**MỤC LỤC**

[Phần lý thuyết: From AT16H with love <3 3](#_Toc131598303)

[Câu 1. Quản lý rủi ro là gì? Tầm quan trọng của Quản lý rủi ro. 3](#_Toc131598304)

[Câu 2. Hãy trình bày quy trình Quản lý rủi ro. 3](#_Toc131598305)

[Câu 3. Hãy trình bày về giai đoạn Thiết lập bối cảnh. 4](#_Toc131598306)

[Câu 4. Hãy trình bày về giai đoạn Nhận diện rủi ro. 5](#_Toc131598307)

[Câu 5. Hãy trình bày về giai đoạn Phân tích rủi ro. 8](#_Toc131598308)

[Câu 6. Hãy trình bày về giai đoạn Xử lý rủi ro. 8](#_Toc131598309)

[Câu 7. Trình bày các thành phần chính của kế hoạch dự phòng. 9](#_Toc131598310)

[Câu 8. Trình bày quy trình kế hoạch dự phòng gồm bảy bước do NIST đề xuất. 11](#_Toc131598311)

[Câu 9. Trình bày quy trình ứng phó sự cố. 11](#_Toc131598312)

[Câu 10. Liệt kê và mô tả các tiêu chí được sử dụng để xác định xem một sự cố thực sự có đang xảy ra hay không. 13](#_Toc131598313)

[Câu 11. Chính sách an toàn thông tin là gì? Tại sao nó lại quan trọng đối với sự thành công của chương trình An toàn thông tin? 14](#_Toc131598314)

[Câu 12. Liệt kê và mô tả ba thách thức trong việc định hình chính sách. 15](#_Toc131598315)

[Câu 13. Phân biệt: Chính sách, tiêu chuẩn, thủ tục 15](#_Toc131598316)

[Câu 14. Trình bày về quy trình xây dựng CS theo cách tiếp cận quản lý dự án 16](#_Toc131598317)

[Câu 15. Hãy trình bày tóm tắt về các thành phần của Quản lý An toàn thông tin. 17](#_Toc131598318)

[Câu 16. Vai trò của Luật pháp và Đạo đức trong Quản lý An toàn thông tin. 19](#_Toc131598319)

[Phần bài tập: From AT16H with love <3 20](#_Toc131598320)

[Câu 1. Xây dựng chính sách an toàn thông tin cho một hệ thống cụ thể (một hệ thống nhỏ hoặc một phần trong hệ thống, cần phải tuân thủ khuôn mẫu của chính sách an toàn thông tin). 20](#_Toc131598321)

[Câu 2. Ước lượng rủi ro cho một hệ thống. 21](#_Toc131598322)

# Phần lý thuyết: From AT16H with love <3

Bố cục đề thi: 02 câu lý thuyết mỗi câu 02 điểm, 02 câu bài tập mỗi câu 03 điểm

## Quản lý rủi ro là gì? Tầm quan trọng của Quản lý rủi ro.

Quản lí rủi ro là quá trình tiếp cận rủi ro một cách khoa học và có hệ thống nhằm nhận diện, kiểm soát, phòng ngừa và giảm thiểu những tổn thất, mất mát, những ảnh hưởng bất lợi của rủi ro. Bao gồm: đánh giá, xử lý và chấp nhận rủi ro.

Tầm quan trọng của quản lý rủi ro:

- Rủi ro mà một tổ chức gặp phải xuất hiện ở bất cứ đâu, bất cứ phần nào trong hệ thống thông tin, từ việc nhỏ như vô tình lộ mật khẩu tài khoản công ty hay vô tình xoá mất dữ liệu.

- Để hạn chế tối đa các tác động của rủi ro cần có một phương pháp quản lý rủi ro trong HTTT một cách hiệu quả.

- Người đứng đầu đơn vị tổ chức phải đảm bảo rằng tổ chức có mức hỗ trợ mong muốn khi đối mặt với các mối đe dọa trong thực tế.

## Hãy trình bày quy trình Quản lý rủi ro.

Quy trình quản lý rủi ro là một quá trình theo bước định hướng giúp tổ chức nhận biết, đánh giá, xử lý, chấp nhận, truyền thông và giám sát các rủi ro tiềm ẩn và có thể xảy ra trong quá trình hoạt động của tổ chức. Quy trình này bao gồm sáu bước chính như sau:

1. Thiết lập bối cảnh: Bước đầu tiên trong quy trình quản lý rủi ro là thiết lập bối cảnh. Điều này bao gồm việc xác định các yếu tố nội bộ và bên ngoài ảnh hưởng đến tổ chức, bao gồm mục tiêu, chiến lược, quy định pháp lý, văn hóa tổ chức, đối thủ cạnh tranh, thị trường và môi trường tổng thể. Việc thiết lập bối cảnh giúp tổ chức hiểu rõ hơn về những nguy cơ tiềm tàng có thể xảy ra trong quá trình hoạt động của mình.

2. Đánh giá rủi ro: Bước tiếp theo trong quy trình quản lý rủi ro là đánh giá rủi ro. Quá trình này bao gồm việc xác định và đánh giá các nguy cơ tiềm tàng và khả năng xảy ra của chúng, cũng như tác động của chúng đối với hoạt động của tổ chức. Đánh giá rủi ro giúp tổ chức đưa ra các quyết định về việc xử lý rủi ro và phân bổ tài nguyên phù hợp.

3. Xử lý rủi ro: Sau khi đánh giá rủi ro, tổ chức cần xác định các biện pháp để xử lý rủi ro. Điều này bao gồm việc đưa ra các giải pháp để giảm thiểu nguy cơ, chuyển giao rủi ro, chấp nhận rủi ro hoặc tránh rủi ro hoàn toàn. Việc xử lý rủi ro là một quá trình liên tục và cần được đánh giá thường xuyên để đảm bảo tính hiệu quả.

