



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 7 Triển khai phương pháp FMEA / FMECA cho QLRR

Nội dung

01

Khái quát (General)

02

Các định nghĩa về FMEA

03

Các định nghĩa về FMECA

04

Triển khai phương pháp FMEA và FMECA

05

Kế hoạch hành động (Action Plan)

7.1

Khái quát (General)



7.1 Khái quát (General) ⁽¹⁾

- Phân tích ảnh hưởng và phương thức lỗi (FMEA) là một mô hình hay phương pháp tiếp cận có hệ thống được sử dụng để xác định những lỗi tiềm ẩn trong một hệ thống, thiết bị, quy trình, sản phẩm hoặc dịch vụ. Phương pháp này được phát triển ở Mỹ từ những năm 1940.



7.1 Khái quát (General) (2)

- Trước khi đưa một quy trình vào hệ thống vận hành, người ta dùng FMEA phân tích tất cả các bước của quy trình; phân tích các thành phần, tổ hợp và hệ thống con có liên quan khi vận hành quy trình để xác định các dạng lỗi tiềm ẩn và ảnh hưởng của chúng lên hệ thống.



7.1 Khái quát (General) ⁽³⁾

- FMEA được sử dụng để xác định các phương thức lỗi hay chế độ hư hỏng hay dạng lỗi (“Failure Mode”) có thể xảy ra, các tác động (“Effect / Impact / Consequence/...”) liên quan của chúng lên hệ thống cũng như khả năng xảy ra và mức độ nghiêm trọng (“Severity”) của từng dạng lỗi.

7.1 Khái quát (General) (4)

➤ Lợi ích của QLRR theo phương pháp FMEA:

FMEA giúp doanh nghiệp dự đoán các vấn đề (lỗi/thất bại/sai sót/hư hỏng hay sự cố...) trước khi chúng xảy ra, cho phép thực hiện các biện pháp phòng ngừa nhằm đáp ứng với sự cố, giảm thiểu rủi ro, giảm chi phí khắc phục, cải thiện chất lượng và đảm bảo cung cấp sản phẩm hoặc dịch vụ đảm bảo chất lượng cho khách hàng.

7.1 Khái quát (General) ⁽⁵⁾

➤ Mục đích của FMEA:

FMEA đề xuất thực hiện các hành động để loại bỏ hoặc giảm thiểu cơ hội xảy ra lỗi (thất bại/sai sót/hư hỏng/sự cố...), xếp hạng các lỗi theo mức độ nghiêm trọng và bắt đầu từ những lỗi (thất bại/sai sót/hư hỏng/sự cố...) có mức độ ưu tiên cao nhất (Criticality / Risk priority number (RPN)).

7.1 Khái quát (General) (6)

➤ Mục đích của FMEA (tiếp theo):

Sử dụng Phụ lục A – ISO 27001:2013 để kiểm tra ATTT tại doanh nghiệp, đã phát hiện ra các rủi ro sau:

Stt	Rủi ro tiềm ẩn được người kiểm tra ATTT phát hiện	Xếp hạng theo 'Severity'
1	Vi phạm yêu cầu về việc rà soát chính sách theo Thông tư của NHNN, ISO 27001, PCI DSS có thể giúp Hacker khai thác lỗ hổng trong chính sách, quy trình lỗi thời để tấn công vào hệ thống thông tin (phát hiện tại A.5.1.2)	[Vị trí xếp hạng là...?]
2	Tổ chức không có danh sách tài sản có thể mất tài sản mà không biết (tại A.8.1.1)	[Vị trí xếp hạng là...?]
3	Doanh nghiệp không có chính sách liên quan đến kiểm soát mật mã khiến thông tin nhạy cảm có thể bị lộ ra ngoài, mất mát dữ liệu (tại A.10.1.1)	[Vị trí xếp hạng là...?]
4	Ngân hàng có thể bị ngừng hoạt động vì không có kế hoạch kinh doanh liên tục (tại A.17.1.1)	[Vị trí xếp hạng là...?]
5	Doanh nghiệp có thể bị rò rỉ thông tin bí mật do không ký thỏa thuận bảo mật thông tin (NDA) với nhà thầu và nhân viên (tại A.13.2.4)	[Vị trí xếp hạng là...?]
6	Nhân viên trong doanh nghiệp có thể đánh cắp các dữ liệu nhạy cảm của doanh nghiệp do Phòng Tổ chức tuyển dụng không sàng lọc hồ sơ nhân viên mới ngay từ các giai đoạn tuyển chọn (tại A.7.1.1)	[Vị trí xếp hạng là...?]
...	...	

7.2

Các định nghĩa về FMEA

7.2.1 Định nghĩa về FMEA và thuật ngữ dùng trong FMEA

7.2.2 Sử dụng FMEA

7.2.3 Thủ tục thực hiện FMEA

7.2.1 Định nghĩa về FMEA và thuật ngữ liên quan⁽¹⁾

- “Failure” từ tiếng Anh có nghĩa là sự thất bại, lỗi, sai sót, hư hỏng, sự trục trặc, sự cố, sự không làm được (việc gì)...Lỗi là bất kỳ sai sót hoặc khiếm khuyết nào, đặc biệt là những sai sót ảnh hưởng đến khách hàng, ảnh hưởng đến vận hành; và có thể tiềm ẩn hoặc thực tế.
- FMEA là từ viết tắt của “**Failure Mode and Effects Aalysis” (Phân tích ảnh hưởng (tác động) và phương thức lỗi).**

()Chú ý: Tài liệu (slides) này sử dụng từ “lỗi” tại tất cả các slides trình bày nhưng các từ tương đương hay đồng nghĩa với từ “lỗi” có trong định nghĩa “Failure” vẫn có thể được dùng mà không có sự khác biệt.*

7.2.1 Định nghĩa về FMEA và thuật ngữ liên quan⁽²⁾

- “**F**ailure **M**ode” là phương thức lỗi hay tình huống nguy hiểm. Một tình huống nguy hiểm (“*a hazardous situation*”) có thể được gọi là “*a failure mode*” và được kích hoạt bởi một nguyên nhân hư hỏng.
- “A risk” (một rủi ro) được định nghĩa là một tình huống nguy hiểm (“*a hazardous situation*”) theo ISO 14971. Một rủi ro chính là một “Failure mode” (phương thức lỗi) theo định nghĩa như trên.

7.2.1 Định nghĩa về FMEA và thuật ngữ liên quan⁽³⁾

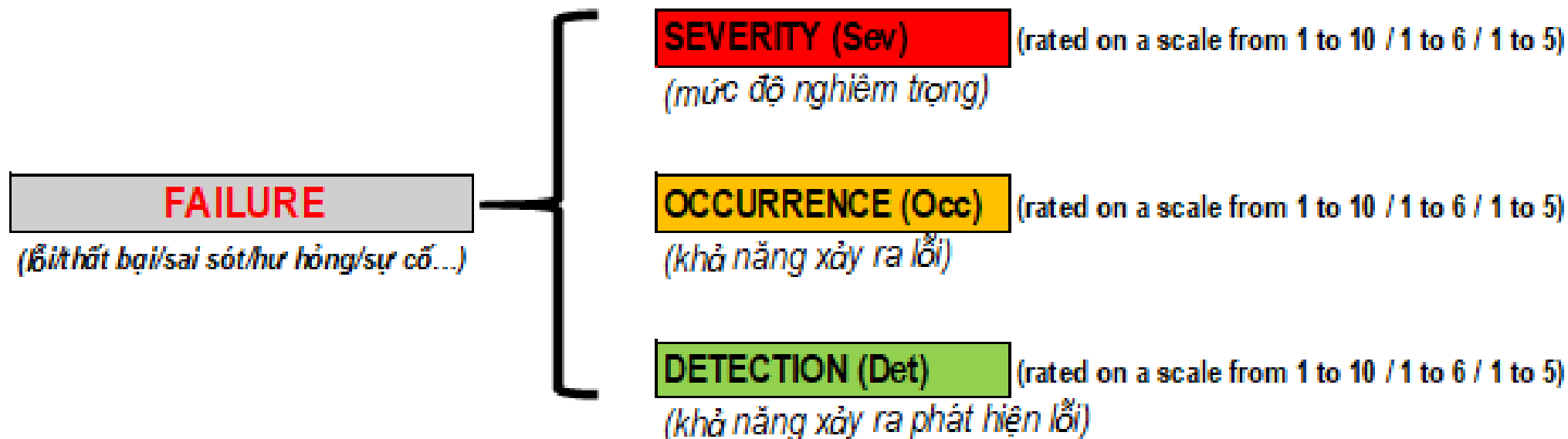
- Phân tích tác động (ảnh hưởng) và phương thức lỗi (FMEA) là phương pháp phân tích, tiếp cận từng bước để xác định tất cả các lỗi tiềm ẩn có thể xảy ra trong thiết kế, quy trình sản xuất hoặc lắp ráp hoặc sản phẩm hoặc dịch vụ hoặc dự án. Nó là một công cụ phân tích quy trình.
- ❑ Phân tích tác động (“Effects Analysis”)^(*) là việc nghiên cứu sự thay đổi (“*change*”) là hậu quả (“*consequence*”) hay kết quả (“*result*”) sinh ra khi lỗi xảy ra.

