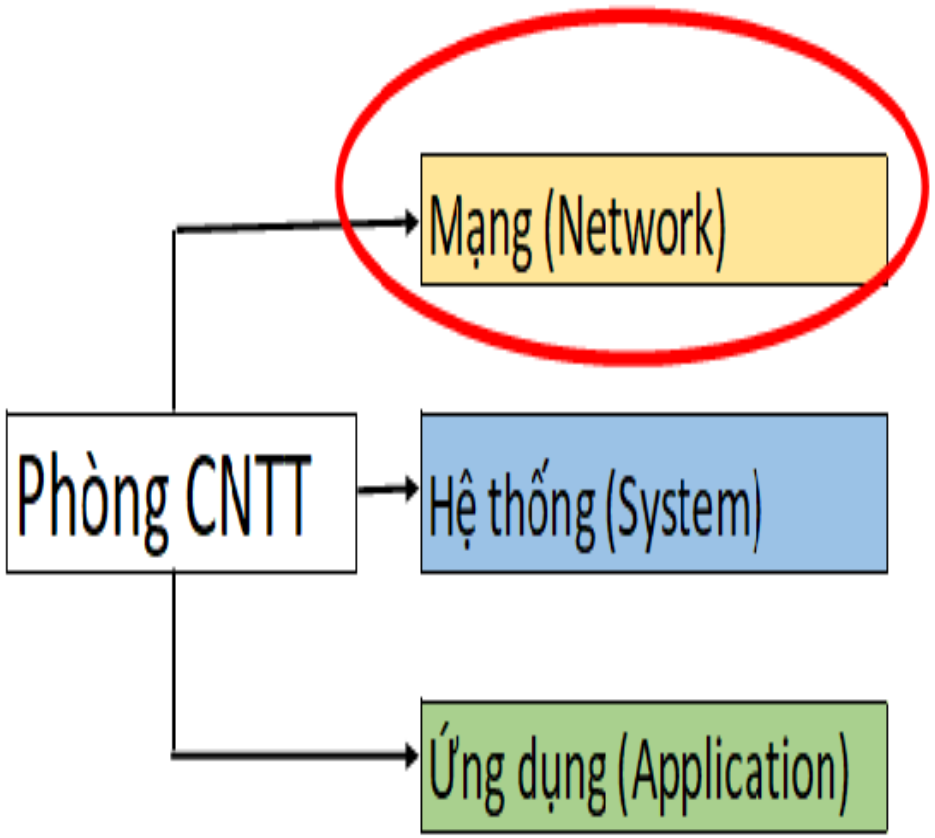
Mục đích của việc thiết lập phạm vi, bối cảnh và tiêu chí là để:

- Tùy chỉnh quá trình quản lý rủi ro, cho phép đánh giá rủi ro một cách hiệu lực và xử lý rủi ro một cách thích hợp.
- Xác định được:
  - Phạm vi của quá trình;
  - Hiểu bối cảnh nội bộ, bối cảnh bên ngoài; và
  - Tiêu chí rủi ro (cao, trung bình, thấp theo thang đo như 5x5, 6x6)

3.2 Xác định phạm vi

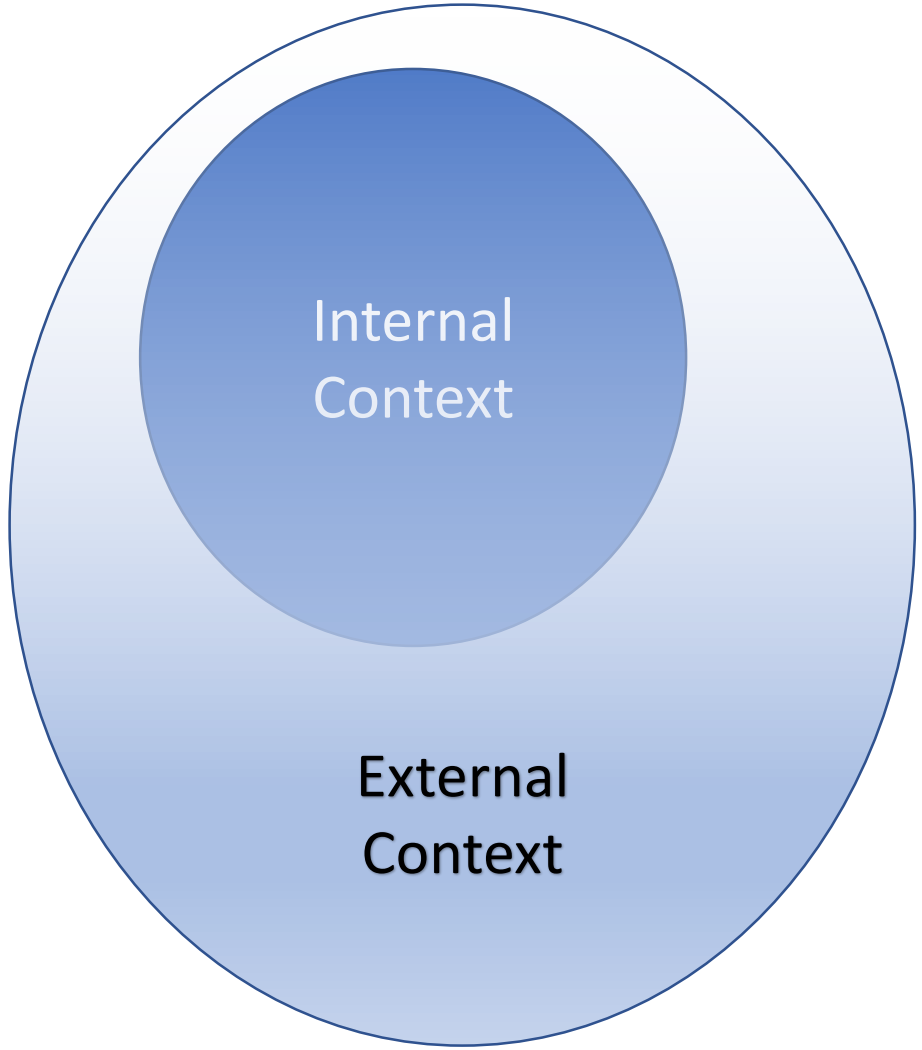
Xác định phạm vi các hoạt động QLRR theo:

- Mục tiêu, sản phẩm / dịch vụ được bàn giao; ranh giới QLRR;
- Quyết định nào cần thực hiện;
- Các cấp khác nhau (chiến lược, tác nghiệp, chương trình, dự án…)
- Thời gian, địa điểm; các công cụ và kỹ thuật áp dụng;
- Mối quan hệ với các dự án, quá trình và hoạt động khác…



3.3 Bối cảnh nội bộ và bên ngoài (1)

- Đáp ứng theo khuôn khổ QLRR (Chương 4 / ISO 31000:2018) nội dung "Hiểu về tổ chức và bối cảnh" bao gồm bối cảnh bên trong (Internal context) và bối cảnh bên ngoài (External context) tổ chức



3.3 Bối cảnh nội bộ và bên ngoài (2)

Yếu tố/bối cảnh bên ngoài	Yếu tố/bối cảnh nội bộ
- Các yếu tố xã hội, văn hóa, chính trị, pháp lý, chế định, tài chính, công nghệ, kinh tế và môi trường ở cấp quốc tế, quốc gia, khu vực hoặc địa phương; - Các yếu tố từ thị trường và nền kinh tế số; - Thay đổi của vòng đời sản phẩm CNTT; - Ngành nghề của tổ chức, xu hướng; - Đối thủ cạnh tranh; - Tình hình địa chính trị; - Hiện trạng công nghệ; - Các mối quan hệ, cảm nhận, các giá trị, nhu cầu và mong đợi của các bên liên quan bên ngoài; - Các mối quan hệ và cam kết theo hợp đồng; - Mức độ phức tạp của mạng lưới và sự lệ thuộc lẫn nhau; - V.v.	- Tầm nhìn, sứ mệnh và các giá trị; - Chiến lược, mục tiêu và chính sách; - Mục tiêu kinh doanh của tổ chức; - Mô hình hoạt động; - Cơ cấu tổ chức, vai trò và trách nhiệm giải trình; - Tầm quan trọng của CNTT; - Các hệ thống thông tin và các dòng thông tin; - Thay đổi trong năng lực quản lý; - Văn hóa doanh nghiệp; - Độ phức tạp của hoạt động và mức độ chấp nhận sự thay đổi; - Mối quan hệ nội bộ và các giá trị của họ; - Các mối quan hệ và cam kết theo hợp đồng; - Sự phụ thuộc trong nội bộ và liên hệ lẫn nhau - V.v.

3.4 Xác định tiêu chí rủi ro (1)

- Xem lại nội dung về “Tiêu chí rủi ro” (Chương 1 / ISO 31000:2018)
- Xác định các tiêu chí để đánh giá mức độ nghiêm trọng (thấp, trung bình, cao) của rủi ro để hỗ trợ việc ra quyết định.
- Quy định số lượng và loại rủi ro được phép hoặc không được phép chấp nhận liên quan đến các mục tiêu.
- **Một văn bản có nội dung tiêu chí rủi ro phải được ban hành đưa vào áp dụng khi bắt đầu quá trình đánh giá rủi ro**.
- Tiêu chí rủi ro thường bao gồm các định nghĩa về các mức độ tác động (‘Impact’) và khả năng khác nhau (‘Likelihood’).

3.4 Xác định tiêu chí rủi ro (2)

BẢNG THANG ĐIỂM CÁC TIÊU CHÍ VỀ KHẢ NĂNG XẢY RA & MỨC ĐỘ ẢNH HƯỞNG CỦA RỦI RO

BẢNG 01: KHẢ NĂNG XẢY RA	
Xếp loại	**Tần suất, khả năng**
Gần như chắc chắn xảy ra/ Xảy ra thường xuyên (6)	Xảy ra thường xuyên – Ít nhất một lần một tuần
Xảy ra nhiều lần (5)	Có thể xảy ra một hoặc hai lần trong tháng tới
Có thể xảy ra (4)	Có thể xảy ra một hoặc hai lần trong 03 tháng tới
Thỉnh thoảng xảy ra (3)	Có thể xảy ra một hoặc hai lần trong năm tới
Ít xảy ra (2)	Có thể xảy ra một hoặc hai lần trong 03 năm tới
Rất hiếm khi xảy ra (1)	Không chắc xảy ra trong 05 năm tới