4. Chấp nhận rủi ro: Một số rủi ro không thể được giảm thiểu hoặc loại trừ hoàn toàn và cần được chấp nhận. Trong bước này, tổ chức cần đánh giá các tùy chọn và quyết định về việc chấp nhận rủi ro đó. Việc chấp nhận rủi ro có thể bao gồm việc thực hiện các biện pháp để giảm thiểu tác động của rủi ro hoặc đưa ra kế hoạch để phục hồi hoạt động của tổ chức khi xảy ra rủi ro.

5. Truyền thông và tư vấn rủi ro ATTT: Trong quá trình quản lý rủi ro, việc truyền thông và tư vấn rủi ro là rất quan trọng. Tổ chức cần thông báo về các rủi ro tiềm tàng và các biện pháp xử lý rủi ro đang được thực hiện để đảm bảo các bên liên quan hiểu rõ về tình hình rủi ro. Tư vấn rủi ro cũng là một phần quan trọng trong quá trình quản lý rủi ro, giúp tổ chức xác định các rủi ro tiềm ẩn và cung cấp các giải pháp để giảm thiểu tác động của chúng.

6. Giám sát và soát xét rủi ro ATTT: Cuối cùng, trong quá trình quản lý rủi ro, việc giám sát và soát xét rủi ro là cần thiết. Tổ chức cần theo dõi các biện pháp xử lý rủi ro đang được thực hiện để đảm bảo tính hiệu quả và đưa ra các điều chỉnh khi cần thiết. Việc soát xét rủi ro cũng giúp tổ chức đánh giá lại quy trình quản lý rủi ro hiện tại và đưa ra các cải tiến để nâng cao khả năng đối phó với các rủi ro tiềm ẩn trong tương lai.

## Hãy trình bày về giai đoạn Thiết lập bối cảnh.

Trình bày giai đoạn Thiết lập bối cảnh:

Thông tin tổng quan về hệ thống thông tin

• Thông tin Chủ quản hệ thống thông tin

• Thông tin Đơn vị vận hành

• Chức năng, nhiệm vụ, cơ cấu tổ chức của đơn vị vận hành

• Các cơ quan, tổ chức liên quan

• Phạm vi, quy mô của hệ thống.

Tiêu chí chấp nhận rủi ro

• Phụ thuộc vào các chính sách, mục đích, mục tiêu bảo đảm ATTT của tổ chức và các lợi ích của các bên liên quan.

• Cần phải xác định mức chấp nhận rủi ro của riêng tổ chức. Việc xác định các tiêu chí chấp nhận rủi ro cần xem xét đến các yếu tố như: Nguồn lực để xử lý rủi ro so với hiệu quả mang lại sau khi rủi ro được xử lý; Khả năng xử lý rủi ro theo điều kiện thực tế của cơ quan, tổ chức.v.v.

• Tiêu chí chấp nhận rủi ro có thể bao gồm nhiều ngưỡng với các tiêu chí tương ứng, căn cứ theo mục tiêu bảo đảm ATTT mà tổ chức đưa ra.

• Khuyến nghị về một số tiêu chí chấp nhận rủi ro như sau:

- HTTT cấp độ 5 không chấp nhận tồn tại rủi ro.

- HTTT cấp độ 3 hoặc cấp độ 4, chỉ chấp nhận tồn tại các rủi ro ở mức thấp.

- HTTT cấp độ 1 hoặc cấp độ 2, không chấp nhận tồn tại các rủi ro mức trung bình.

Phạm vi và giới hạn

• Phạm vi quản lý an toàn thông tin

- Các mục tiêu bảo đảm an toàn thông tin của cơ quan, tổ chức

- Các quy định pháp lý phải tuân thủ

- Quy chế, chính sách bảo đảm an toàn thông tin của tổ chức.

• Phạm vi kỹ thuật

- Sơ đồ tổng thể (vật lý, logic) và các thành phần trong hệ thống (thiết bị mạng, bảo mật, máy chủ, thiết bị đầu cuối...).

- Xác định các HTTT khác có liên quan hoặc có kết nối đến hoặc có ảnh hưởng quan trọng tới hoạt động bình thường của HTTT được đề xuất; trong đó, xác định rõ mức độ ảnh hưởng đến HTTT đang được đề xuất cấp độ khi các hệ thống này bị mất ATTT;

- Danh mục các nguy cơ tấn công mạng, mất ATTT đối với hệ thống và các ảnh hưởng.

Tổ chức thực hiện đánh giá và quản lý rủi ro

• Phương án, kế hoạch thực hiện đánh giá và quản lý rủi ro.

• Quy trình tổ chức thực hiện đánh giá và quản lý rủi ro.

• Cơ chế phối hợp với các bên liên quan trong quá trình thực hiện.

• Phương án, kế hoạch giám sát quy trình đánh giá và quản lý rủi ro

## Hãy trình bày về giai đoạn Nhận diện rủi ro.

Trình bày giai đoạn Nhận diện rủi ro:

Là quá trình tìm kiếm, thừa nhận và ghi lại các rủi ro.

Bao gồm:

* Nhận biết về tài sản: để xác định danh mục các tài sản của tổ chức cần bảo vệ bao gồm TT, HTTT.
* Nhận biết về mối đe dọa: để xác định các mối đe dọa đối với mỗi tài sản.
* Nhận biết về điểm yếu: để xác định các điểm yếu có thể tồn tại đối với mỗi tài sản.
* Kết quả: danh mục các mối đe dọa và điểm yếu đối với các tài sản được xác định.

Phương pháp nhận diện rủi ro

1. Thiết lập bảng kê

2. Phân tích tài chính

3. Phương pháp lưu đồ

4. Phân tích công nghệ

5. Kiểm tra hiện trường

6. Tham khảo các chuyên gia khác trong tổ chức

7. Phương pháp thông qua tư vấn

8. Phương pháp phân tích hợp đồng

9. Nghiên cứu các số liệu tổn thất trong quá khứ

10. Nhận diện những mối nguy tiềm năng.

Nhận biết tài sản

Cần xác định và thu thập TT đầy đủ về tài sản đang được quản lý, đặc biệt là các TT liên quan đến đặc điểm, nơi lưu trữ, mức độ quan trọng và giá trị, đặc thù của tài sản. Các kỹ thuật thu thập thông tin về hệ thống:

* Bảng câu hỏi
* Phỏng vấn tại chỗ
* Xem xét tài liệu
* Sử dụng Công cụ quét tự động.

