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 1

Giới thiệu về QLRR - Phạm vi QLRR – Các thuật ngữ và định nghĩa

Định nghĩa rủi ro (Risk)

RISK (rủi ro)

1. Định nghĩa 1: Rủi ro (Risk) là tác động của sự không chắc chắn lên mục tiêu [ISO 31000:2018];

2. Định nghĩa 2: Rủi ro là sự kết hợp ba yếu tố: sự kiện tiềm ẩn (“potential event ”) **+ khả năng (xác suất) xảy ra** (“probability / likelihood”) **+ mức độ nghiêm trọng tiềm ẩn** (“Potential Severity / Impact / Consequence”);

3. Định nghĩa 3: Rủi ro ATTT liên quan đến khả năng các mối đe dọa khai thác được điểm yếu (hay lỗ hổng bảo mật) của tài sản thông tin và hệ quả là gây thiệt hại *(vật chất, danh tiếng, uy tín…)* **cho doanh nghiệp.**

Định nghĩa quản lý rủi ro (Risk Management)

Định nghĩa:

Quản lý rủi ro là các hoạt động phối hợp để chỉ đạo và kiểm soát một tổ chức liên quan đến rủi ro *('coordinated activities to direct and control an organization (3.50) with regard to risk'* - [ISO 27000, ISO 31000:2018]

Cách tiếp cận Quy trình trong quản lý rủi ro

- **Rủi ro được quản lý thông qua <u>Quy trình quản lý rủi ro</u>** (Chương 5)
- **Quy trình quản lý rủi ro là sự áp dụng có hệ thống các chính sách quản lý, thủ tục và thực hành vào các hoạt động truyền đạt, tham vấn, thiết lập bối cảnh và xác định, phân tích, đánh giá, xử lý, giám sát và rà soát rủi ro** *('systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context and identifying, analysing, evaluating, treating, monitoring and reviewing risk'*

Tiêu chí rủi ro (Risk Criteria)(1)

- **Tiêu chí rủi ro (Risk criteria) là điều khoản tham chiếu mà theo đó ý nghĩa của rủi ro được đánh giá** *('terms of reference against which the significance of risk is evaluated'* – [ISO 27000:2018])
- Trong quản lý rủi ro, tiêu chí rủi ro đề cập đến các tiêu chuẩn hoặc hướng dẫn đã được thiết lập được sử dụng để đánh giá *(cao → thấp)* và đo lường ý nghĩa của rủi ro *(mức độ nghiêm trọng)*, thường bao gồm các yếu tố như khả năng xảy ra *(cao → thấp)* và tác động *(lớn → nhỏ)*, đóng vai trò là điểm tham chiếu để doanh nghiệp xác định xem chiến lược quản lý rủi ro (Chương 6) nào được chọn để đối phó với rủi ro.

Tiêu chí rủi ro (Risk Criteria)(2)

- **Theo định nghĩa 2 về rủi ro thì định lượng rủi ro theo R=f(x,y):**

  x là khả năng xảy ra (hay xác suất xảy ra); và

  y là mức độ nghiêm trọng trong thiệt hại tài sản.

- Khả năng xảy ra rủi ro (x) và mức độ nghiêm trọng (y) có thể được xếp hạng theo thang đo từ 1 – 5 (hoặc từ 1 – 6 hay thang đo chi tiết hơn) trong bảng tiêu chí rủi ro (“Risk Criteria”) còn gọi là ma trận rủi ro (Risk matrix).

Tiêu chí rủi ro (Risk Criteria)[3]

3.13 Risk criteria *(tiếp)* – *Risk matrix*

Xếp hạng rủi ro, khả năng xảy ra và hậu quả được trình bày theo ma trận rủi ro:

Consequences / Impact							
	Catastrophic	5	5	10	15	20	25
	Major	4	4	8	12	16	20
	Moderate	3	3	6	9	12	15
	Minor	2	2	4	6	8	10
	Insignificant	1	1	2	3	4	5
			1	2	3	4	5
			Rare	Unlikely	Possible	Likely	Almost certain
Likelihood / Probability							

Tiêu chí rủi ro (Risk Criteria)(4)

	KHẢ NĂNG XẢY RA ("Likelyhood, probability")			
	KHẢ NĂNG XẢY RA (định tính)		KHẢ NĂNG / XÁC SUẤT XẢY RA (định lượng)	
			TẦN SUẤT	*TỶ LỆ %*
1	Rare	Có thể không bao giờ xảy ra hay lập lại	*Ví dụ: không chắc xảy ra trong 5 năm*	*Ví dụ: ~ 0%*
2	Unlikely	Không mong đợi xảy ra hay lập lại nhưng có thể làm như vậy	*Ví dụ: 1 đến 2 lần thời gian <5 năm*	*Ví dụ: 10%*
3	Possible	Thỉnh thoảng có thể xảy ra	*Ví dụ: 1 đến 2 lần/năm*	*Ví dụ: 20%*
4	Likely	Sẽ xảy ra hay lập lại nhưng không là một tình huống kéo dài hay dai dẳng	*Ví dụ: 1 đến 2 lần/tháng*	*Ví dụ: 30%*
5	Almost certain	Chắc chắn xảy ra hay lập lại, có thể thường xuyên	*Ví dụ: 1 đến 2 lần/tuần*	*Ví dụ: 100%*

Tiêu chí rủi ro (Risk Criteria)

	TÁC ĐỘNG / HẬU QUẢ / TÍNH NGHIÊM TRỌNG ("Impact / Consequence / Severity")		
1	**Negligible**	Không đáng kể	*Ví dụ:* *= trị giá bằng tiền là < 100 triệu đồng*
2	**Minor**	Nhỏ	*Ví dụ:* *= trị giá bằng tiền là từ 100 – <500 triệu đồng*
3	**Moderate**	Trung bình	*Ví dụ:* *= trị giá bằng tiền là từ 500 - < 1tỷ đồng*
4	**Major**	Lớn	*Ví dụ:* *= trị giá bằng tiền là từ 1 tỷ đến < 5tỷ đồng*
5	**Catastrophic**	Thảm khốc	*Ví dụ:* *= trị giá bằng tiền là ≥ 5 tỷ đồng*

Phạm vi quản lý rủi ro an toàn thông tin (QLRR ATTT)

- Môn học QLRR ATTT hướng dẫn SV về quản lý các rủi ro an toàn thông tin trong doanh nghiệp theo tiêu chuẩn ISO 31000:2018 có kết hợp với ISO 27000:2018, ISO 27001:2013, ISO 27002:2013, ISO 27005:2008 và ISO 22301:2019. Việc áp dụng các hướng dẫn có thể được điều chỉnh cho phù hợp với tổ chức theo bối cảnh.
- Sử dụng tiêu chuẩn ISO 31000:2018 về QLRR cung cấp một phương pháp tiếp cận chung để quản lý mọi loại hình rủi ro và không quy định cụ thể cho ngành hoặc lĩnh vực nào.

Quy trình quản lý rủi ro an toàn thông tin (QLRR ATTT)

- Để bảo vệ tính bảo mật, toàn vẹn và khả dụng của thông tin, doanh nghiệp phải áp dụng quy trình quản lý rủi ro ATTT.
- Quy trình quản lý rủi ro ATTT được áp dụng để xác định các rủi ro liên quan đến việc mất tính bảo mật, toàn vẹn và khả dụng của thông tin trong phạm vi quản lý của hệ thống quản lý ATTT.

Hết Tóm tắt Chương 01

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

(*)Một số hình minh họa được tải từ trang https://www.pixabay.com/; https://www.freepik.com/free-photos-vectors/; https://www.pexels.com/;