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

Học kỳ 2 - Năm học 2024 - 2025

Nội dung môn học

Chương 1: Giới thiệu về quản lý rủi ro - Phạm vi - Các thuật ngữ và định nghĩa

Chương 2*: Mối đe dọa, Điểm yếu và Rủi ro (Threats, Vulnerabilities and Risks)

Chương 3: Các nguyên tắc quản lý rủi ro (Principles)

Chương 4: Khuôn khổ quản lý rủi ro (Framework)

Chương 5*: Quy trình quản lý rủi ro (Process)

Chương 6*: Chiến lược quản lý rủi ro (Risk Strategy)

Chương 7*: Quản lý rủi ro theo FMEA (Failure mode and Effects Analysis)

Chương 8: Kế hoạch hoạt động liên tục (Business Continuity Plan)

Chương 9*: Các chỉ số rủi ro trọng yếu (Key Risk Indicators)

Chương 01

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

1.1 Giới thiệu về QLRR

1.1.1 Tầm quan trọng của QLRR

1.1.2 Thuộc tính của rủi ro (khả năng xảy ra / xác xuất xảy ra và ảnh hưởng của rủi ro)

1.2 Phạm vi QLRR

1.3 Các thuật ngữ và định nghĩa về RR và QLRR theo ISO 31000:2018, ISO 27001:2013 và ISO 27000:2018

Chương 02

Mối đe dọa, Điểm yếu và Rủi ro

2.1 Mối đe dọa

2.2 Lỗ hổng / Điểm yếu

2.3 Các mục tiêu kiểm soát, biện pháp kiểm soát và nhận diện rủi ro có liên quan đến 14 hạng mục an toàn thông tin theo Phụ lục A ISO 27001:2013

Chương 03

Các nguyên tắc quản lý rủi ro (Principles)

3.1 Mục đích QLRR
3.2 Các nguyên tắc QLRR (principles)
- a) Được tích hợp (Integrated)
- b) Có cấu trúc và toàn diện (Structured and Comprehensive)
- c) Được tùy chỉnh (Customized)
- d) Sự tham gia (Inclusive)
- e) Tính động (Dynamic)
- f) Thông tin sẵn có tốt nhất (Best Available Information)
- g) Yếu tố con người và văn hóa (Human and Cultural Factors)
- h) Cải tiến liên tục (Continual Improvement)

Chương 04

Khuôn khổ quản lý rủi ro (Framework)

4.1 Khái quát (General)

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

4.3 Tích hợp (Intergration)

4.4 Thiết kế (Design)

4.5 Áp dụng (Implementation)

4.6 Xem xét đánh giá (evaluation)

4.7 Cải tiến (Improvement)

Chương 05

Quy trình quản lý rủi ro (Process)

5.1 Khái quát (General)

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

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

5.4 Đánh giá (Risk Assessment)

5.5 Xử lý rủi ro (Risk Treatment)

5.6 Theo dõi và xem xét (Monitoring and review)

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

Chương 06

Chiến lược quản lý rủi ro

6.1 Khái quát (General)

6.1.1 Mục đích của doanh nghiệp (Purpose/Aim of Enterprise)

6.1.2 Mục tiêu của doanh nghiệp (Target/Goal/Objective of Enterprise)

6.2 Các định nghĩa chiến lược

6.2.1 Chiến lược là gì?

6.2.2 Chiến lược kinh doanh / chiến lược hoạt động của doanh nghiệp

6.2.3 Yêu cầu về chiến lược QLRR của doanh nghiệp

6.3 Chiến lược QLRR (Risk Strategy)

6.3.1 Chấp nhận RR (Risk Acceptance)

6.3.2 Giảm nhẹ RR (Risk Mitigation)

6.3.3 Tránh RR (Risk Avoidance)

6.3.4 Chuyển giao RR (Risk Transfer)

Chương 07

Triển khai công cụ (phương pháp) FMEA / FMECA cho Quản Lý Rủi Ro

7.1 Khái quát và định nghĩa FMEA

7.2 Khái quát và định nghĩa FMECA

7.3 Triển khai công cụ FMEA

7.4 Triển khai công cụ FMECA

7.5 Kế hoạch hành động

Chương 08

Kế hoạch hoạt động liên tục (BUSINESS CONTINUITY PLAN)

8.1 Khái quát (General)

8.2 Vai trò của BCP (Roles of the BCP)

8.3 Quy trình thực hiện (Implementation by process)

Chương 09

CÁC CHỈ SỐ RỦI RO CNTT TRỌNG YẾU (Key Risk Indicators)

9.1 Bảng các chỉ số rủi ro trọng yếu (KRI)

9.2 Giải thích KRI

Ôn tập – Dự trữ

Một số điểm cần lưu ý

1. QLRR - Quản trị rủi ro (‘Risk MANAGEMENT’);
2. ATTT - An toàn thông tin (‘Information security’) (Bảo mật thông tin);
3. Thời gian: từ tuần 17/02/2025 – 03/05/2025 (10 tuần) tiết 234 (08g15 – 10g30): *có điểm danh; Lợi ích của việc điểm danh?*
4. Kỹ năng: tiếng Anh đọc hiểu tài liệu tiêu chuẩn *(ISO 31000, ISO 27001, ISO 27002, ISO 27005,…)*;
5. Khuyến nghị: học nhóm và làm bài tập theo nhóm;
6. Lưu hồ sơ cá nhân: các email giao tiếp với giảng viên và điểm số nhận được.