Nhận dạng mối đe dọa

Mối đe dọa có thể được xác định dựa vào các điểm yếu của TT, HTTT => xác định các mối đe dọa có thể dựa vào việc phân nhóm các điểm yếu

Thiết lập bảng đánh giá với một số câu hỏi cơ bản như:

* Mối đe dọa nào nguy hiểm với tài sản của tổ chức trong môi trường hoạt động đã biết?
* Mối đe dọa nào gây nguy hiểm nhất đối với thông tin của tổ chức?
* Nếu tấn công xảy ra thì phải mất chi phí bao nhiêu để phục hồi?
* Mối đe dọa nào yêu cầu chi phí phòng tránh lớn nhất?

Mối đe dọa có thể được phân, nhưng không giới hạn các nhóm như sau:

\* Nhóm các mối đe dọa từ việc tồn tại điểm yếu, lỗ hổng trong HT

\* Nhóm các mối đe dọa từ việc thiếu hoặc không đáp ứng các biện pháp quản lý

\* Nhóm các mối đe dọa từ việc thiếu hoặc không đáp ứng các biện pháp

kỹ thuật.

Nhận dạng điểm yếu:

Các điểm yếu có thể có nhiều tiêu chí xác định và được phân làm các nhóm khác nhau.

Xem xét lại đối với mỗi mối đe dọa có thể ảnh hưởng tới tài sản → Lập danh sách các điểm yếu

* Đôi khi mang tính chủ quan, phụ thuộc nhiều vào kinh nghiệm và kiến thức của người thực hiện

→ Nên được bởi một nhóm hiểu thực sự về tổ chức.

Các điểm yếu có thể được phân thành các nhóm sau:

* Nhóm các điểm yếu liên quan đến tồn tại lỗ hổng, điểm yếu ATTT trong HT
* Nhóm các điểm yếu liên quan đến thiếu hoặc không đáp ứng các biện pháp quản lý: không có quy định về sử dụng mật khẩu an toàn, không có quy định về lưu trữ có mã hóa, không có quy định về quy trình xử lý sự cố .v.v.
* Nhóm các điểm yếu liên quan đến thiếu hoặc không đáp ứng các biện pháp kỹ thuật: không có biện pháp phòng chống xâm nhập, không có biện pháp phòng chống mã độc, không có biện pháp phòng chống tấn công .v.v.

## Hãy trình bày về giai đoạn Phân tích rủi ro.

Trình bày giai đoạn Phân tích rủi ro:

Là tạo dựng hiểu biết về rủi ro.

Gồm:

• Đánh giá các hậu quả để xác định mức ảnh hưởng đối với cơ quan, tổ chức khi tài sản bị khai thác điểm yếu gây ra các mối nguy.

• Đánh giá khả năng xảy ra đối với từng loại sự cố.

=> Kết quả: xác định được các hậu quả, mức ảnh hưởng mà cơ quan, tổ chức phải xử lý.

Các phương pháp:

• Định tính: xác định hệ quả, xác suất và mức rủi ro bằng các mức như “cao”, “trung bình” và “thấp”, có thể kết hợp hệ quả và xác suất, và đánh giá mức rủi ro theo các tiêu chí định tính

• Bán định lượng: sử dụng thang chia bằng số đối với hệ quả và xác suất kết hợp chúng để đưa ra một mức rủi ro bằng cách sử dụng công thức. Thang đo có thể là tuyến tính hoặc theo logarit, hay có mối quan hệ khác nào đó, công thức được sử dụng cũng có thể khác nhau.

• Định lượng: ước tính giá trị thực tế đối với hệ quả và xác suất của chúng, và đưa ra giá trị về mức rủi ro theo các đơn vị cụ thể được xác định khi xây dựng bối cảnh.

Mức độ chi tiết cần thiết phụ thuộc vào ứng dụng cụ thể, sự sẵn có của dữ liệu đáng tin cậy và các nhu cầu ra quyết định của tổ chức. Một số phương pháp và mức độ chi tiết của phân tích có thể do luật pháp quy định.

## Hãy trình bày về giai đoạn Xử lý rủi ro.

Trình bày giai đoạn Xử lý rủi ro:

1. Xác định tài sản thông tin: Bước đầu tiên trong quá trình xử lý rủi ro là xác định và đánh giá các tài sản thông tin cần được bảo vệ. Các tài sản thông tin này có thể bao gồm thông tin khách hàng, dữ liệu nhân viên, thông tin tài chính, bí mật công nghệ, v.v.

2. Đánh giá rủi ro: Sau khi xác định được các tài sản thông tin cần được bảo vệ, bước tiếp theo là đánh giá và xác định rủi ro đối với các tài sản đó. Điều này bao gồm việc xác định các nguy cơ tiềm ẩn và xác định mức độ nghiêm trọng của các rủi ro đó.

3. Xây dựng chiến lược và kế hoạch khắc phục: Dựa trên kết quả đánh giá rủi ro, các tổ chức cần xây dựng chiến lược và kế hoạch khắc phục để giảm thiểu hoặc loại bỏ các rủi ro đó.

4. Thực hiện kiểm soát: Sau khi xây dựng kế hoạch khắc phục, các tổ chức cần triển khai các biện pháp kiểm soát để giảm thiểu rủi ro và bảo vệ các tài sản thông tin của mình.

5. Đánh giá kiểm soát: Các tổ chức cần đánh giá hiệu quả của các biện pháp kiểm soát để đảm bảo rằng chúng đang hoạt động đúng cách và giảm thiểu được rủi ro đối với các tài sản thông tin.

6. Kiểm tra các biện pháp kiểm soát có đầy đủ hay chưa: Các tổ chức cần kiểm tra các biện pháp kiểm soát của mình để đảm bảo rằng chúng đang được triển khai đầy đủ và hiệu quả.