7.2.1 Định nghĩa về FMEA và thuật ngữ liên quan⁽⁴⁾

- ❑ Phương thức lỗi (“Failure mode”) là cách thức mà một đối tượng hay một điều gì đó (hệ thống, thiết bị, quy trình, sản phẩm, dịch vụ,...) có thể bị lỗi. Ví dụ: Các thiết bị cơ khí có 4 “failure mode” là: ăn mòn (“corrosion”), xói mòn (“erosion”), mỏi (“fatigue”) và quá tải (“overload”).

7.2.1 Định nghĩa về FMEA và thuật ngữ liên quan⁽⁵⁾

- Các lỗi (“Failures”) và phương thức lỗi (“Failure mode”) được phân tích và xếp hạng ưu tiên theo mức độ nghiêm trọng (“Severity”) của hậu quả khi lỗi xảy ra, khả năng xảy ra lỗi (“Occurrence”) và khả năng phát hiện lỗi (“Detection”).(*)



7.2.1 Định nghĩa về FMEA và thuật ngữ liên quan⁽⁶⁾

- **Mức độ nghiêm trọng của lỗi** (là mức độ tác động của Rủi ro hoặc mức độ nghiêm trọng của rủi ro) (**“Severity”/ “Sev”**) là số xếp hạng mức độ tác hại dự kiến hoặc tác động bất lợi có thể xảy ra do tiếp xúc với Rủi ro. Mức độ nghiêm trọng đo lường mức độ tồi tệ có thể xảy ra nếu một rủi ro cụ thể xảy ra. “Severity” (là “Impact”) có giá trị định lượng đo lường từ 1 đến 5 (hoặc 1 – 6 / 1 - 10) nếu sử dụng thang đo điểm đánh giá từ 1 đến 5 (hoặc 1 – 6 / 1 – 10 tương ứng). Giá trị đánh giá mức độ nghiêm trọng của lỗi càng **cao** cho thấy rủi ro càng **ng nghiêm trọng**.^(*)

7.2.1 Định nghĩa về FMEA và thuật ngữ liên quan⁽⁷⁾

- **Khả năng xảy ra lỗi** (hay cơ hội xảy ra rủi ro tiềm ẩn) (“**Occurrence**” / “**Occ**”) là xếp hạng khả năng xảy ra rủi ro được đo lường bằng các giá trị định tính như thấp, trung bình hoặc cao. “Occurrence” (là “Likelihood” hay “Probability”) có giá trị định lượng đo lường từ 1 đến 5 (hoặc 1 – 6 / 1 – 10) nếu sử dụng thang đo điểm đánh giá từ 1 đến 5 (hoặc 1 – 6 / 1 – 10 tương ứng). Giá trị xếp hạng khả năng xảy ra lỗi càng **cao** (“high failure”) phản ánh khả năng xảy ra lỗi càng **cao**. (*)

7.2.1 Định nghĩa về FMEA và thuật ngữ liên quan⁽⁸⁾

- **Khả năng phát hiện lỗi** (hay khả năng phát hiện rủi ro) (“**Detectability**” / “**Det**”): đánh giá khả năng phát hiện (hay khám phá/nhận biết) ra vấn đề của các biện pháp kiểm soát (“control”) trong quy trình trước khi vấn đề xảy ra cho người dùng/khách hàng cuối. Khả năng phát hiện lỗi (“Det”) được đánh giá (hay xếp hạng) theo thang điểm từ 1 đến 5 (hoặc 1 – 6 / 1 – 10) nếu sử dụng thang đo điểm đánh giá từ 1 đến 5 (hoặc 1 – 6 / 1 – 10 tương ứng). Giá trị xếp hạng phát hiện càng **cao** phản ánh khả năng phát hiện lỗi càng **thấp**.^(*)

7.2.1 Định nghĩa về FMEA và thuật ngữ liên quan⁽⁹⁾

➤ Số Ưu tiên Rủi ro, hay RPN (Risk Priority Number) (*):

Là đánh giá bằng số về rủi ro được chỉ định cho một quy trình hoặc các bước trong quy trình, như một phần của phương pháp FMEA, trong đó một nhóm chỉ định từng giá trị số của phương thức lỗi ('Failure Mode') để định lượng khả năng xảy ra, khả năng phát hiện và mức độ nghiêm trọng của tác động/ảnh hưởng (Effect).

7.2.1 Định nghĩa về FMEA và thuật ngữ liên quan⁽¹⁰⁾

- Số Ưu tiên Rủi ro, hay RPN (Risk Priority Number):(*)
 - Số Ưu tiên Rủi ro được đánh giá bằng số về mức độ ưu tiên rủi ro của một dạng lỗi/nguyên nhân lỗi trong phân tích FMEA. RPN được tính bằng cách nhân các chỉ số Mức độ nghiêm trọng của lỗi (Sev), Khả năng xảy ra lỗi (Occ) và Khả năng phát hiện lỗi (Det).
 - Giá trị bằng số của Số Ưu tiên rủi ro (RPN) được thể hiện trong phần giao cắt trong một ma trận rủi ro khi trình bày theo dạng bảng (table) (xem từ slides 32).

7.2.1 Định nghĩa về FMEA và thuật ngữ liên quan⁽¹¹⁾

- Số Ưu tiên Rủi ro, hay RPN (Risk Priority Number) (*):

$$\text{RPN} = \text{Severity} \times \text{Occurrence} \times \text{Detection}$$

Số ưu tiên
rủi ro

Mức độ
nghiêm trọng

Khả năng
xảy ra

Khả năng
phát hiện

RPN dao động từ 1 (tốt nhất tuyệt đối) đến 125 (tệ nhất tuyệt đối) nếu cả 3 biến số đầu vào đều được xếp hạng theo thang điểm từ 1 đến 5

(*) 'Occurrence': 'Likelihood' or 'Probability'; 'Risk Severity': 'Risk Impact'

7.2.1 Định nghĩa về FMEA và thuật ngữ liên quan⁽¹²⁾

➤ Ngưỡng RPN (Threshold RPN)

- ❑ Số Ưu tiên rủi ro (RPN) còn được gọi là Ngưỡng RPN.
- ❑ Ngưỡng RPN là Số ưu tiên rủi ro (RPN) tối đa mà dưới đó rủi ro được coi là có thể chấp nhận được. Một bước quy trình bất kỳ nào trong quy trình có RPN trên ngưỡng này đều cần phải có kế hoạch hành động để giảm rủi ro.
- ❑ Ví dụ: với thang đo $10 \times 10 \times 10$ cho $Occ \times Sev \times Det$ thì giá trị RPN sẽ biến thiên từ 1 đến 1000. 5% của 1000 (giá trị RPN tối đa) là 50. Chủ doanh nghiệp có thể quy định bất kỳ RPN nào trên 50 (hoặc trên 300) được xác định là "RỦI RO CAO", cần phải xem xét, cập nhật kế hoạch hành động và (có thể) cải tiến hoặc nâng cấp biện pháp kiểm soát.