Một số điểm cần lưu ý

1. Kiểm tra quá trình để lấy điểm quá trình A1 (25%): có 4-5 bài tập cá nhân và 5 bài tập Nhóm theo từng Chương;
2. Kiểm tra giữa kỳ (bài thực hành) để lấy điểm thực hành A2 (25%): 60 câu trắc nghiệm trong 90 – 120 phút tại lớp;
3. Kiểm tra cuối kỳ để lấy điểm cuối kỳ A3 (50%): 20 câu trắc nghiệm và câu hỏi Tự luận (QLRR) trong 90 phút tại lớp.

CÁC YÊU CẦU KHÁC ĐỐI VỚI SINH VIÊN(1)

SINH VIÊN XEM NHƯ ĐÃ CÓ KIẾN THỨC VỀ:

- Mạng máy tính và truyền thông;
- Lý thuyết về mạng LAN, WAN, MPLS….;
- Mô hình mạng 7 lớp (OSI) và 4 lớp…;
- Các thiết bị mạng như router, switch, firewall, IDS/IPS …;
- Các giao thức mạng, thuật toán, ngôn ngữ lập trình, cơ sở dữ liệu…;
- An toàn mạng máy tính…;
- v.v.

CÁC YÊU CẦU KHÁC ĐỐI VỚI SINH VIÊN(2)

SINH VIÊN nên:

- **Giao tiếp với GV qua EMAIL MS OUTLOOK (Email cá nhân mà UIT đã cấp) hoặc Q/A tại lớp;**
- **Dành 5 phút/ngày KIỂM TRA EMAIL (check mail);**

(*)Khi phát sinh nhu cầu giao tiếp theo hình thức khác, giảng viên sẽ thông báo trước cho cả lớp.

CÁC YÊU CẦU KHÁC ĐỐI VỚI SINH VIÊN(3)

- **MỖI SINH VIÊN PHẢI CÓ MỤC TIÊU HỌC TẬP PHÙ HỢP;**
- **MỖI SINH VIÊN phải luôn nhớ về mục tiêu học tập của mình:**

Ví dụ: Một sinh viên có thể có 3 mục tiêu học tập như sau:

- *Đạt điểm trung bình các môn học ≥ 7 điểm;*
- *Giữ được học bổng đã từng nhận – ví dụ 15 triệu đồng VN;*
- *Tốt nghiệp đúng ngày – ví dụ là ngày 01/10/2025 (theo như kế hoạch giảng dạy tại UIT)*

- **Mục tiêu học tập phải chi phối mọi suy nghĩ, mọi hành động và mọi quyết định của SINH VIÊN trong khi học môn học QLRR ATTT… ở UIT; đặc biệt là khi làm bài kiểm tra (ví dụ kiểm tra 15 phút, KTGK, KTCK) thì phải luôn nhớ đến mục tiêu học tập.**

CÁC YÊU CẦU KHÁC ĐỐI VỚI SINH VIÊN(4)

SINH VIÊN PHẢI TỰ ĐỀ RA MỘT CHIẾN THUẬT KHI LÀM BÀI KIỂM TRA MÔN HỌC QLRR ATTT, cụ thể:

- **Chiến thuật phải có liên hệ đến mục tiêu học tập;**
- **Chiến thuật không làm phát sinh rủi ro có thể phá hỏng việc hoàn thành mục tiêu học tập;**
- **Câu nào làm trước – Câu nào làm sau để có thể đạt điểm tốt nhất mà không gặp rủi ro.**

CÁC YÊU CẦU KHÁC ĐỐI VỚI SINH VIÊN(5)

Sinh viên:

- **Cố gắng thu xếp thời gian tham dự các buổi kiểm tra tại Lớp theo đúng lịch đã báo trước.**
- **Không tham dự kiểm tra theo lịch đã báo trước sẽ gặp khó khi dự buổi kiểm tra lại lần 2 dành cho những ai vắng mặt lần 1. Khó khăn đó là gì?**
  - **ĐỀ kiểm tra lần 2 sẽ khó hơn ĐỀ kiểm tra lần 1;**
  - **Không được các thành viên trong Nhóm hỗ trợ;**
  - **Hiểu sai đề bài hoặc bị lạc đề.**