7. Kế hoạch bảo trì: Các tổ chức cần có kế hoạch bảo trì để đảm bảo rằng các biện pháp kiểm soát và chiến lược khắc phục đang hoạt động tốt trong suốt thời gian.

8. Đo lường rủi ro đối với tài sản thông tin: Các tổ chức cần đo lường rủi ro đối với các tài sản thông tin của mình để đảm bảo rằng các biện pháp kiểm soát đang hoạt động hiệu quả và hiểu rõ được mức độ rủi ro đối với các tài sản thông tin đó.

9. Xác định xem rủi ro có chấp nhận được hay không: Các tổ chức cần xác định xem mức độ rủi ro đối với các tài sản thông tin có chấp nhận được hay không. Nếu mức độ rủi ro quá cao, các tổ chức cần phải đưa ra các biện pháp khác nhau để giảm thiểu rủi ro đối với các tài sản thông tin đó. Nếu mức độ rủi ro chấp nhận được, các tổ chức có thể tiếp tục triển khai các biện pháp kiểm soát hiện tại để giảm thiểu rủi ro đối với các tài sản thông tin của mình.

## Trình bày các thành phần chính của kế hoạch dự phòng.

* Lập kế hoạch dự phòng (Contingency planning - CP) là quá trình mà các cộng đồng quan tâm đến CNTT và ATTT định vị tổ chức của họ để chuẩn bị, phát hiện, phản ứng và phục hồi từ các sự kiện đe dọa đến AT của tài nguyên và tài sản TT, cả con người và nhân tạo.
* Việc phát triển một kế hoạch để xử lý các sự kiện bất ngờ không mong muốn nên được ưu tiên hàng đầu đối với tất cả các nhà quản lý
* Để một kế hoạch được tất cả các thành viên của tổ chức coi là hợp lệ, kế hoạch đó phải được chấp thuận và được hỗ trợ tích cực bởi cộng đồng doanh nghiệp cùng quan tâm.

CP được tạo thành từ bốn thành phần chính:

* Quy trình thu thập dữ liệu và tài liệu được gọi là phân tích tác động kinh doanh (Business impact analysis - BIA)
* Kế hoạch Ứng phó Sự cố (Incident response plan- IRP)
* Kế hoạch khôi phục sau thảm họa (Disaster recovery plan - DRP)
* Kế hoạch liên tục kinh doanh (Business continuity plan - BCP),

Các tổ chức lớn có thể có nhiều loại kế hoạch và các tổ chức nhỏ có thể có một kế hoạch đơn giản, nhưng hầu hết đều có kế hoạch không đầy đủ

Có thể tạo và phát triển ba yếu tố lập kế hoạch của quá trình CP (kế hoạch IR, DR và ​BC) như một kế hoạch thống nhất hoặc có thể tạo ba yếu tố riêng biệt kết hợp với một tập hợp các thủ tục lồng ghép với nhau để cho phép tính liên tục.

Bốn nhóm tham gia vào việc lập kế hoạch dự phòng và các hoạt động dự phòng:

* nhóm quản lý CP
* nhóm IRP
* nhóm DRP
* nhóm BCP.

Để đảm bảo tính liên tục trong quá trình tạo ra các thành phần CP, quy

trình CP gồm 07 bước:

1. Xây dựng tuyên bố chính sách lập kế hoạch dự phòng.

2. Tiến hành BIA.

3. Xác định các biện pháp kiểm soát phòng ngừa.

4. Tạo chiến lược dự phòng

5. Xây dựng kế hoạch dự phòng

6. Đảm bảo kế hoạch kiểm tra, đào tạo và bài tập

7. Đảm bảo duy trì kế hoạch.

## Trình bày quy trình kế hoạch dự phòng gồm bảy bước do NIST đề xuất.

Trong khái niệm của NIST (National Institute of Standards and Technology), kế hoạch dự phòng (disaster recovery plan - DRP) là một bộ các quy trình được thực hiện trước, trong và sau khi xảy ra sự cố, để giúp tổ chức phục hồi các dịch vụ và hoạt động kinh doanh của mình. Để xây dựng một kế hoạch dự phòng hiệu quả, NIST đề xuất 7 bước sau đây:

1. Khởi đầu và lập danh sách tài sản: Tổ chức cần định danh tất cả các tài sản của mình (như hệ thống, ứng dụng, dữ liệu...) và xác định mức độ quan trọng của chúng đối với hoạt động kinh doanh.
2. Phân tích rủi ro: Tổ chức cần đánh giá các rủi ro tiềm ẩn có thể xảy ra, bao gồm cả các rủi ro về hệ thống, ứng dụng và con người, để tìm ra những điểm yếu cần được bảo vệ.
3. Xác định các biện pháp kiểm soát rủi ro: Tổ chức cần đề xuất các biện pháp kiểm soát rủi ro để giảm thiểu hoặc loại bỏ các rủi ro được xác định trong bước 2.
4. Xây dựng kế hoạch phục hồi: Tổ chức cần xây dựng kế hoạch phục hồi để tái thiết lập các dịch vụ và hoạt động kinh doanh nhanh chóng sau khi xảy ra sự cố.
5. Phát triển kế hoạch kiểm tra và đánh giá: Tổ chức cần phát triển các kế hoạch kiểm tra và đánh giá để đảm bảo tính hiệu quả và đáp ứng kế hoạch phục hồi khi xảy ra sự cố.
6. Thực hiện kế hoạch: Tổ chức cần đào tạo nhân viên và thực hiện kế hoạch phục hồi thường xuyên để đảm bảo sẵn sàng cho các sự cố.
7. Kiểm tra và cập nhật kế hoạch: Tổ chức cần thường xuyên kiểm tra và cập nhật kế hoạch dự phòng để đảm bảo tính hiệu quả và đáp ứng các thay đổi về môi trường kinh doanh, công nghệ và rủi ro mới.