3.4 Xác định tiêu chí rủi ro (3)

BẢNG 02: THANG ĐIỂM ĐÁNH GIÁ ẢNH HƯỞNG		
Xếp loại	**Giá trị ảnh hưởng**	**Tiêu chí**
Thảm họa (6)	Tổn thất tiềm tàng hoặc tổn thất thực tế trên 50 tỷ VND	- Gây ảnh hưởng cực kỳ nghiêm trọng đến hoạt động kinh doanh - Rủi ro hoạt động vô cùng cao hoặc vi phạm rất nghiêm trọng trong quản trị doanh nghiệp - Công tác kiểm soát cực kỳ lỏng lẻo - Các hình phạt pháp lý nghiêm trọng (ví dụ: thu hồi giấy phép ngân hàng, bắt giam) - Rủi ro giá cổ phiếu có thể bị tác động hoặc thực tế đã bị tác động - Xảy ra các sự cố gián đoạn hệ thống trong thời gian kéo dài với tần suất xảy ra lớn và phạm vi xảy ra trên toàn hệ thống, gây ảnh hưởng nghiêm trọng đến hoạt động của các đơn vị. - Số lượng lớn khách hàng cùng khiếu nại, phản ánh gây ảnh hưởng danh tiếng nghiêm trọng trong thời gian dài dẫn đến suy giảm nghiêm trọng thị phần - Phát sinh tai nạn nghiêm trọng, có thể gây chết người hoặc gây thương tật vĩnh viễn cho nhân viên, khách hàng, người dân.

3.4 Xác định tiêu chí rủi ro (4)

- Chú ý: Bảng 2 -Thang điểm đánh giá ảnh hưởng thể hiện số tiền (50 tỷ VND) trong cột "Giá trị ảnh hưởng" chính là **khẩu vị rủi ro** (Risk Appetite) của doanh nghiệp ứng với xếp loại ảnh hưởng mức độ là 6 – xem lại định nghĩa ở Chương 1
- Khẩu vị rủi ro theo Bảng 2 cho từng loại ảnh hưởng của rủi ro được chỉ rõ: *Theo Bảng 2 thì tổn thất về tài chính cho mỗi rủi ro xảy ra theo xếp loại từ 1- 6 là không được vượt quá 500 triệu VNĐ, 1 tỷ VNĐ, 5 tỷ VNĐ, [5, 10) tỷ VNĐ, [10, 50] tỷ VNĐ và >50 tỷ VNĐ.*

3.4 Xác định tiêu chí rủi ro (5)

- V/v Khẩu vị rủi ro (Risk Appetite): Khẩu vị rủi ro cao hoặc thấp sẽ thể hiện sự chấp nhận tổn thất để theo đuổi mục tiêu của doanh nghiệp. Khẩu vị rủi ro vạch ra giới hạn mà trong đó, các hoạt động QLRR được thực hiện trong giới hạn này mà không cần lãnh đạo doanh nghiệp phải phê duyệt lại khi mà môi trường hoạt động ổn định; vai trò và trách nhiệm cá nhân đã được chỉ định rõ.

3.4 Xác định tiêu chí rủi ro (6)

- Xem chi tiết đầy đủ Bảng 1 và Bảng 2 – Thang điểm đánh giá Khả năng xảy ra và Tác động/Ảnh hưởng theo tập tin đính kèm Ch.05: Ch.05_MatranRR_Thangdiem_KhaNangXayRa-HeQua.pdf
- Phối hợp từng tiêu chí của Khả năng xảy ra và từng tiêu chí Tác động sẽ được một Ma trận đánh giá rủi ro (‘Risk Matrix’).