7.2.1 Định nghĩa về FMEA và thuật ngữ liên quan⁽¹³⁾

- Nếu doanh nghiệp được kiểm soát tốt với tương đối ít hạng mục RỦI RO CAO, thì giá trị 5% có thể được mở rộng lên, chẳng hạn như 15% để giải quyết các rủi ro thấp hơn.
- Nếu có quá nhiều mục RỦI RO CAO cần giải quyết cùng một lúc, chúng có thể được giải quyết theo trình tự từ trên xuống theo RPN.
- Danh sách rủi ro xếp thứ tự theo RPN giúp chủ doanh nghiệp doanh nghiệp cơ sở hợp lý để xác định lượng nguồn lực cần áp dụng để giảm thiểu rủi ro: điểm giới hạn sẽ nằm xa hơn trong danh sách nếu có nhiều nguồn lực hơn được phân bổ và ngược lại.

7.2.1 Định nghĩa về FMEA và thuật ngữ liên quan⁽¹⁴⁾

- Dù với thang đo nào cho Sev x Occ x Det (từ 1 – 5 / 1 – 6 / 1 – 10) thì RPN đưa ra trọng số ngang nhau cho Sev, Occ và Det. Vì lý do này, RPN có thể dẫn đến các số rủi ro tương tự cho các kết hợp rất khác nhau của Sev, Occ và Det nên nhiều chuyên gia sử dụng số AP thay cho RPN.

7.2.1 Định nghĩa về FMEA và thuật ngữ liên quan⁽¹⁵⁾

- Số AP hay số thể hiện Ưu tiên hành động (AP – Action Priority)
 - AP là phương pháp xếp hạng ưu tiên xử lý rủi ro dựa trên Mức độ nghiêm trọng khi kết hợp 3 giá trị Mức độ nghiêm trọng, Khả năng xảy ra và Khả năng phát hiện.
 - AP khác với Số Ưu tiên rủi ro (RPN) là giá trị đánh giá rủi ro dựa trên tích số (Mức độ nghiêm trọng x Khả năng xảy ra Sự xuất hiện và phát hiện) thì AP dựa vào mức độ nghiêm trọng khi xử lý rủi ro.

7.2.1 Định nghĩa về FMEA và thuật ngữ liên quan⁽¹⁶⁾

- AP nhấn mạnh hơn vào Mức độ nghiêm trọng ('Severity') trước tiên khi quyết định rủi ro nào phải xử lý trước.
- Ưu tiên hành động (AP – Action Priority) là cách tiếp cận biểu thị mức độ ưu tiên về việc thực hiện các hành động được đề xuất trong FMEA để **ưu tiên kiểm soát mức độ nghiêm trọng trước** kế tiếp là khả năng xảy ra và cuối cùng là khả năng phát hiện.
- AP không phải là việc ưu tiên rủi ro, mà là việc ưu tiên nhu cầu hành động để giảm thiểu rủi ro.

7.2.2 Sử dụng FMEA⁽¹⁾

- FMEA được sử dụng trước tiên trong quá trình thiết kế (hệ thống/thiết bị/quy trình/sản phẩm/dịch vụ/...) để ngăn ngừa lỗi. Sau đó, nó được sử dụng để kiểm soát trước và trong quá trình vận hành liên tục của quy trình.
- FMEA được sử dụng trong quá trình cải tiến liên tục (“Improvement”) thông qua việc ghi lại kiến thức và các hành động hiện tại về rủi ro của lỗi (thất bại/sai sót/hư hỏng...).

7.2.2 Sử dụng FMEA⁽²⁾

- FMEA còn được sử dụng trong các trường hợp sau:
 - Khi một quy trình, sản phẩm hoặc dịch vụ được thiết kế hoặc thiết kế lại hoặc được áp dụng theo cách mới; hoặc trước khi phát triển kế hoạch kiểm soát cho một quy trình mới hoặc quy trình sửa đổi.
 - Quản lý rủi ro trong các dự án cũng như trên toàn bộ hoạt động của các phòng ban và tổ chức.

7.2.2 Sử dụng FMEA⁽³⁾

- FMEA còn được sử dụng trong các trường hợp sau:
 - Khi các mục tiêu cải tiến được lên kế hoạch cho một quy trình, sản phẩm hoặc dịch vụ hiện có.
 - Khi phân tích lỗi của một quy trình, sản phẩm hoặc dịch vụ hiện có định kỳ trong suốt vòng đời của quy trình, sản phẩm hoặc dịch vụ.

7.2.3 Thủ tục thực hiện FMEA⁽¹⁾

Lưu ý: Đây là một thủ tục thực hiện chung. Các chi tiết cụ thể có thể khác nhau tùy theo tiêu chuẩn của doanh nghiệp hoặc ngành nghề hoặc đối tượng phân tích.

1. Chọn một Quy trình phải phân tích rủi ro thuộc phạm vi và kỳ đánh giá.
2. Tập hợp một nhóm đa chức năng gồm những người có kiến thức đa dạng về các quy trình, sản phẩm hoặc dịch vụ về ATTT cũng như các bên có liên quan với doanh nghiệp.
3. Sử dụng biểu mẫu BẢNG NHẬN DIỆN RỦI RO TIỀM ẨN, ĐÁNH GIÁ RỦI RO & HIỆU QUẢ CỦA CÁC BIỆN PHÁP KIỂM SOÁT có các nội dung phân tích tương tự theo FMEA.

7.2.3 Thủ tục thực hiện FMEA⁽²⁾

Biểu mẫu phân tích rủi ro theo FMEA áp dụng cho quy trình:

$$1. \text{RPN} = \text{Occ} \times \text{Sev}$$

[illegible]

7.2.3 Thủ tục thực hiện FMEA⁽³⁾

Biểu mẫu phân tích rủi ro theo FMEA áp dụng cho quy trình:

2. RPN = Occ x Sev x Det

[illegible]

7.2.3 Thủ tục thực hiện FMEA⁽⁴⁾

4. Sử dụng bảng **Tiêu chí rủi ro**^(*) đã ban hành tại doanh nghiệp bao gồm ba (3) yếu tố sau đây đã được xếp hạng từ thấp nhất đến cao nhất theo thang chia n bậc (n là 5 hoặc 6 hoặc 10... ví dụ thang chia từ 1 đến 5, từ 1 đến 6, từ 1 đến 10 v.v.):

4.1 Khả năng xảy ra “Occ” (“**Occurrence**”) rủi ro (*khả năng hay xác suất rủi ro có thể xảy ra với **tần suất** như thế nào? ‘**how likely is it?**’);*

7.2.3 Thủ tục thực hiện FMEA⁽⁵⁾

4.2 Mức độ nghiêm trọng (hay mức độ tác động) “Sev” (“**Severity**”) do rủi ro gây ra (*là tác động hay ảnh hưởng **ng nghiêm trọng** hay tệ hại như thế nào? “**How seriously is it?**” Or “**How badly is it?**”);*

4.3 Khả năng phát hiện “Det” (“**Detection**”) rủi ro xảy ra (*là khả năng phát hiện sớm như thế nào nếu rủi ro xảy ra? “**How soon can you detect it? Or How quickly can you detect it?**”*).