## Trình bày quy trình ứng phó sự cố.

Quy trình ứng cứu sự cố

1. Bắt đầu

2. Chính sách ứng cứu sự cố

3. Lập kế hoạch ứng cứu sự cố

4. Phát hiện sự cố

5. Phản ứng sự cố

6. Phục hồi sau sự cố

1. Bắt đầu:

\* CPMT hình thành IRPT, bắt đầu hoạt động bằng cách phát triển CS xác định hoạt động của nhóm, nêu rõ phản ứng của tổ chức đối với các loại sự cố khác nhau và tư vấn cho người dùng cách đóng góp vào phản ứng hiệu quả của tổ chức , thay vì góp phần vào vấn đề đang xảy ra.

\* IRPT hình thành nhóm ứng phó sự cố bảo mật máy tính (CSIRT)

2. Chính sách ứng cứu sự cố

\* phải được sự hỗ trợ đầy đủ của lãnh đạo cao nhất và được tất cả các bên bị ảnh hưởng hiểu rõ ràng

=> đảm bảo rằng CSIRT đang thực hiện các hành động được ủy quyền; bảo vệ cả các thành viên CSIRT và tổ chức khỏi sự hiểu lầm và trách nhiệm pháp lý tiềm ẩn.

3. Lập kế hoạch ứng cứu sự cố...

* Trách nhiệm tạo kế hoạch IR của tổ chức thường thuộc về CIO, CISO hoặc người quản lý CNTT có trách nhiệm về ATTT
* CISO nên chọn các thành viên từ mỗi cộng đồng liên quan để thành lập một nhóm IR độc lập, nhóm này thực hiện kế hoạch IR.
* Vai trò và trách nhiệm của các thành viên trong nhóm IR được lập thành văn bản và truyền đạt rõ ràng trong toàn tổ chức.
* IRP cũng bao gồm một danh sách cảnh báo, liệt kê một số cá nhân và tổ chức quan trọng nhất định cần được liên hệ trong quá trình xảy ra sự cố.

4. Phát hiện sự cố

\* Phân loại sự cố là quá trình mà nhóm IR xem xét một ứng cử viên sự cố và xác định xem nó có cấu thành một sự cố thực sự hay không.

\* Sau khi sự cố thực tế được xác định và phân loại đúng, các thành viên của nhóm IR có thể thực hiện hiệu quả các thủ tục tương ứng từ IRP.

\* Ba loại chỉ số sự cố được sử dụng: có thể, có thể xảy ra và xác định

5. Phản ứng sự cố

- Thông báo của Nhân sự Chủ chốt: Có hai cách để kích hoạt danh sách cảnh báo: tuần tự và phân cấp (có sẵn nhiều HT tự động tạo điều kiện thuận lợi cho cả hai cách tiếp cận)

- Ghi lại sự cố: phải ghi lại ai, cái gì, khi nào, ở đâu, tại sao và cách thức của từng hành động được thực hiện trong khi sự cố đang xảy ra.

- Các chiến lược ngăn chặn sự cố: Vô hiệu hóa tài khoản người dùng bị xâm phạm, Cấu hình lại tường lửa để chặn lưu lượng sự cố, …

- Báo cáo sự cố: trong quá trình BIA, phải xác định thời điểm một sự cố được coi là một thảm họa. Các tiêu chí này phải được bao gồm trong IRP. Tổ chức cũng phải lập thành văn bản khi nào cần sự tham gia của những người phản ứng bên ngoài.

6. Phục hồi sau sự cố

- Khi sự cố đã được kiểm soát và kiểm soát hệ thống đã được khôi phục, quá trình khắc phục sự cố có thể bắt đầu.

- Thông báo cho nguồn nhân lực phù hợp

- CSIRT phải đánh giá toàn bộ mức độ thiệt hại để xác định những gì phải làm để khôi phục hệ thống

## Liệt kê và mô tả các tiêu chí được sử dụng để xác định xem một sự cố thực sự có đang xảy ra hay không.

Việc xác định xem một sự cố thực sự đang xảy ra hay không là rất quan trọng để đưa ra các biện pháp ứng cứu kịp thời. Dưới đây là một số tiêu chí thường được sử dụng để xác định xem một sự cố thực sự đang xảy ra hay không:

+ Các thông báo từ hệ thống: Hệ thống có thể đưa ra các thông báo về các lỗi hoặc cảnh báo khi có sự cố xảy ra.

+ Sự gián đoạn hoạt động: Một sự cố thường làm gián đoạn hoạt động của hệ thống hoặc quá trình sản xuất, do đó, nếu có bất kỳ sự gián đoạn nào trong quá trình làm việc, có thể xem xét rằng có sự cố đang xảy ra.

+ Sự cố xảy ra đột ngột: Sự cố thường xảy ra đột ngột mà không có dấu hiệu cảnh báo hoặc thông báo trước đó.

+ Khi lượng sản phẩm hoặc dịch vụ không đạt được các tiêu chuẩn chất lượng: Nếu sản phẩm hoặc dịch vụ không đạt được tiêu chuẩn chất lượng hoặc các yêu cầu về quy trình sản xuất thì có thể đó là dấu hiệu của một sự cố.

+ Điểm báo từ nhân viên hoặc khách hàng: Nhân viên hoặc khách hàng có thể phát hiện ra sự cố và báo cáo lại cho nhóm ứng cứu.

+ Phân tích dữ liệu: Các dữ liệu về hoạt động của hệ thống hoặc quá trình sản xuất có thể được phân tích để tìm ra các dấu hiệu của sự cố.

+ Thực tế vật lý: Sự cố có thể dẫn đến các hư hỏng vật lý, cháy nổ, ảnh hưởng đến môi trường hoặc đe dọa đến sự an toàn của con người, do đó, việc quan sát và phát hiện các thay đổi trong vật lý là một cách xác định sự cố.

+Trong quá trình xác định sự cố, nhóm ứng cứu cần phải đưa ra quyết định kịp thời và chính xác để đảm bảo an toàn và giảm thiểu thiệt hại tối đa.