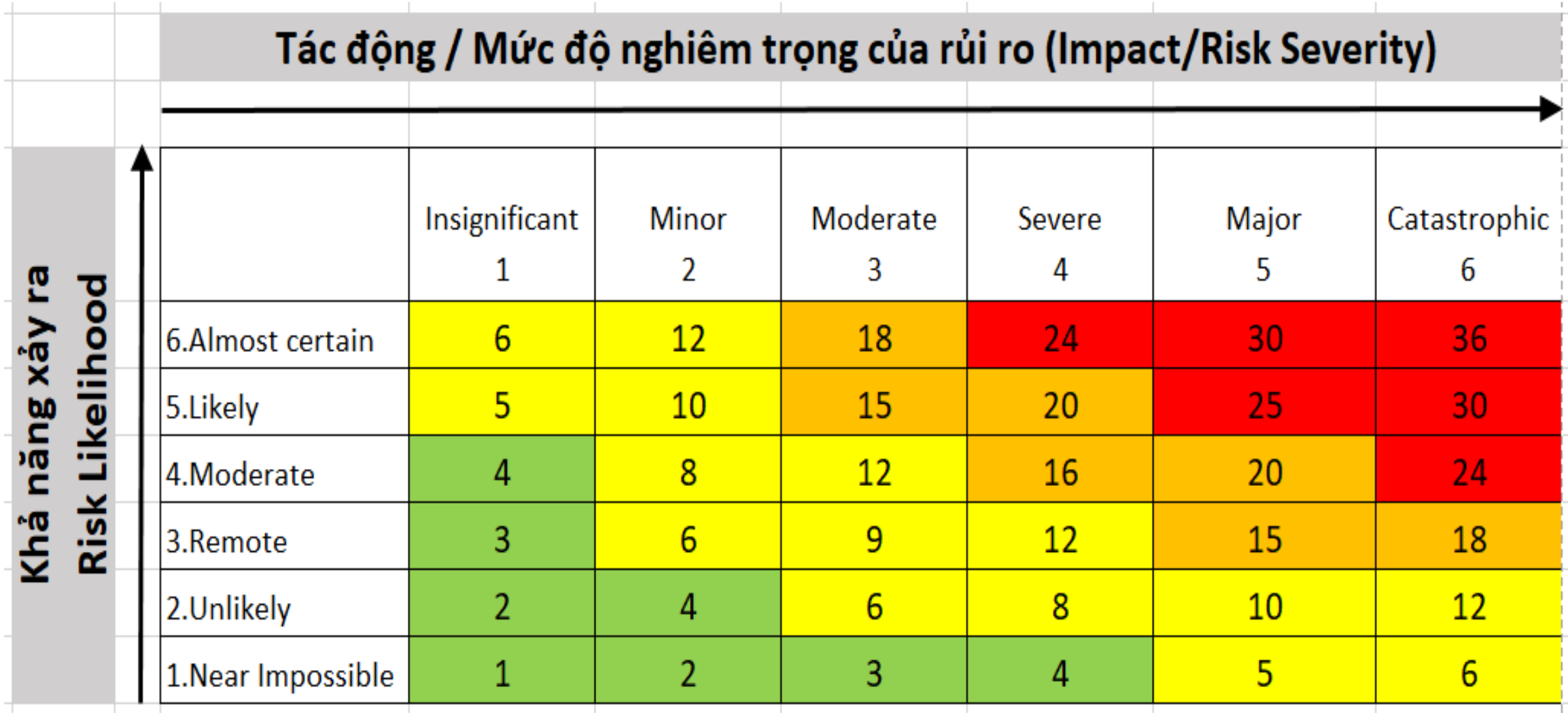
3.4 Xác định tiêu chí rủi ro (7)

- Thang đánh giá rủi ro cấp độ 6x6 bao gồm sáu hàng và sáu cột (thường gọi là ma trận rủi ro 6x6 ‘Risk Matrix 6x6’), trong đó:
  - Các cột biểu thị khả năng xảy ra rủi ro (‘Likelihood’); và
  - Các hàng biểu thị mức độ nghiêm trọng (‘Severity / Impact) của rủi ro.
- Rủi ro có thể được phân loại thành 36 ô khác nhau, dựa trên mức độ nghiêm trọng của rủi ro và khả năng xảy ra rủi ro.

3.4 Xác định tiêu chí rủi ro [8]

			1	2	3	4	5	6
Khả năng xảy ra ('Likelihood')	6	Có thể ('Likely')	M	H	E	E	E	E
	5	Thỉnh thoảng ('Occasional')	M	H	H	E	E	E
	4	Hiếm khi ('Seldom')	L	M	H	H	E	E
	3	Không chắc ('Unlikely')	L	M	M	H	H	E
	2	Mơ hồ/xa vời ('Remote')	L	L	M	M	H	H
	1	Hiếm có ('Rare')	L	L	L	L	M	M
			Không đáng kể ('Insignificant')	Nhỏ / Yếu ('Minor')	Vừa phải ('Moderate')	Lớn ('Major')	Nghiêm trọng ('Severe')	Thảm họa ('Catastrophic')
			Tác động ('Impact')					

3.4 Xác định tiêu chí rủi ro (9)



	Insignificant 1	Minor 2	Moderate 3	Severe 4	Major 5	Catastrophic 6
6.Almost certain	6	12	18	24	30	36
5.Likely	5	10	15	20	25	30
4.Moderate	4	8	12	16	20	24
3.Remote	3	6	9	12	15	18
2.Unlikely	2	4	6	8	10	12
1.Near Impossible	1	2	3	4	5	6

3.4 Xác định tiêu chí rủi ro (10)

Quan sát hoạt động QLRR của một Ngân hàng TMCP X, họ mô tả các cấp độ rủi ro trong ma trận 6X6 như sau:

Theo đó, các cấp độ rủi ro được mô tả như sau:

Xếp hạng	Giá trị rủi ro đã phân theo các cấp	Mô tả cấp độ rủi ro
Rủi ro rất cao (E)	18 - 36	Đây là các rủi ro rất khó có thể điều tiết trong bất kỳ hoàn cảnh nào, một khi rủi ro xảy ra sẽ dẫn đến hậu quả khó lường cho ngân hàng. Do vậy, đối với các rủi ro này ngân hàng phải tích cực triển khai ngay các hành động để giải quyết rủi ro, trong đó cần cân nhắc xem xét đến phương án phòng tránh rủi ro hoặc nếu không thể, phải xây dựng một kế hoạch hành động chi tiết để ứng phó, đồng thời việc triển khai thực hiện kế hoạch cần được kiểm tra, giám sát chặt chẽ.
Rủi ro cao (H)	10 - 17	Đối với các rủi ro được xếp hạng ở mức độ cao, ngân hàng cần sớm triển khai các hành động cần thiết để giải quyết rủi ro. Trong đó, các kế hoạch hành động tương ứng cần được nghiên cứu và xây dựng một cách kỹ lưỡng để đảm bảo việc kiểm soát, giảm thiểu rủi ro về mức chấp nhận của ngân hàng.