7.2.3 Thủ tục thực hiện FMEA⁽⁶⁾

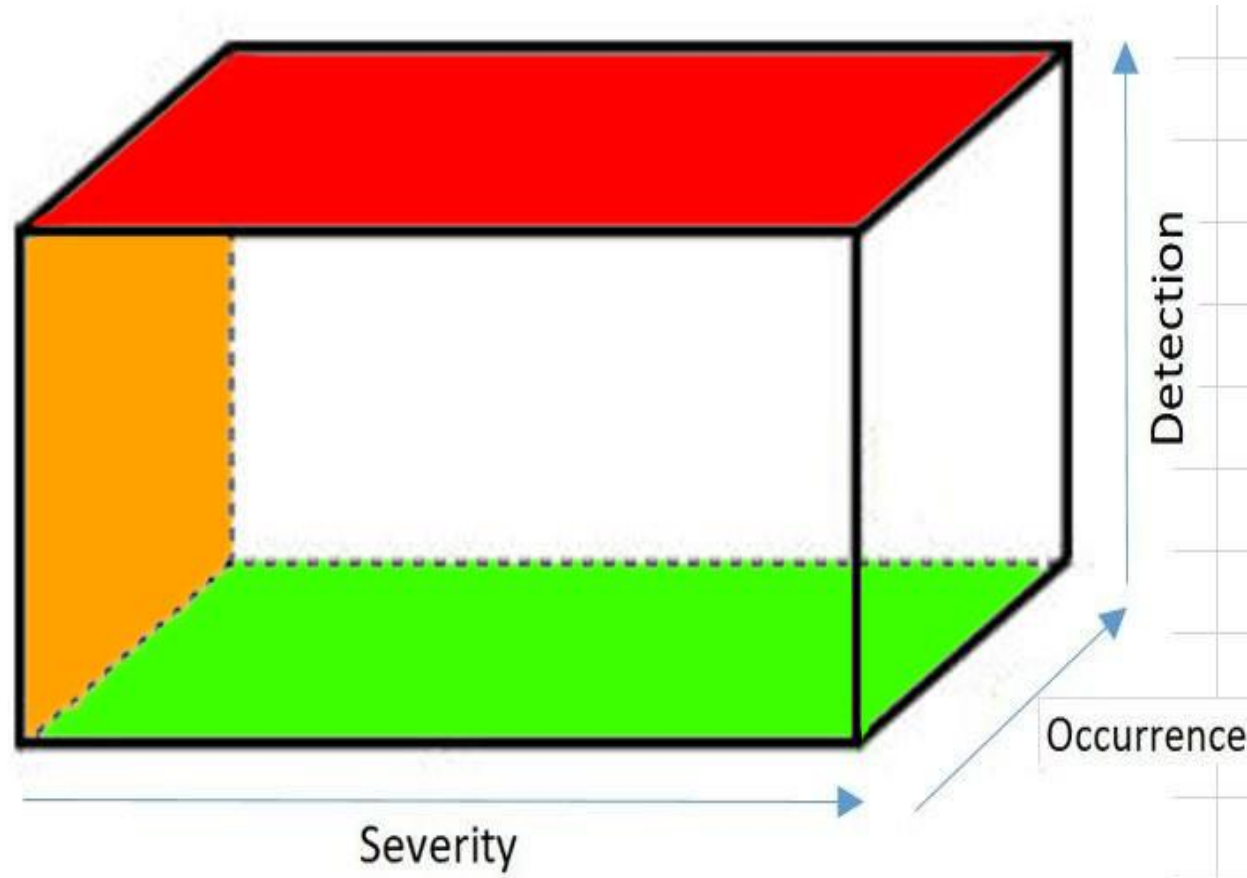
4.4 Số ưu tiên rủi ro (RPN)

Mỗi yếu tố trong số ba yếu tố Sev, Occ, Det được xếp hạng định lượng theo thang điểm từ 1 (Tốt nhất) đến 5 (Xấu nhất).

Tác động tổng hợp của ba yếu tố này là Số ưu tiên rủi ro (RPN). Đây là phép tính rủi ro của một dạng lỗi (thất bại) cụ thể và được xác định bằng phép tính sau: **$RPN = Sev \times Occ \times Det$**

7.2.3 Thủ tục thực hiện FMEA⁽⁶⁾

Số ưu tiên rủi ro (RPN): $RPN = Sev \times Occ \times Det$



7.2.3 Thủ tục thực hiện FMEA⁽⁷⁾

5 x 5 Risk Matrix						
		Risk Severity				
Risk Likelihood		Insignificant 1	Minor 2	Significant 3	Major 4	Severe 5
	5.Almost certain	Medium 5	High 10	Very High 15	Extreme 20	Extreme 25
	4.Likely	Medium 4	Medium 8	High 12	Very High 16	Extreme 20
	3.Moderate	Low 3	Medium 6	Medium 9	High 12	Very High 15
	2.Unlikely	Very Low 2	Low 4	Medium 6	Medium 8	High 10
	1.Rare	Very Low 1	Very Low 2	Low 3	Medium 4	Medium 5

7.2.3 Thủ tục thực hiện FMEA⁽⁷⁾

Tác động ('Impact')	5	Thảm họa ('Catastrophic')	Trung bình/Cao	Trung bình/Cao	Cao	Cao	Cao
	4	Lớn ('Major')	Thấp/Trung bình	Trung bình/Cao	Trung bình/Cao	Cao	Cao
	3	Vừa phải ('Moderate')	Thấp/Trung bình	Thấp/Trung bình	Trung bình/Cao	Trung bình/Cao	Cao
	2	Nhỏ / Yếu ('Minor')	Thấp	Thấp	Thấp/Trung bình	Thấp/Trung bình	Trung bình/Cao
	1	Không đáng kể ('Insignificant')	Thấp	Thấp	Thấp	Thấp/Trung bình	Thấp/Trung bình
			Hiếm ('Rare') < 3% cơ hội xảy ra	Không thể ('Unlikely') 3% -10% cơ hội xảy ra	Vừa phải ('Moderate') 10%-50% cơ hội xảy ra	Có thể ('Likely') 50% -90% cơ hội xảy ra	Chắc chắn ('Certain') >90% cơ hội xảy ra
			1	2	3	4	5
Khả năng xảy ra ('Likelihood')							

7.2.3 Thủ tục thực hiện FMEA⁽⁷⁾

6 x 6 Risk Matrix							
Risk Severity							
Risk Likelihood		Insignificant	Minor	Moderate	Severe	Major	Catastrophic
		1	2	3	4	5	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

7.2.3 Thủ tục thực hiện FMEA⁽⁸⁾

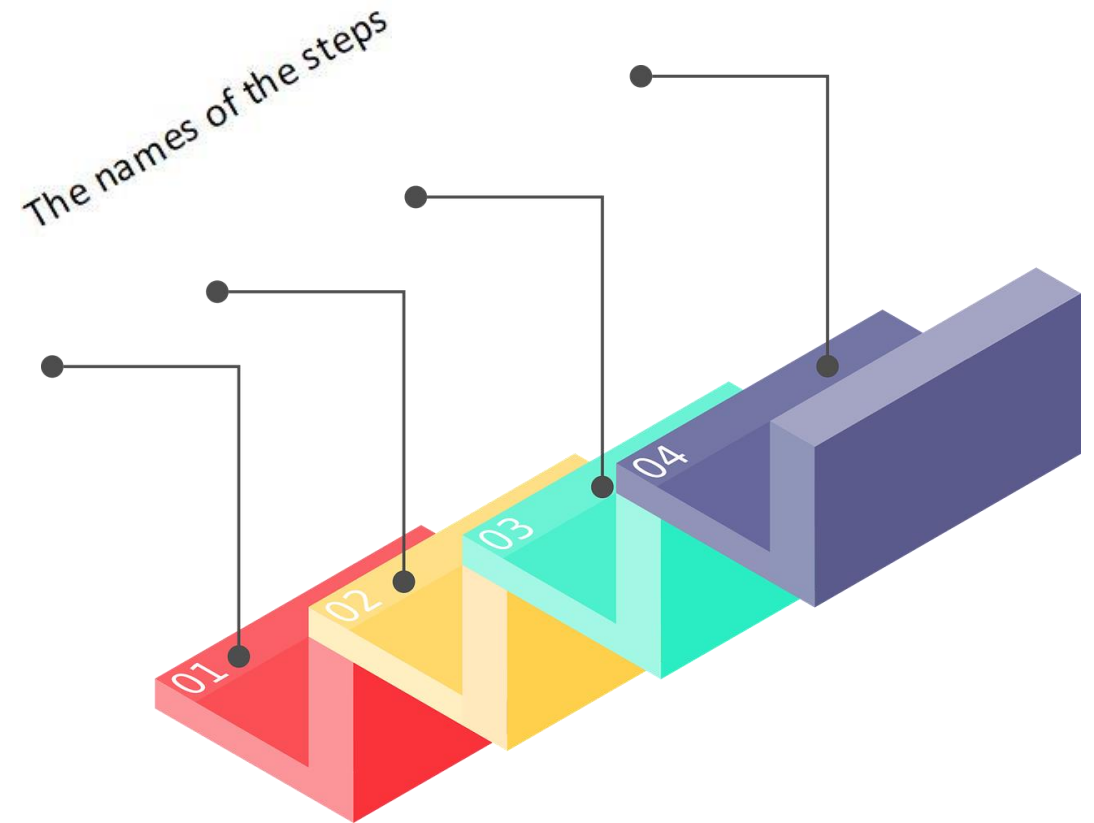
5. Xác định phạm vi của FMEA:

- Phạm vi dành cho khái niệm, hệ thống, quy trình, sản phẩm hay dịch vụ gì có liên quan đến ATTT?
- Ranh giới nhận diện rủi ro và chi tiết được nhận diện đến mức nào?
- Sử dụng lưu đồ/sơ đồ để xác định phạm vi và đảm bảo mọi thành viên trong nhóm hiểu nó một cách chi tiết.