## Chính sách an toàn thông tin là gì? Tại sao nó lại quan trọng đối với sự thành công của chương trình An toàn thông tin?

CSATTT là: Các hướng dẫn bằng văn bản do cấp quản lý cung cấp nhằm thông báo cho nhân viên và những người khác tại nơi làm việc về hành vi thích hợp liên quan đến việc sử dụng thông tin và tài sản thông tin một cách thích hợp và an toàn.

Chính sách an toàn thông tin rất quan trọng đối với sự thành công của chương trình An toàn thông tin vì các lý do sau:

* Bảo vệ thông tin quan trọng: Chính sách an toàn thông tin giúp đảm bảo rằng thông tin quan trọng và nhạy cảm của tổ chức được bảo vệ khỏi các cuộc tấn công mạng, tấn công từ bên trong và sự cố an ninh mạng khác.
* Tuân thủ các quy định và luật pháp: Các chính sách an toàn thông tin định hướng tổ chức tuân thủ các quy định và luật pháp liên quan đến bảo vệ thông tin, như GDPR, PCI DSS, HIPAA và nhiều hơn nữa.
* Đảm bảo tính sẵn sàng: Chính sách an toàn thông tin giúp đảm bảo tính sẵn sàng của hệ thống và thông tin của tổ chức. Nó hướng dẫn các quy trình phục hồi dữ liệu và khôi phục hệ thống sau sự cố an ninh mạng, giúp tổ chức phục hồi dữ liệu nhanh chóng và tránh mất mát dữ liệu quan trọng.
* Tăng niềm tin của khách hàng: Chính sách an toàn thông tin là một yếu tố quan trọng để tăng niềm tin của khách hàng vào tổ chức. Nó cho thấy rằng tổ chức đang làm việc chăm chỉ để đảm bảo rằng thông tin khách hàng được bảo mật và an toàn.
* Giảm rủi ro: Bằng cách đưa ra các biện pháp an toàn cần thiết, chính sách an toàn thông tin giúp giảm rủi ro an ninh mạng, đồng thời giảm thiểu các thiệt hại liên quan đến sự cố an ninh mạng.

## Liệt kê và mô tả ba thách thức trong việc định hình chính sách.

Định hình chính sách là quá trình lập kế hoạch và thiết lập các quy định và nguyên tắc để điều hành một lĩnh vực hoặc hành động cụ thể của một tổ chức hoặc chính phủ. Có nhiều thách thức trong việc định hình chính sách, tuy nhiên, dưới đây là ba thách thức chính:

+ Thách thức về thông tin: Đối với các quyết định chính sách chính xác, cần phải có thông tin đầy đủ, chính xác và đáng tin cậy. Tuy nhiên, trong một số trường hợp, thông tin có thể bị giấu kín hoặc không được công khai, điều này có thể làm cho quá trình định hình chính sách trở nên khó khăn hoặc bị lệch hướng. Ngoài ra, thông tin có thể bị bóp méo bởi các lợi ích riêng của những người liên quan đến chính sách đó.

+ Thách thức về tham gia: Các chính sách được thiết lập có thể ảnh hưởng đến nhiều bên liên quan, bao gồm các nhóm cộng đồng, tổ chức và các bên liên quan khác. Do đó, việc đảm bảo rằng các bên liên quan tham gia vào quá trình định hình chính sách là rất quan trọng. Tuy nhiên, việc đưa ra quyết định có thể bị ảnh hưởng bởi những người có quyền lực, không đảm bảo đúng mức độ phù hợp với các lợi ích của các bên liên quan khác.

+ Thách thức về tài chính: Các chính sách thường phải đi kèm với ngân sách để thực hiện. Điều này có thể gây ra thách thức trong việc định hình chính sách, đặc biệt là trong những trường hợp ngân sách bị giới hạn. Nếu quá trình định hình chính sách không xem xét được khía cạnh tài chính, các chính sách đó có thể gây áp lực tài chính không mong muốn, làm ảnh hưởng đến các dự án và hoạt động khác của tổ chức hoặc chính phủ.

## Phân biệt: Chính sách, tiêu chuẩn, thủ tục

Chính sách, tiêu chuẩn và thủ tục là các thuật ngữ liên quan đến việc quản lý và điều hành trong một tổ chức. Tuy nhiên, chúng có ý nghĩa và phạm vi khác nhau. Dưới đây là sự khác biệt giữa chính sách, tiêu chuẩn và thủ tục:

+ Chính sách: là các quy định, nguyên tắc hoặc hướng dẫn chi tiết mà một tổ chức thiết lập để quản lý hoạt động của mình và đảm bảo các hoạt động này đúng với mục đích của tổ chức. Chính sách thường có tầm nhìn và chiến lược dài hạn, và chú trọng đến các giá trị và tiêu chuẩn của tổ chức.

+ Tiêu chuẩn: là các tiêu chí hoặc yêu cầu cụ thể được đặt ra để đảm bảo rằng các sản phẩm, dịch vụ hoặc hoạt động của tổ chức đáp ứng được chất lượng, an toàn, độ tin cậy hoặc hiệu quả mong muốn. Tiêu chuẩn thường được thiết lập bởi các tổ chức chuẩn hóa và công nhận trên cơ sở các tiêu chuẩn quốc tế, vì vậy các sản phẩm hoặc dịch vụ đáp ứng tiêu chuẩn này có thể được chấp nhận trên toàn cầu.

+ Thủ tục: là các bước hoặc quy trình cụ thể được thiết lập để điều hành các hoạt động hoặc quy trình trong tổ chức. Thủ tục thường được thiết lập để đảm bảo rằng các hoạt động hoặc quy trình được thực hiện đúng cách và đáp ứng được các tiêu chuẩn và chính sách của tổ chức. Thủ tục thường được thiết lập với mục đích hạn chế các rủi ro và tối ưu hóa hiệu suất hoạt động của tổ chức.