CÁC YÊU CẦU KHÁC ĐỐI VỚI SINH VIÊN(6)

Sinh viên:

- **Phải (hoặc nên) luôn tìm kiếm và kết bạn để có nhiều mối <u>QUAN HỆ</u> *('Relationship')* trong xã hội.**
- **Phải (hoặc nên) tham gia làm thành viên các hội, nhóm, diễn đàn… có liên quan đến ngành nghề CNTT, QLRR và ATTT để gầy dựng QUAN HỆ.**

CÁC YÊU CẦU KHÁC ĐỐI VỚI SINH VIÊN(7)

Sinh viên học môn QLRR và ATTT phải:

- **Tham gia Nhóm học tập – mỗi nhóm từ 5 – 7 thành viên;**
- **Tham gia vào Nhóm của Lớp trưởng nếu như sinh viên không thể tham gia vào bất cứ Nhóm nào khác;**
- **Các sinh viên chưa được Nhóm nào kết nạp hoặc không muốn làm việc với các Nhóm đã có thì nên gặp nhau để hình thành Nhóm mới.**

TRẢ LỜI MỘT SỐ CÂU HỎI CỦA SINH VIÊN(1)

Câu 1st:

Tại sao học QLRR ATTT …là học về ISO 31000, ISO 27005, ISO 27001, ISO 27002 mà không học theo các giáo trình khác?

Trả lời: Học theo chuẩn ISO để:

- ***Không gặp trở ngại khi giao tiếp về QLRR và ATTT;***
- ***Có thể truyền đạt kiến thức với đồng nghiệp;***
- ***Xin việc làm ở các doanh nghiệp lớn (ngân hàng, tập đoàn…);***
- ***Cải tiến hoạt động QLRR theo cách thức định lượng: Tạo giá trị - Đo lường – Phân tích – Quản lý – Kiểm soát – Cải tiến***
- v.v.

TRẢ LỜI MỘT SỐ CÂU HỎI CỦA SINH VIÊN(2)

Câu 2nd:

Tại sao không học phiên bản ISO 27001: 2022 mà lại học phiên bản ISO 27001:2013?

Trả lời:

- ***Phiên bản 2013 có nhiều doanh nghiệp ở VN áp dụng hơn (doanh nghiệp thường chỉ muốn chọn đúng người biết làm về ISO 27001:2013);***
- ***Học phiên bản 2013 là căn bản, làm cơ sở để SV tự nghiên cứu phiên bản 2022;***
- ***Đa số các doanh nghiệp tại VN đạt chứng nhận ATTT theo ISO 27001:2013 thay vì ISO 27001:2022;***
- ***Phiên bản 2013 có nhiều tài liệu hơn (như bài học kinh nghiệm, phương pháp triển khai v.v.) trên mạng để SV sưu tầm và học hỏi.***
- ***v.v.***

TRẢ LỜI MỘT SỐ CÂU HỎI CỦA SINH VIÊN(3)

Câu 3rd:

Tài liệu học tập nên gửi qua trang Courses hay qua Email (Outlook)?

Trả lời:

- ***Tất cả Tài liệu học tập như giáo trình, bài tập, biểu mẫu, tài liệu tham khảo đều gửi qua trang Courses;***
- ***Các nội dung như yêu cầu đối với bài tập, kết quả bài làm, bảng điểm, nội dung hướng dẫn cách làm bài tập, lời mách nước (tips), lời khuyên và các nội dung có tính riêng tư… sẽ gửi qua Email;***

(*)Lưu ý: SV không nên đòi hỏi giảng viên phải gửi tài liệu học tập giống với các giảng viên khác khi giảng dạy chỉ để thuận lợi cho SV học.

TRẢ LỜI MỘT SỐ CÂU HỎI CỦA SINH VIÊN(4)

Câu 4th:

Đề thi môn học này mang tính chất quan điểm phụ thuộc vào người làm đề, không có tính khách quan cao. Đề thi không rõ ràng, gây tốn thời gian khi thi….?

Trả lời:

- ***Người soạn đề có thể chứng minh tính đúng sai của đáp án của đề thi bằng cách đưa ra bằng chứng là đã có nhiều người nhiều tổ chức dùng đáp án này để giải bài toán tương tự;***
- ***Người soạn đề đã có quá trình làm việc lâu năm và không gặp sự cố trong khi hành nghề tại các doanh nghiệp;***
- ***Nếu ai đó hoặc SV cho là lời giải của mình đúng hơn đáp án của người soạn đề; hãy đưa ra bằng chứng có tính thuyết phục hơn đáp án.***

TRẢ LỜI MỘT SỐ CÂU HỎI CỦA SINH VIÊN(5)

Câu 5th:

Học QLRR và ATTT…áp dụng vào công việc gì tại doanh nghiệp?