3.4 Xác định tiêu chí rủi ro (11)

Rủi ro trung bình (M)	5 - 9	Rủi ro được xếp hạng ở mức độ trung bình có thể kiểm soát được thông qua việc cải tiến các kiểm soát hiện hữu hoặc thực hiện thêm các biện pháp kiểm soát cần thiết để giảm thiểu mức độ rủi ro về mức chấp nhận được của ngân hàng.

Xếp hạng	Giá trị rủi ro đã phân theo các cấp	Mô tả cấp độ rủi ro
Rủi ro thấp (L)	1 - 4	Đối với những rủi ro được xếp hạng ở mức độ thấp, Ngân hàng có thể xem xét chấp nhận được nếu mức độ tổn thất được dự đoán nằm trong ngưỡng kỳ vọng. Ngân hàng sẽ không cần các hành động hoặc biện pháp khắc phục nào thêm ngoài việc bảo đảm các biện pháp kiểm soát hiện hữu (nếu có) hoạt động hiệu quả. Ngân hàng cần xem xét kỹ lưỡng các kiểm soát đã xây dựng để đảm bảo không thực hiện kiểm soát quá mức cần thiết đối với các rủi ro thấp này.

04

Đánh giá (Risk Assessment)

4.1 Khái quát (General)

4.2 Nhận diện rủi ro (Risk Identification)

4.3 Phân tích rủi ro (Risk Analysis)

4.4 Định mức rủi ro (Risk Evaluation)

4.1 Khái quát

- Tuân thủ 8 nguyên tắc QLRR (Chương 3 / ISO 31000:2018) khi tiến hành đánh giá rủi ro.
- Đánh giá rủi ro cần được tiến hành một cách hệ thống và lặp lại.

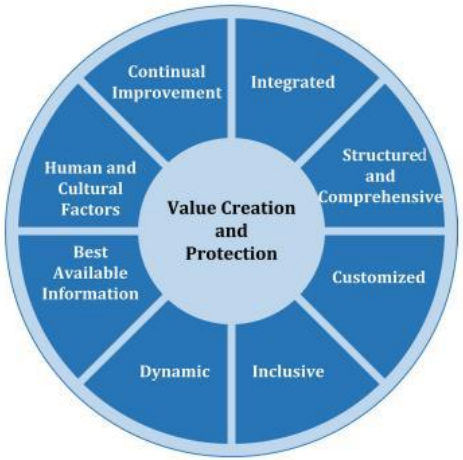


Figure 2 — Principles

4.2 Nhận diện rủi ro (1)

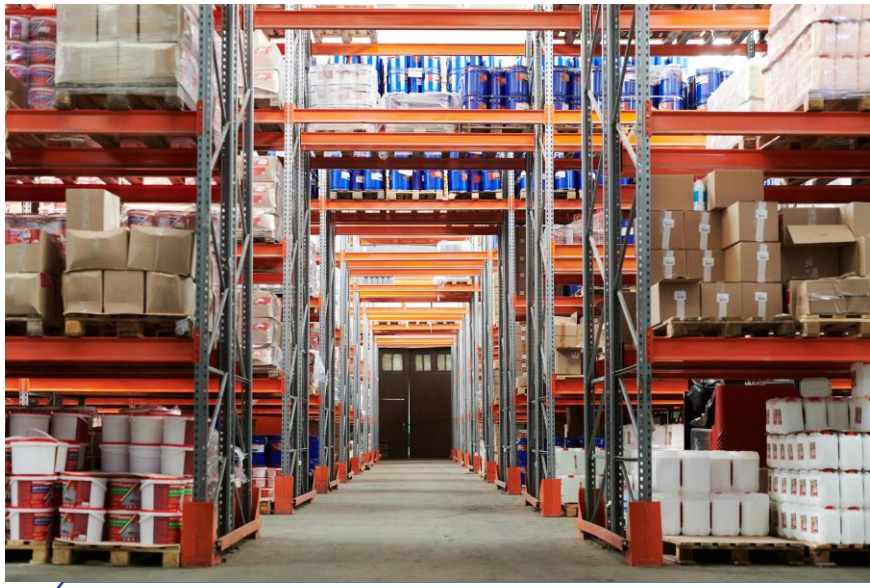
4.2.1 Mục đích là phát hiện, ghi nhận và mô tả các rủi ro cản trở việc đạt được các mục tiêu của tổ chức.

4.2.2 Một văn bản v/v Báo cáo nhận diện rủi ro tiềm ẩn phải được biên soạn, tổng hợp và trình lãnh đạo phê duyệt đối với từng đối tượng khảo sát (như tài sản, hoạt động vận hành…).