7.2.3 Thủ tục thực hiện FMEA⁽⁹⁾

6. Thực hiện theo trình tự:

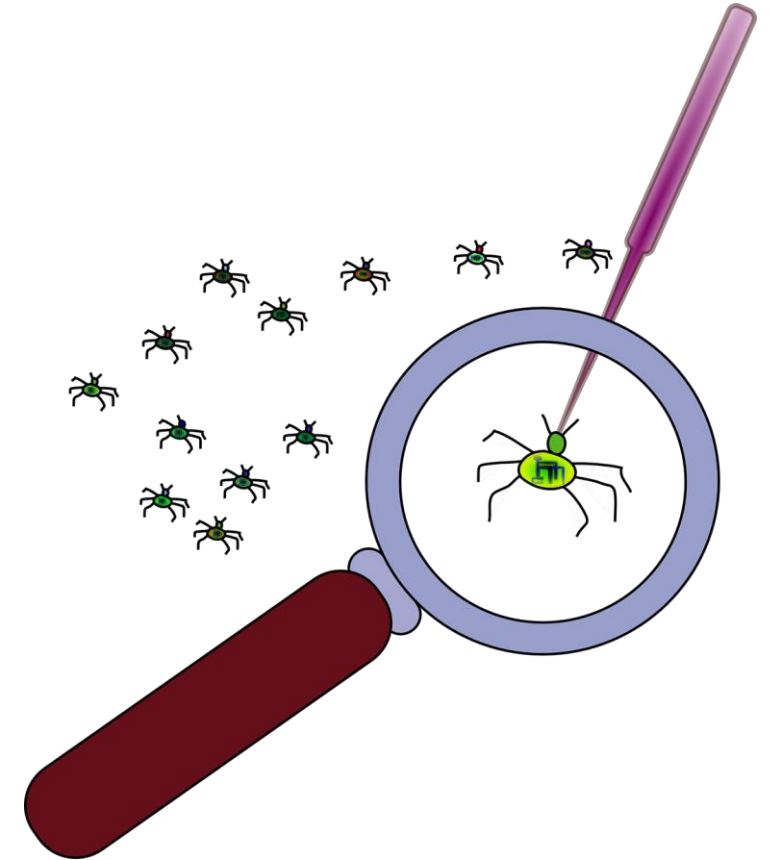
Bước 1: Nhập tên bước (hoặc tên hoạt động, tên chức năng, tên hệ thống con, tên hạng mục, tên bộ phận, hoặc tên các bước xử lý riêng biệt) của quy trình tại cột số (1) (hay cột F).



7.2.3 Thủ tục thực hiện FMEA⁽¹⁰⁾

6. Thực hiện theo trình tự:

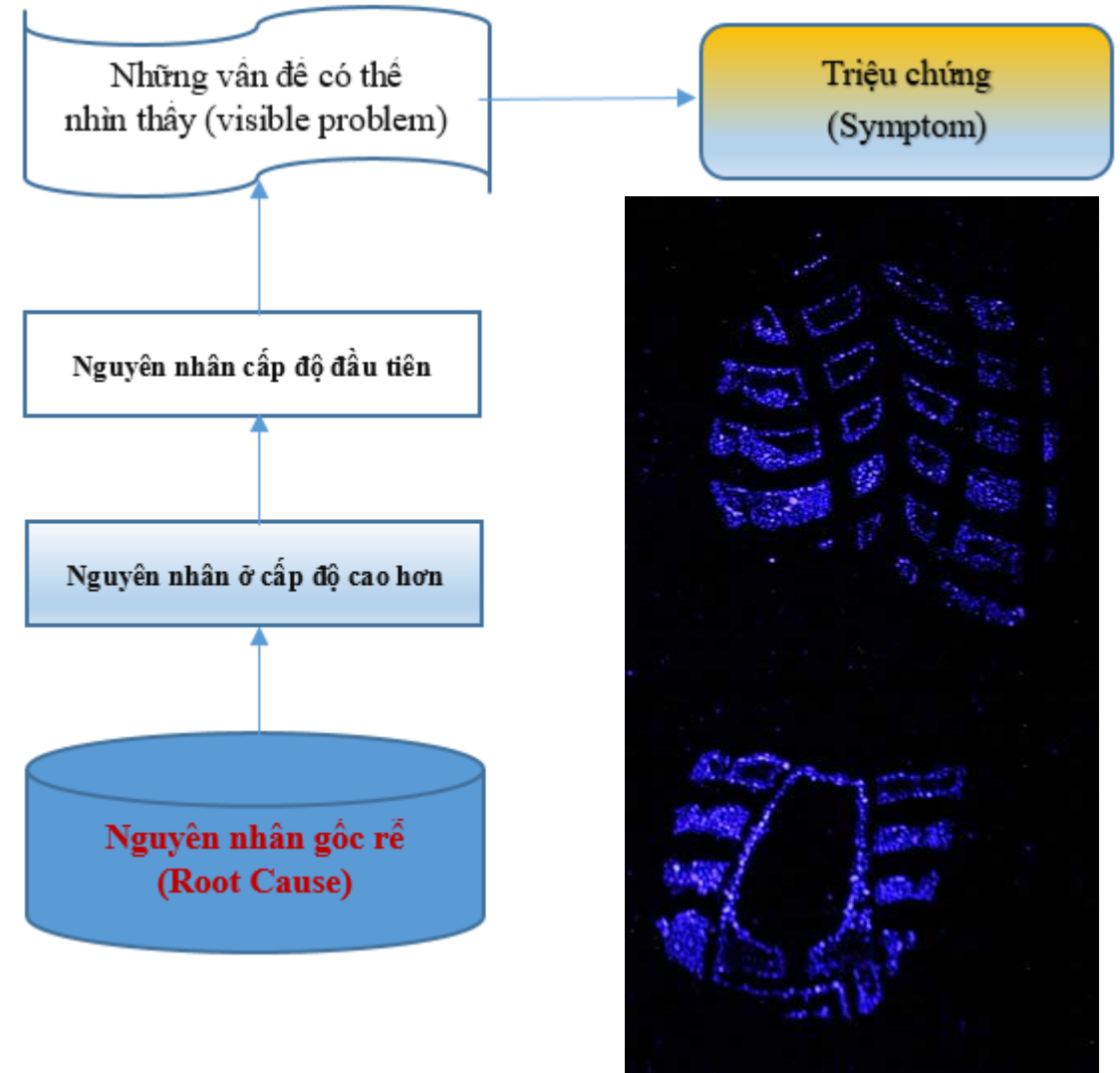
Bước 2: Tại cột số (2) (hay cột G), hãy ghi ra tất cả các phương thức lỗi là những rủi ro tiềm ẩn có thể xảy ra đối với hoạt động ở bước này. Nếu chưa xác định được, xem lại và viết lại các hoạt động thực hiện trong bước đó một cách chi tiết hơn để đảm bảo rằng khi rủi ro xảy ra thì hoạt động đó không thực hiện được.



7.2.3 Thủ tục thực hiện FMEA⁽¹¹⁾

6. Thực hiện theo trình tự: (tiếp)

Bước 3: Tại cột số (3) (hay cột H), tìm kiếm, phát hiện và liệt kê tất cả các nguyên nhân cho từng rủi ro tiềm ẩn trên biểu mẫu: 1 dòng là 1 nguyên nhân.



7.2.3 Thủ tục thực hiện FMEA⁽¹¹⁾

Bước 3: (tiếp)

Tại cột số (3) (hay cột H), tìm kiếm, phát hiện và liệt kê tất cả các nguyên nhân cho từng rủi ro tiềm ẩn...



7.2.3 Thủ tục thực hiện FMEA⁽¹²⁾

6. Thực hiện theo trình tự: (tiếp)

Bước 4: Tại cột số (4) (hay cột I), đối với mỗi nguyên nhân, xác định xếp hạng tương đối khả năng xảy ra (Occ) là ước tính xác suất xảy ra rủi ro vì nguyên nhân đó trong suốt thời gian tồn tại của phạm vi. Khả năng xảy ra nếu được đánh giá theo thang điểm từ 1 đến 5 (hay 1 - 5)^(*) thì 1 là cực kỳ khó xảy ra và 5 là không thể tránh khỏi.