Trả lời:

- ***Các doanh nghiệp cần lao động nhận sinh viên vào làm việc thường đưa vào các đội dự án để triển khai dự án mới tạo ra sản phẩm/dịch vụ mới cho doanh nghiệp thay vì làm các công việc lập lại mỗi ngày;***
- ***Sinh viên phải có kiến thức và kỹ năng viết / đọc các tài liệu để có thể biên soạn hay góp ý nội dung QLRR và ATTT…đối với sản phẩm/dịch vụ mới:***
  - ***Báo cáo nghiên cứu khả thi / Báo cáo kinh tế kỹ thuật của dự án;***
  - ***Soạn Đề nghị mời thầu (Request for proposal/information (RFP/RFI); …***
- ***Sinh viên được đưa vào làm việc tại các phòng nghiệp vụ có yêu cầu về kiến thức QLRR và ATTT để phối hợp với bộ phận chuyên trách về QLRR và ATTT (đã có) lập hồ sơ về QLRR và ATTT cho doanh nghiệp;***
- ***v.v.***

TRẢ LỜI MỘT SỐ CÂU HỎI CỦA SINH VIÊN(6)

Câu 6th:

Học QLRR và ATTT theo ISO 27001:2013 và ISO 27005:2008 có thể áp dụng vào công việc gì tại doanh nghiệp?

Trả lời:

- ***Kiểm toán viên ATTT CNTT (IT Security Auditor);***
- ***Nhân viên ATTT CNTT (IT security staff/executive/officer);***
- ***Thành viên đội dự án triển khai ISO 27001:2013 (2022);***
- ***v.v.***

CÁC CÔNG VIỆC TẠI DOANH NGHIỆP CÓ YÊU CẦU QLRR

- Quản trị mạng (‘Network administration’);
- Quản trị hệ thống (‘System administration’);
- Quản trị sản phẩm/thiết bị (‘Product/Device management’);
- Quản lý sự thay đổi (‘Change management’);
- Quản lý hoạt động mua sắm (‘Procurement management’);
- Quản lý hoạt động triển khai (‘Implementation management’);
- Phân tích kinh doanh (‘Business Analysis’);
- Quản trị quy trình (‘Process Management’)

CÁC CÔNG VIỆC TẠI DOANH NGHIỆP CÓ YÊU CẦU QLRR

➢ **Quản trị dự án (‘Project management’):**

- **Biên soạn bản Yêu cầu đề xuất (’Request for Proposal’);**
- **Biên soạn kế hoạch triển khai dự án (‘Project implementation’);**
- **Biên soạn Hợp đồng dịch vụ (‘Service Contract’);**
- **Soạn Biên bản nghiệm thu (‘Acceptance report’)**

CÁC CÔNG VIỆC TẠI DOANH NGHIỆP CÓ YÊU CẦU QLRR

➢ **Bản Yêu cầu đề xuất (’Request for Proposal’);**

- Yêu cầu đề xuất (RFP) là yêu cầu mở cho việc đấu thầu hoàn thành một dự án mới do công ty hoặc tổ chức khác phát hành đề xuất.

CÁC CÔNG VIỆC TẠI DOANH NGHIỆP CÓ YÊU CẦU QLRR

➢Bản Yêu cầu đề xuất (’Request for Proposal’);

- Yêu cầu đề xuất (RFP) là một tài liệu kinh doanh công bố một dự án, mô tả dự án và mời thầu từ các nhà thầu đủ điều kiện để hoàn thành dự án.
- Hầu hết các tổ chức thích triển khai dự án của họ bằng RFP và nhiều chính phủ luôn sử dụng chúng.
- Khi sử dụng RFP, đơn vị yêu cầu đấu thầu có trách nhiệm đánh giá tính khả thi của các hồ sơ dự thầu đã nộp, tình hình tài chính của các công ty đấu thầu và khả năng thực hiện dự án của từng đơn vị đấu thầu.

CÁC CÔNG VIỆC TẠI DOANH NGHIỆP CÓ YÊU CẦU QLRR

➢Bản Yêu cầu đề xuất (’Request for Proposal’);

- RFP là một tài liệu mà một doanh nghiệp, tổ chức phi lợi nhuận hoặc cơ quan chính phủ tạo ra để phác thảo các yêu cầu cho một dự án cụ thể - luôn có yêu cầu về quản lý rủi ro.
- Quy trình RFP giúp thu thập giá thầu từ các nhà cung cấp và xác định nhà cung cấp nào đủ điều kiện nhất để hoàn thành dự án.
- RFP đảm bảo các đề nghị từ các nhà cung cấp khác nhau.

Hết

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