4.2 Nhận diện rủi ro (2)

4.2.3 Sử dụng kỹ thuật để nhận diện rủi ro (sự không chắc chắn) có thể ảnh hưởng đến mục tiêu của doanh nghiệp, như:

- Rà soát danh sách tài sản (hữu hình và vô hình) của doanh nghiệp;
- Hồ sơ kết quả đánh giá độc lập (từ đơn vị kiểm toán bên ngoài);
- Tìm hiểu sự cố và phân tích nguyên nhân gốc rễ (“root cause analysis”);
- Sử dụng Phụ lục A – ISO 27001;
- Hồ sơ đánh giá nội bộ;
- Khảo sát thực tế hoạt động vận hành;
- Rà soát lại các yêu cầu (dự án…);
- Thảo luận nhóm để có các ý tưởng về rủi ro;
- Phỏng vấn các bên liên quan;
- …



4.2 Nhận diện rủi ro (3)

4.2.4 Nhận diện rủi ro ATTT thông qua tìm điểm yếu (lỗ hổng bảo mật) và nhận ra mối đe dọa nào khai thác được điểm yếu:

- Dựa vào Yêu cầu về ATTT theo ISO 27001 và ISO 27002;
- Dựa vào Báo cáo Kết quả kiểm toán / Báo cáo đánh giá ATTT (từ các đơn vị kiểm toán ATTT bên ngoài)

4.2 Nhận diện rủi ro (4)

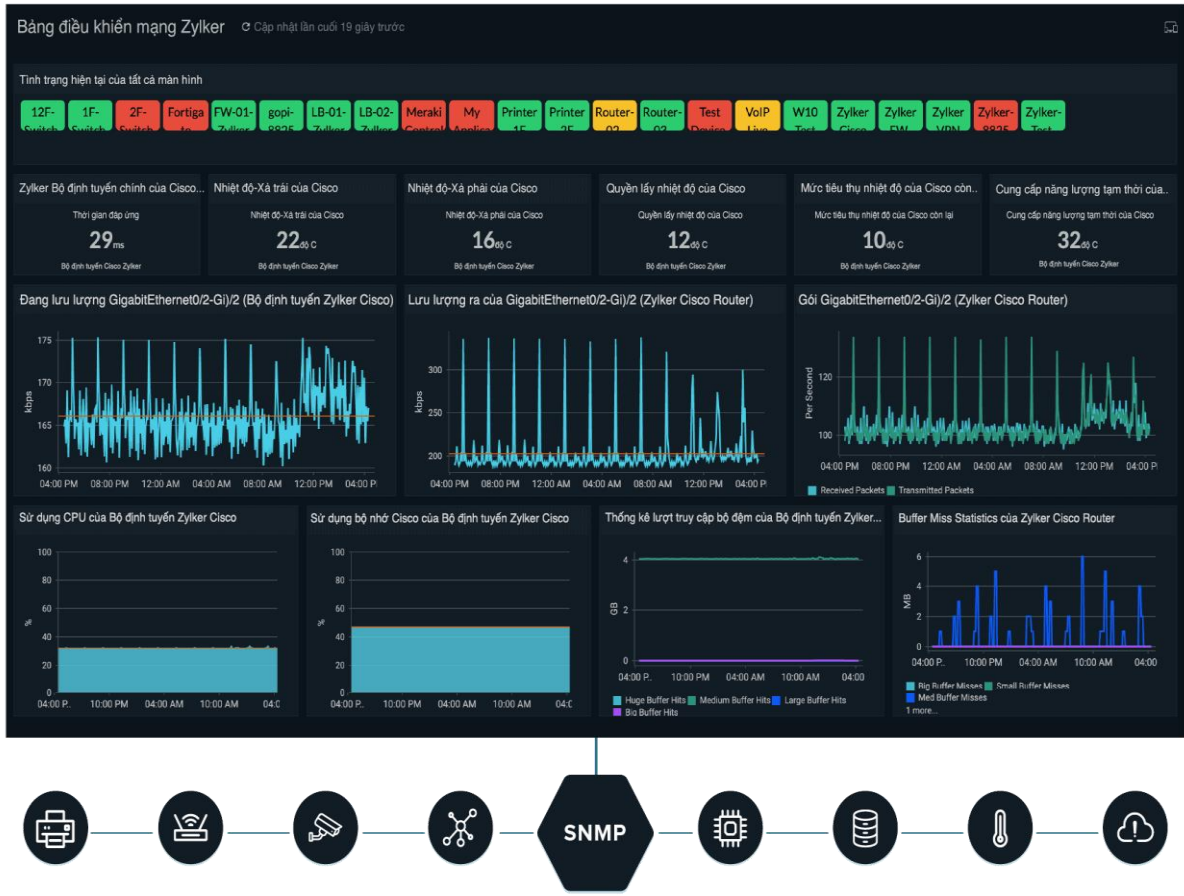
4.2.5 Các khu vực phát sinh rủi ro phổ biến:

- Quản lý tài sản (quản lý bản vá lỗi, chưa đăng ký tài sản, bảo trì,…)
- Các hệ thống "legacy" (do lỗi thời, thiếu bản vá, cần thay thế …);
- Mạng lưới liên kết;
- Công nghệ vận hành;
- Văn hóa bảo mật;
- Quản trị, rủi ro, tuân thủ;
- An ninh mạng, mô hình vận hành…