7.2.3 Thủ tục thực hiện FMEA⁽¹²⁾

6. Thực hiện theo trình tự: (tiếp)

Thang điểm đánh giá 1 – 5 về khả năng xảy ra có ý nghĩa như sau:

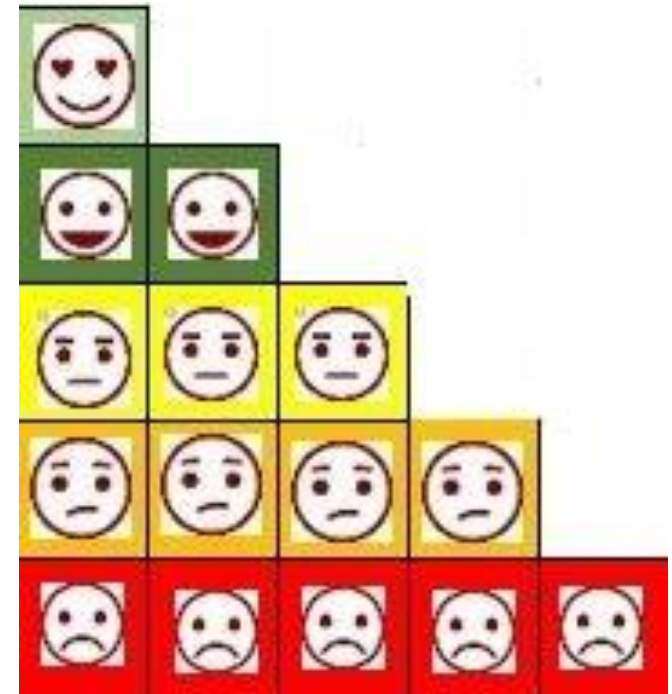
1 = Cực kỳ hiếm xảy ra, gần như không có khả năng xảy ra (**Unlikely**)

2 = Tương đối hiếm xảy ra nhưng có ít khả năng biểu hiện (**Seldom**)

3 = Điển hình hơn, khả năng xảy ra khoảng 50/50 (**Occasional**)

4 = Có khả năng xảy ra cao (**Likely**)

5 = Hầu như chắc chắn sẽ xảy ra (**Almost certain / High / Definite**)



7.2.3 Thủ tục thực hiện FMEA⁽¹³⁾

6. Thực hiện theo trình tự: (tiếp)

Bước 5: Tại cột số (5) (hay cột J), ghi ra tất cả các hậu quả có thể xảy ra (consequence/...) ứng với từng nguyên nhân.



7.2.3 Thủ tục thực hiện FMEA⁽¹⁴⁾

6. Thực hiện theo trình tự: *(tiếp)*

Bước 6: Tại cột số (6) (hay cột K), ghi ra mức độ nghiêm trọng (hay mức độ tác động) ứng với từng nguyên nhân. Đây là mức xếp hạng tương đối tính nghiêm trọng (hay Sev). Mức độ nghiêm trọng thường được đánh giá theo thang điểm từ 1 đến 5 (hay 1 - 5), trong đó 1 là không đáng kể và 5 là thảm khốc. Nếu một rủi ro có nhiều hơn một tác động, chỉ ghi vào bảng FMEA mức độ tác động cao nhất cho rủi ro đó.



7.2.3 Thủ tục thực hiện FMEA⁽¹⁴⁾

6. Thực hiện theo trình tự: (tiếp)



Thang điểm đánh giá 1 – 5 về mức độ nghiêm trọng có ý nghĩa như sau:

1 = Không đáng kể / Hiếm / Không thể xảy ra /Thấp (Insignificant / Rare / Improbable / Low)

2 = Nhỏ/Không chắc xảy ra/Khó xảy ra/Trung bình (Minor / Unlikely / Remote / Medium)

3 = Vừa phải/Thỉnh thoảng/Trung bình (Moderate / Occasional / Medium)

4 = Lớn / Có khả năng / Có thể / Cao (Major / Likely / Probable / High)

5 = Thảm họa / Gần như chắc chắn / Thường xuyên / Cao (Catastrophic / Almost certain / Frequent / High)

7.2.3 Thủ tục thực hiện FMEA⁽¹⁵⁾

6. Thực hiện theo trình tự: (tiếp)

Bước 6: Tại cột số (7) (hay cột L), ghi ra xếp hạng khả năng phát hiện (“Likelihood of Detection”) rủi ro (hay Det). Đây là mức xếp hạng tương đối khả năng phát hiện rủi ro (hay khám phá/nhận biết rủi ro). Khả năng phát hiện thường được xếp hạng theo thang điểm từ 1 đến 5 (hay 1 – 5 hoặc 1- 6 hoặc 1 - 10), trong đó 1 là hầu như chắc chắn phát hiện (khám phá/nhận biết) sớm được rủi ro và 5 là không thể phát hiện (khám phá/nhận biết) được.



7.2.3 Thủ tục thực hiện FMEA⁽¹⁵⁾

6. Thực hiện theo trình tự: (tiếp)

Phát hiện/Nhận biết (‘Detection’)	Khả năng phát hiện/nhận biết (‘Likelihood of Detection’)	Xếp hạng
‘Absolute Uncertainty’	Biện pháp kiểm soát <u>không thể phát hiện</u> chế độ lỗi và nguyên nhân tiềm ẩn	5
‘Low’	Khả năng biện pháp kiểm soát sẽ phát hiện chế độ lỗi và nguyên nhân là <u>thấp</u>	4
‘Moderate’	Khả năng biện pháp kiểm soát sẽ phát hiện chế độ lỗi và nguyên nhân là <u>trung bình</u>	3
‘High’	Khả năng biện pháp kiểm soát sẽ phát hiện chế độ lỗi và nguyên nhân là <u>cao</u>	2
‘Almost Certain’	Biện pháp kiểm soát <u>chắc chắn sẽ phát hiện</u> chế độ lỗi và nguyên nhân tiềm ẩn	1

7.2.3 Thủ tục thực hiện FMEA⁽¹⁶⁾

6. Thực hiện theo trình tự: *(tiếp)*

Bước 7: Tại cột số (8), tính và ghi ra số ưu tiên rủi ro, hay RPN, bằng cách nhân giá trị tại các cột số (4), (6) và (7) với nhau ($\text{Occ} \times \text{Sev} \times \text{Det}$). Số RPN này có thể dùng để xếp hạng các rủi ro tiềm ẩn (hay lỗi/thất bại/...) theo thứ tự.

$$\text{RPN} = \text{Sev} \times \text{Occ} \times \text{Det}$$

7.2.3 Thủ tục thực hiện FMEA⁽¹⁶⁾

6. Thực hiện theo trình tự: (tiếp)

$$\text{RPN} = \text{Severity} \times \text{Occurrence} \times \text{Detection}$$

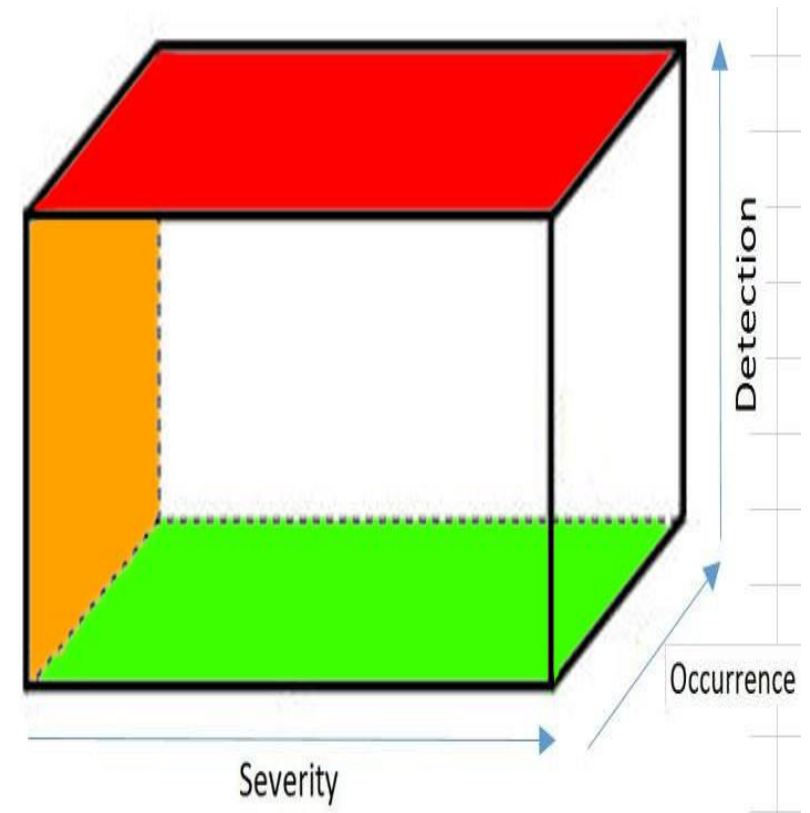
Số ưu tiên
rủi ro

Mức độ
tác động

Khả năng
xảy ra

Khả năng
phát hiện

RPN dao động từ 1 (tốt nhất tuyệt đối) đến 125 (tệ nhất tuyệt đối) nếu cả 3 biến số đầu vào đều được xếp hạng theo thang điểm từ 1 đến 5