Tóm lại, chính sách, tiêu chuẩn và thủ tục đều là các công cụ quản lý được sử dụng trong một tổ chức. Chính sách và tiêu chuẩn thường được thiết lập để định hướng cho hoạt động của tổ chức, trong khi thủ tục thường được sử dụng để điều hành và quản lý các hoạt động cụ thể của tổ chức.

## Trình bày về quy trình xây dựng CS theo cách tiếp cận quản lý dự án

Tiếp cận quản lý dự án trong xây dựng chính sách bảo mật (CS) được xem như một cách tiếp cận hợp lý, giúp đảm bảo rằng các hoạt động xây dựng CS sẽ được thực hiện một cách có tổ chức và hiệu quả. Quy trình xây dựng CS theo cách tiếp cận quản lý dự án có thể được chia thành các giai đoạn sau:

Giai đoạn khảo sát: Nhóm phát triển CS cần đạt được:

* Hỗ trợ từ quản lý cấp cao
* Hỗ trợ và tham gia tích cực vào quản lý CNTT, đặc biệt là CIO
* Mô tả rõ ràng các mục tiêu
* Sự tham gia của các cá nhân phù hợp từ các cộng đồng có lợi ích bị ảnh hưởng bởi các CS
* Đề cương chi tiết về phạm vi của dự án phát triển CS và các ước tính hợp lý về chi phí và lịch trình của dự án.

Giai đoạn phân tích

* Đánh giá rủi ro mới hoặc gần đây hoặc kiểm toán CNTT ghi lại các nhu cầu ATTT hiện tại của tổ chức.
* Tập hợp các tài liệu tham khảo chính, bao gồm CS hiện hành.
* Xác định triết lý cơ bản của tổ chức khi đưa ra CS. Triết lý này thường thuộc một trong hai nhóm:

“Điều nào không được phép sẽ bị cấm” (phương pháp “danh sách trắng”)

"Điều nào không bị cấm được cho phép” (phương pháp “danh sách đen”).

Giai đoạn thiết kế: Nhiệm vụ đầu tiên trong giai đoạn thiết kế là soạn thảo văn bản CS thực tế. Thông số kỹ thuật cho bất kỳ công cụ tự động nào. Sửa đổi báo cáo phân tích khả thi dựa trên chi phí và lợi ích được cải thiện khi thiết kế được làm rõ. Chuyển đến người quản lý hoặc điều hành phê duyệt để thực thi.

Giai đoạn thực thi: Người dùng hoặc các thành viên của tổ chức phải thừa nhận một cách rõ ràng rằng họ đã nhận và đọc CS (tuân thủ). Các chính sách sẽ được phân phối như thế nào. Việc xác minh phân phối sẽ được thực hiện như thế nào

Giai đoạn bảo trì: Nhóm phát triển CS giám sát duy trì và sửa đổi CS khi cần thiết để đảm bảo rằng CS đó vẫn hiệu quả như một công cụ để đáp ứng các mối đe dọa đang thay đổi. Phải có một cơ chế tích hợp để người dùng có thể báo cáo sự cố, tốt nhất là ẩn danh thông qua biểu mẫu Web được giám sát bởi nhóm pháp lý của tổ chức hoặc một ủy ban được giao nhiệm vụ thu thập và xem xét nội dung đó. Phải đảm bảo rằng mọi người được yêu cầu tuân theo CS một cách bình đẳng và các CS không được thực hiện khác nhau trong các lĩnh vực hoặc thứ bậc khác nhau của tổ chức.

## Hãy trình bày tóm tắt về các thành phần của Quản lý An toàn thông tin.

Quản lý An toàn thông tin là một quá trình quản lý các hoạt động, chính sách, quy trình và công cụ để bảo vệ thông tin quan trọng của tổ chức khỏi các mối đe dọa bảo mật. Quản lý an toàn thông tin bao gồm các thành phần sau:

* Chính sách: Đây là các hướng dẫn, quy định và quy tắc mà tổ chức thiết lập để quản lý thông tin an toàn. Chính sách an toàn thông tin phải được cập nhật thường xuyên và đảm bảo rằng các hoạt động an toàn thông tin đang được thực hiện theo các tiêu chuẩn an toàn thông tin hiện đại.
* Quản lý rủi ro: Quản lý rủi ro bao gồm việc đánh giá các mối đe dọa bảo mật, xác định các điểm yếu của hệ thống và tìm cách giảm thiểu rủi ro. Các hoạt động quản lý rủi ro bao gồm đánh giá rủi ro, xác định các giải pháp bảo mật, triển khai các biện pháp bảo mật và theo dõi hiệu quả của các biện pháp bảo mật đã triển khai.
* Quản lý truy cập: Quản lý truy cập đảm bảo rằng chỉ những người được ủy quyền mới có thể truy cập vào thông tin quan trọng của tổ chức. Quản lý truy cập bao gồm việc xác định quyền truy cập của từng người dùng, kiểm soát quyền truy cập vào các tài nguyên và theo dõi việc sử dụng tài nguyên.
* Quản lý nhân viên: Quản lý nhân viên bao gồm việc đảm bảo rằng nhân viên được đào tạo về an toàn thông tin, đảm bảo việc tuyển dụng an toàn và thực hiện các biện pháp an toàn cho nhân viên như kiểm soát truy cập, giám sát hoạt động và giáo dục.
* Quản lý liên kết: Quản lý liên kết đảm bảo rằng các liên kết với các tổ chức khác đều tuân thủ các tiêu chuẩn an toàn thông tin. Quản lý liên kết bao gồm việc đánh giá các mối đe dọa bảo mật từ các liên kết và đảm bảo rằng các tiêu chuẩn an toàn thông tin được áp dụng trong quá trình liên kết với các đối tác và nhà cung cấp khác.
* Quản lý bảo vệ dữ liệu: Quản lý bảo vệ dữ liệu đảm bảo rằng thông tin quan trọng của tổ chức được bảo vệ khỏi các mối đe dọa bảo mật như lắng nghe trái phép, tấn công mạng và phá hoại dữ liệu. Quản lý bảo vệ dữ liệu bao gồm việc áp dụng các biện pháp bảo mật dữ liệu, lưu trữ và chia sẻ dữ liệu một cách an toàn.
* Quản lý sự cố: Quản lý sự cố đảm bảo rằng tổ chức có khả năng phát hiện, ứng phó và khắc phục các sự cố an toàn thông tin. Quản lý sự cố bao gồm việc xác định và đánh giá các sự cố, phát triển kế hoạch ứng phó, thực hiện các biện pháp khẩn cấp và phục hồi sau sự cố.
* Kiểm tra và đánh giá: Kiểm tra và đánh giá đảm bảo rằng các biện pháp bảo mật an toàn thông tin đang được thực hiện theo các tiêu chuẩn an toàn thông tin hiện đại. Các hoạt động kiểm tra và đánh giá bao gồm kiểm tra bảo mật hệ thống, kiểm tra đánh giá rủi ro và kiểm tra đánh giá hiệu quả của các biện pháp bảo mật.