SSL 1.0
SSL 2.0

4.3 Phân tích rủi ro(1)

- Phân tích rủi ro cung cấp đầu vào cho việc định mức rủi ro, ra các quyết định xử lý rủi ro, cách thức xử lý, phương pháp và chiến lược xử lý rủi ro thích hợp nhất. (*)



4.3 Phân tích rủi ro (2)

- Mục đích của phân tích rủi ro là hiểu bản chất của rủi ro và các đặc trưng của rủi ro bao gồm cả mức độ rủi ro.
- Xem xét một cách chi tiết sự không chắc chắn, các nguồn rủi ro, các hệ quả, khả năng xảy ra, các sự kiện và thời gian, các kịch bản, các kiểm soát và hiệu lực của chúng…
- Các kỹ thuật phân tích rủi ro có thể định tính, định lượng hoặc kết hợp cả hai, tùy thuộc vào hoàn cảnh và mục đích sử dụng.

4.3 Phân tích rủi ro(3)

- Một văn bản v/v Báo cáo phân tích rủi ro có nội dung theo hướng dẫn trong ISO 31000:2018 (6.4.3) phải được biên soạn và trình lãnh đạo phê duyệt.

4.4 Định mức rủi ro (Risk Evaluation) (1)

- Mục đích định mức rủi ro là để hỗ trợ ra các quyết định.
- Xem xét lại các mục tiêu có thể bị ảnh hưởng bởi rủi ro.
- So sánh kết quả phân tích rủi ro với các tiêu chí rủi ro đã được thiết lập để xác định hành động ứng phó:
  - Không làm gì thêm;
  - Cân nhắc các phương án xử lý rủi ro;
  - Duy trì các kiểm soát hiện có;
  - Thiết lập các biện pháp kiểm soát mới hoặc dự phòng.

4.4 Định mức rủi ro (Risk Evaluation) (2)

- Một văn bản v/v Báo cáo định mức rủi ro có nội dung theo hướng dẫn trong ISO 31000:2018 (6.4.4) phải được biên soạn và trình lãnh đạo phê duyệt.(*)
- Báo cáo định mức rủi ro cần được lưu hồ sơ, trao đổi thông tin và được xác nhận giá trị sử dụng ở các cấp thích hợp trong tổ chức (doanh nghiệp).

05

Xử lý rủi ro (Risk Treatment)

5.1 Khái quát (General)

5.2 Lựa chọn các phương án xử lý rủi ro (Selection of risk options)

5.3 Chuẩn bị và thực hiện các kế hoạch xử lý rủi ro (Preparing and implementing risk treatment plans)

5.1 Khái quát

- Mục đích của xử lý rủi ro (‘Risk Treatment’) là lựa chọn và thực hiện các phương án để giải quyết rủi ro.
- Xử lý rủi ro liên quan đến quá trình lặp lại gồm:

- Hình thành và lựa chọn các phương án;
- Lập kế hoạch thực hiện việc xử lý;
- Đánh giá hiệu lực của việc xử lý đó;
- Quyết định xem rủi ro còn lại có chấp nhận được hay không;
- Nếu không chấp nhận được, thực hiện xử lý tiếp.

5.2 Lựa chọn các phương án xử lý rủi ro (1)

- Phương án xử lý rủi ro thích hợp nhất **phải cân đối giữa lợi ích và chi phí của doanh nghiệp**; có tính đến nghĩa vụ tuân thủ và cam kết của doanh nghiệp; phù hợp với các mục tiêu, các tiêu chí rủi ro và các nguồn lực sẵn có của doanh nghiệp…
- Việc xử lý rủi ro cũng có thể tạo ra những rủi ro mới hoặc có thể gây ra những hệ quả không mong muốn
- Một văn bản v/v Báo cáo kết quả lựa chọn phương án xử lý rủi ro có nội dung theo hướng dẫn trong ISO 31000:2018 (6.5.2) phải được biên soạn và trình lãnh đạo phê duyệt.

5.2 Lựa chọn các phương án xử lý rủi ro (2)

Các phương án xử lý rủi ro có thể là một hoặc nhiều nội dung sau:

- **Tránh né rủi ro** bằng cách quyết định không bắt đầu hoặc không tiếp tục hoạt động làm tăng rủi ro hoặc loại bỏ nguồn rủi ro;
- **Chấp nhận rủi ro** hoặc làm tăng rủi ro để theo đuổi một cơ hội;
- **Giảm rủi ro** bằng cách thay đổi khả năng xảy ra ('Likelihood') và/hoặc thay đổi hệ quả ('Impact/Severity/Consequence') của rủi ro;
- **Chuyển giao rủi ro** (như thông qua các hợp đồng, mua bảo hiểm);
- Phương án khác.

5.2 Lựa chọn các phương án xử lý rủi ro (3)

Các phương án xử lý rủi ro có thể là một hoặc nhiều nội dung sau:

5.3 Chuẩn bị và thực hiện các kế hoạch xử lý rủi ro

- Mục đích của kế hoạch xử lý rủi ro là quy định cách thức phương án xử lý đã được lựa chọn sẽ được triển khai và tiến trình so với kế hoạch đó có thể được theo dõi.
- Kế hoạch xử lý cần xác định rõ ràng trình tự theo đó việc xử lý rủi ro cần được thực hiện.
- Một mẫu văn bản v/v Kế hoạch xử lý rủi ro có nội dung theo hướng dẫn trong ISO 31000:2018 (6.5.3) phải được biên soạn và trình lãnh đạo phê duyệt.