7.2.3 Thủ tục thực hiện FMEA⁽¹⁷⁾

6. Thực hiện theo trình tự: (tiếp)

Bước 8: Tại cột số (9), với mỗi nguyên nhân, xác định các biện pháp kiểm soát quy trình hiện tại (hiện hữu). Đây là những biện pháp hay cơ chế hiện có để ngăn chặn rủi ro hoặc giảm rủi ro xảy ra.



7.2.3 Thủ tục thực hiện FMEA⁽¹⁸⁾

6. Thực hiện theo trình tự (tiếp)

Bước 9: Tại cột số (10), chỉ định người chịu trách nhiệm thực hiện hành động đề nghị và ấn định ngày hoàn thành.

() Trường hợp rủi ro tiềm ẩn có RPN/Criticality xếp hạng **cao** hoặc có chỉ định của cấp trên, một kế hoạch hành động chi tiết (theo cấu trúc 5W1H) phải được soạn thảo (hoặc soạn theo biểu mẫu tại slide số 67 (7.5)) có nêu ra chiến lược QLRR nào được chọn cùng với mục đích và mục tiêu phải đạt được trong khoảng thời gian giới hạn.*

7.2.3 Thủ tục thực hiện FMEA⁽¹⁹⁾

6. Thực hiện theo trình tự (tiếp)

Bước 10: Sau khi hoàn thành ở Bước 9, nhóm ghi nhận lại kết quả: xếp hạng lại khả năng xảy ra (Occ) ở cột (11), xếp hạng lại mức độ nghiêm trọng (Sev) ở cột (12), xếp hạng lại khả năng phát hiện (Det) ở cột (13) và tính lại giá trị RPN' mới.

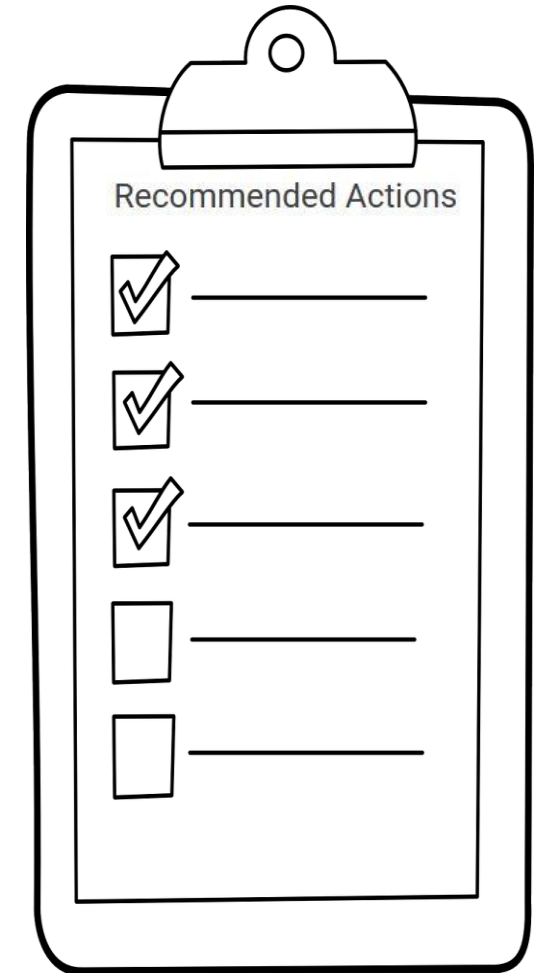


7.2.3 Thủ tục thực hiện FMEA⁽²⁰⁾

6. Thực hiện theo trình tự (tiếp)

Bước 11: Ghi ‘Có’ để duy trì biện pháp kiểm soát hiện hữu tại cột số (15) hoặc ghi ‘Không’ để có các hành động được đề nghị ‘Có’ tại cột số (16).

Những hành động này có thể là thay đổi trong quy trình để giảm giá trị RPN hoặc là tăng các biện pháp kiểm soát (“control”) bổ sung để cải thiện khả năng phát hiện rủi ro, giảm khả năng xảy ra rủi ro và/hoặc giảm mức độ nghiêm trọng do rủi ro gây ra.



Recommended Actions

<input checked="" type="checkbox"/>	_____
<input checked="" type="checkbox"/>	_____
<input checked="" type="checkbox"/>	_____
<input type="checkbox"/>	_____
<input type="checkbox"/>	_____

7.3

Các định nghĩa về FMECA

7.3.1 Định nghĩa về FMECA

7.3.2 Sử dụng FMECA

7.3.3 Thủ tục thực hiện FMECA

7.3.1 Định nghĩa về FMECA⁽¹⁾

- FMECA là từ viết tắt của “Failure Mode, Effects and Criticality Analysis” (Phân tích mức độ nghiêm trọng, tác động và phương thức lỗi).
- FMECA là một công cụ phân tích quy trình, phân tích mức độ nghiêm trọng, tác động và phương thức lỗi (FMECA) tương tự FMEA; là phương pháp tiếp cận từng bước để xác định tất cả các rủi ro tiềm ẩn do lỗi có thể xảy ra trong thiết kế, quy trình sản xuất hoặc lắp ráp hoặc sản phẩm hoặc dịch vụ.

7.3.1 Định nghĩa về FMECA⁽²⁾

- FMECA khác với FMEA như sau:
 - Các phương thức lỗi được phân tích khả năng xảy ra, mức độ tác động, khả năng phát hiện giống như với FMEA, nhưng FMECA đi sâu vào chi tiết hơn (như về mức độ nghiêm trọng) để cung cấp kết quả chính xác hơn, cùng với việc xếp hạng các lỗi đó với mức độ nghiêm trọng (tới hạn) (Criticality) cao nhất.

7.3.1 Định nghĩa về FMECA⁽³⁾

- FMECA khác với FMEA như sau: *(tiếp)*
 - FMEA thiếu xếp hạng mức độ nghiêm trọng (tới hạn): Criticality
 - FMEA cung cấp thông tin định tính thì FMECA cung cấp cả thông tin định tính và định lượng, cho phép người dùng đo lường mức độ nghiêm trọng (tới hạn) (Criticality) đối với các phương thức lỗi và sắp xếp chúng theo mức độ quan trọng.

7.3.1 Định nghĩa về FMECA⁽⁴⁾

- FMECA khác với FMEA như sau: *(tiếp)*
 - FMECA thường được tiến hành theo cách tiếp cận từ trên xuống (Top-Down) (như phân tích rủi ro ở giai đoạn thiết kế ban đầu) hoặc từ dưới lên (Bottom-Up) (như phân tích rủi ro từng thành phần từ cấp độ thấp nhất trở lên).

7.3.2 Sử dụng FMECA

- FMECA yêu cầu áp dụng FMEA trước khi bổ sung hành động phân tích mức độ nghiêm trọng (tới hạn).
- Hiện nay, các mẫu dành cho FMEA được phát triển, bổ sung và cải tiến nên FMECA trở nên ít cần thiết hơn.