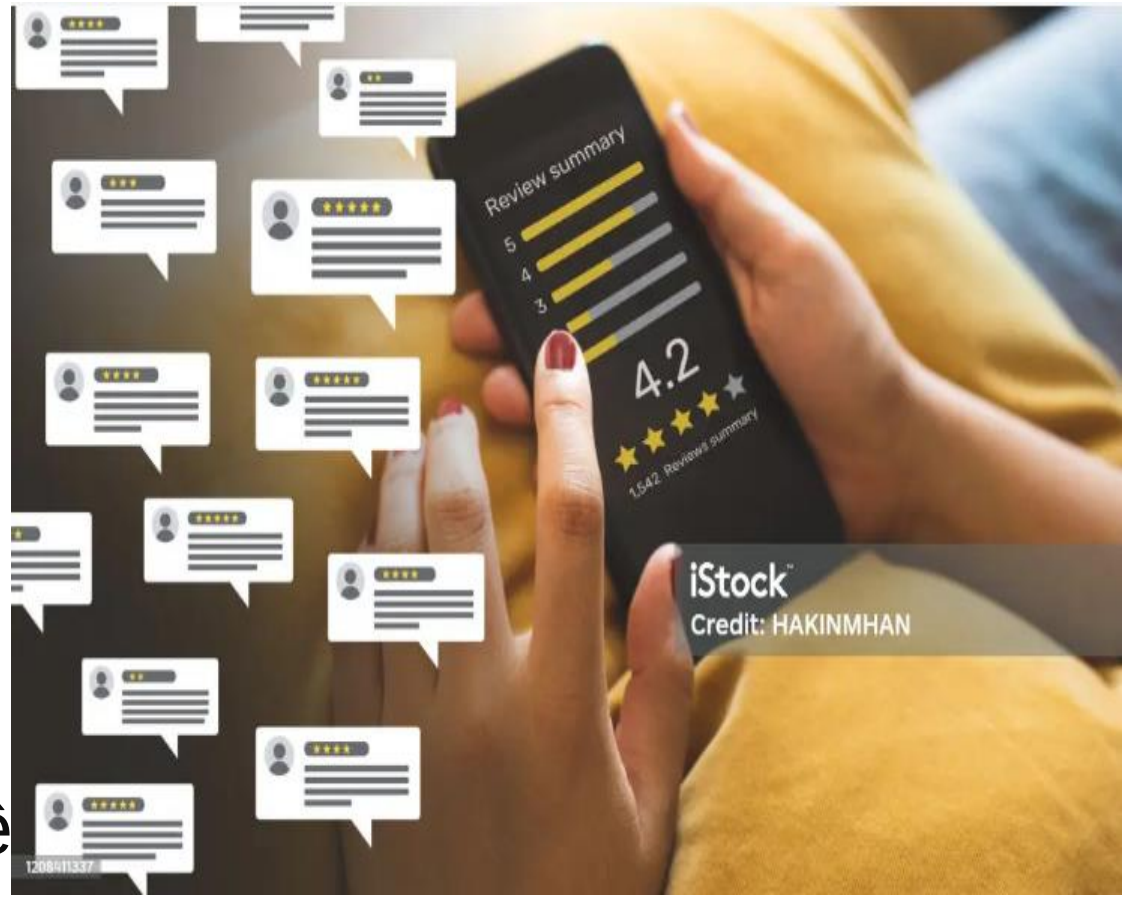
06

Theo dõi và Xem xét (Monitoring and review)

6. Theo dõi và xem xét

- Mục đích của theo dõi liên tục và xem xét định kỳ là cải tiến chất lượng, hiệu lực của việc thiết kế, áp dụng các biện pháp kiểm soát rủi ro và các kết quả của quá trình QLRR.

- Một văn bản v/v Báo cáo kết quả theo dõi và xem xét theo hướng dẫn trong ISO 31000:2018 (6.6) phải được biên soạn và trình lãnh đạo phê duyệt sau mỗi lần xem xét.



07

Cải tiến, lập hồ sơ và báo cáo (Improving,Recording and Reporting)

7. Cải tiến, lập hồ sơ và báo cáo(1)

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

7. Cải tiến, lập hồ sơ và báo cáo(2)

- Lập hồ sơ quá trình QLRR theo hướng dẫn trong ISO 31000:2018 (6.7) bao gồm các văn bản phát sinh trong từng hoạt động của quá trình QLRR và lưu trữ hồ sơ.
- Báo cáo cho các bên liên quan thông qua cơ chế thích hợp và theo yêu cầu về thông tin cụ thể của họ./.

Tài liệu tham khảo

- ISO 31000:2018 Risk management — Guidelines
- BS ISO/IEC 27005:2008 Information technology – Security techniques – Information Security Risk Management
- ISO/IEC 27002:2018 Information technology – Security techniques – Information Security Management Systems – Overview and vocabulary
- ISO/IEC 27001:2013 Information technology – Security techniques – Information Security Management Systems – Requirements

Hết Chương 5

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

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