7.3.3 Thủ tục thực hiện FMECA⁽¹⁾

Biểu mẫu FMECA dùng cho phân tích lỗi Quy trình

TT	Các bước thực hiện quy trình	Rủi ro tiềm ẩn	Nguyên nhân của rủi ro	Khả năng xảy ra	Hậu quả có thể gây ra	Mức độ ảnh hưởng	Biện pháp kiểm soát hiện hữu	Khả năng phát hiện	RPN ₁ = 5x7x9	Mức độ nghiêm trọng (CRIT) = 5x7	Hành động đề nghị	Trách nhiệm và ngày hoàn thành	Kết quả Hành động				
													Khả năng xảy ra	Mức độ ảnh hưởng	Khả năng phát hiện	RPN ₂ = 14x15x16	Mức độ nghiêm trọng (CRIT) = 14x15
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18

(*) RPN₁ : (là số ưu tiên rủi ro) khi biện pháp kiểm soát hiện hữu; RPN₂: (là số ưu tiên rủi ro) khi có biện pháp kiểm soát mới theo đề nghị

(*)CRIT (Criticality) mức độ nghiêm trọng = Khả năng xảy ra (O) x Mức độ ảnh hưởng (S)



7.3.3 Thủ tục thực hiện FMECA(2)

Biểu mẫu FMECA dùng cho phân tích lỗi sản phẩm/dịch vụ/tài sản/...

Company Name (Tên Công ty _____)

Department: XYZ Department (Phòng XYZ)

RISK ANALYSIS AND ASSESSMENT TABLE (FMEA/FMECA)

No.	Business / Service	Asset Name	Asset Number	Function	Potential Failure Mode(s)	Potential Technical Effect(s) of Failure	Potential Business Consequence(s) of Failure	Severity	Potential Cause(s)/ Mechanism(s) of Failure	Occurrence	Criticality	Current Controls (Các biện pháp kiểm soát hiện đang áp dụng)		Detectability	RPN	Recommended Controls (Các biện pháp kiểm soát được khuyến nghị phải áp dụng)		Responsibility & Target Completion Date	Action Results						
												Preventive Controls	Detective Controls			Implemented Controls (Các biện pháp kiểm soát đã triển khai)			New Severity	New Occurrence	New Detectability	New Criticality	New RPN		
																Preventive Controls	Detective Controls								
(Số thứ tự)	(Hoạt động kinh doanh/Dịch vụ)	(Tên tài sản)	(Mã số tài sản)	(Chức năng)	(Rủi ro tiềm ẩn (các dạng lỗi tiềm ẩn))	(Tác động tiềm ẩn về mặt kỹ thuật do lỗi gây ra)	(Hậu quả tiềm ẩn về mặt kinh doanh do lỗi gây ra)	Severity	(Nguyên nhân tiềm ẩn/Cơ chế gây ra lỗi)	Occurrence	Criticality	(Các biện pháp kiểm soát ngăn ngừa lỗi)	(Các biện pháp kiểm soát phát hiện lỗi)	Detectability	RPN	(Các biện pháp kiểm soát ngăn ngừa lỗi)	(Các biện pháp kiểm soát phát hiện lỗi)	(Trách nhiệm thực hiện và ngày hoàn thành mục tiêu)	(Các biện pháp kiểm soát ngăn ngừa lỗi)	(Các biện pháp kiểm soát phát hiện lỗi)	Severity mở i	Occurrence mở i	Detectability mở i	Criticality mở i	RPN mở i
8	Protecting IT Assets	Firewall	5000	To block unauthorized requests	Rules not appropriately configured	IP Spoofing	Diversion of sensitive data traffic, fraud	8	Procedures not followed	2	16	Procedures available		4	64		Increase audit frequency	XYZ by end Jan 2006		Increase audit frequency	5	3	2	15	30
4	Protecting IT Assets	Firewall	5000	To block unauthorized requests	Rules not appropriately configured	Entry for External Hackers	Disclosure or modification of business records; prosecution; bad PR; customer defection	7	Procedures not followed	2	14		Log Monitoring	4	56		Increase audit frequency	XYZ by end Jan 2006		Increase audit frequency	5	3	2	15	30

7.3.3 Thủ tục thực hiện FMECA⁽³⁾

$$\text{CRITICALITY} = \text{Severity} \times \text{Occurrence}$$

MỨC ĐỘ NGHIÊM
TRỌNG

Mức độ
nghiêm trọng

Khả năng
xảy ra

CRITICALITY dao động từ 1 (tốt nhất tuyệt đối) đến 25 (tệ nhất tuyệt đối) nếu cả 2 biến số đầu vào đều được xếp hạng theo thang điểm từ 1 đến 5

7.4

Triển khai phương pháp FMEA và FMECA

7.4.1 Triển khai phương pháp FMEA

7.4.2 Triển khai phương pháp FMECA

7.4 Triển khai phương pháp FMEA và FMECA⁽¹⁾

7.4.1 Triển khai phương pháp FMEA

- Mỗi nhóm tự đề xuất một quy trình (hoặc thủ tục) trong hoạt động CNTT để thực hành triển khai phương pháp FMEA.
- Yêu cầu của bài thực hành là:
 - Vẽ lưu đồ quy trình bằng MS Visio / MS Word;
 - Mô tả từng bước (1, 2, 3,...) cách thực hiện hành động gì trong quy trình theo 5W1H (Who-What-Why-Where-When-How);
 - Lập bảng nhận diện rủi ro tiềm ẩn, đánh giá rủi ro và hiệu quả các biện pháp kiểm soát theo biểu mẫu FMEA;
 - Thời gian hoàn thành bài thực hành: không quá 10 ngày trong tuần kể từ __/__/_____.

7.4 Triển khai phương pháp FMEA và FMECA⁽²⁾

- Gợi ý tên một số quy trình có thể đưa vào thực hành FMEA:
 - Quy trình bảo trì máy tính cá nhân (PC) tại doanh nghiệp
 - Quy trình khắc phục sự cố mạng LAN / WAN tại doanh nghiệp
 - Quy trình cấp / thu hồi quyền truy cập vật lý/ứng dụng cho người dùng thiết bị CNTT (Users) tại doanh nghiệp
 - Quy trình tiếp nhận/bàn giao tài sản CNTT (phần cứng/phần mềm) tại doanh nghiệp
 - Quy trình mua sắm tài sản CNTT tại doanh nghiệp
 - Quy trình quản lý dự án phát triển phần mềm tại doanh nghiệp
 - v.v.

7.4 Triển khai phương pháp FMEA và FMECA⁽³⁾

7.4.2 Triển khai phương pháp FMECA

- Nội dung thực hành triển khai phương pháp FMECA tương tự như nội dung thực hành tại 7.4.1 cho FMEA nhưng có bổ sung tính giá trị Mức độ nghiêm trọng (tới hạn) (CRITICALITY) trong biểu mẫu FMEA.

7.5

Kế hoạch hành động (Action Plan)

7.5 Kế hoạch hành động⁽¹⁾

Biểu mẫu Kế hoạch hành động

KẾ HOẠCH HÀNH ĐỘNG

(Thời điểm/...../.....)

1. ĐƠN VỊ THỰC HIỆN:

2. QUY TRÌNH:

(Sản Phẩm/Dịch Vụ/Hệ thống)

3. NGÀY THỰC HIỆN:

STT	Rủi ro đề xuất kế hoạch hành động	Bước quy trình liên quan đến rủi ro	Phương án xử lý rủi ro đề xuất	Dự kiến nguồn lực, chi phí để thực hiện	Đơn vị/ cá nhân thực hiện		Lịch trình triển khai	Thời hạn hoàn thành
					Chính	Phối hợp hỗ trợ		

7.5 Kế hoạch hành động⁽²⁾

- Kế hoạch hành động được yêu cầu xây dựng sau khi:
 - Hoàn thành phân tích rủi ro theo FMEA/FMECA và được nhóm phụ trách QLRR từ các đơn vị khác nhau nghiệm thu;
 - Xếp hạng rủi ro tiềm ẩn theo Số ưu tiên rủi ro hoặc mức độ nghiêm trọng tới hạn (RPN/Criticality) từ cao đến thấp;
 - Quyết định chỉ lập kế hoạch hành động cho các rủi ro tiềm ẩn có RPN/Criticality xếp hạng CAO hoặc có chỉ định;
 - Lập kế hoạch hành động theo biểu mẫu đã phê duyệt.

Hết Chương 7

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://www.bvda.com/en/luminol>