Tóm lại, quản lý an toàn thông tin bao gồm nhiều thành phần quan trọng để đảm bảo rằng thông tin quan trọng của tổ chức được bảo vệ khỏi các mối đe dọa bảo mật. Các thành phần này bao gồm chính sách, quản lý rủi ro, quản lý truy cập, quản lý nhân viên, quản lý liên kết, quản lý bảo vệ dữ liệu, quản lý sự cố và kiểm tra và đánh giá.

## Vai trò của Luật pháp và Đạo đức trong Quản lý An toàn thông tin.

Luật pháp và đạo đức đóng vai trò rất quan trọng trong quản lý an toàn thông tin. Cả hai yếu tố này đều có mục đích là đảm bảo rằng thông tin quan trọng của tổ chức được bảo vệ khỏi các mối đe dọa bảo mật.

Luật pháp được sử dụng để thiết lập các quy định pháp lý và các quy tắc mà tổ chức phải tuân thủ để đảm bảo an toàn thông tin. Các quy định này có thể bao gồm các quy định về bảo mật mạng, quyền riêng tư và bảo vệ dữ liệu. Ngoài ra, luật pháp cũng thiết lập các biện pháp xử phạt cho các tổ chức không tuân thủ các quy định an toàn thông tin.

Đạo đức cũng đóng vai trò quan trọng trong quản lý an toàn thông tin. Nó bao gồm các nguyên tắc đạo đức và giá trị mà tổ chức phải tuân thủ trong việc quản lý và sử dụng thông tin. Ví dụ như, đạo đức yêu cầu các tổ chức không sử dụng thông tin của khách hàng hoặc nhân viên một cách phi pháp hoặc không đúng mục đích. Đạo đức còn yêu cầu các tổ chức phải bảo vệ thông tin của khách hàng và nhân viên khỏi các mối đe dọa bảo mật.

Các tổ chức cần phải có chính sách và quy trình rõ ràng để đảm bảo rằng các quy định pháp lý và các nguyên tắc đạo đức được tuân thủ. Ngoài ra, các tổ chức cần có một nền văn hóa an toàn thông tin, nơi mọi người trong tổ chức được đào tạo và hướng dẫn về quy định và nguyên tắc đạo đức trong việc quản lý an toàn thông tin.

Tóm lại, Luật pháp và đạo đức đóng vai trò quan trọng trong quản lý an toàn thông tin. Các tổ chức cần tuân thủ các quy định pháp lý và nguyên tắc đạo đức để đảm bảo rằng thông tin quan trọng của họ được bảo vệ khỏi các mối đe dọa bảo mật.

# Phần bài tập: From AT16H with love <3

## Xây dựng chính sách an toàn thông tin cho một hệ thống cụ thể (một hệ thống nhỏ hoặc một phần trong hệ thống, cần phải tuân thủ khuôn mẫu của chính sách an toàn thông tin).

Xây dựng chính sách an toàn thông tin (Information Security Policy) là một quá trình quan trọng giúp đảm bảo rằng các thông tin quan trọng của tổ chức được bảo vệ khỏi các mối đe dọa bảo mật. Dưới đây là các bước để xây dựng chính sách an toàn thông tin tuân thủ khuôn mẫu cho một hệ thống cụ thể:

Tên chính sách và thông tin định danh:

1. Mục đích

2. Tổng quan

3. Phạm vi

4. Chính sách

5. Vai trò và trách nhiệm

6. Luật/Hướng dẫn áp dụng

7. Tính hiệu lực

8. Thông tin và hỗ trợ

9. Phê chuẩn

10. Tài liệu tham chiếu ./.

***Ví dụ như sau:***

Tên chính sách: Chính sách an toàn thông tin của công ty ABC

1. Mục đích: Chính sách an toàn thông tin của công ty ABC nhằm đảm bảo tính bảo mật và an toàn cho thông tin của công ty và khách hàng, tránh nguy cơ mất mát thông tin, ảnh hưởng đến hoạt động kinh doanh và danh tiếng của công ty.

2. Tổng quan: Chính sách này áp dụng cho tất cả các hoạt động liên quan đến thông tin của công ty ABC, bao gồm thông tin nội bộ, thông tin khách hàng, thông tin nhân viên, thông tin đối tác và các thông tin liên quan khác.

3. Phạm vi: Chính sách này bao gồm các quy định và hướng dẫn về việc quản lý, bảo mật và sử dụng thông tin, cũng như các biện pháp phòng chống các mối đe dọa về an ninh mạng và các cuộc tấn công mạng khác.

4. Chính sách: Công ty ABC cam kết thực hiện các biện pháp bảo mật thông tin bằng cách áp dụng các tiêu chuẩn và quy trình bảo mật thông tin hiện đại, đảm bảo tính bảo mật và an toàn cho thông tin của công ty và khách hàng.

5. Vai trò và trách nhiệm: Mỗi nhân viên và bộ phận trong công ty đều có trách nhiệm chung trong việc thực hiện chính sách an toàn thông tin. Công ty cũng có các chuyên gia bảo mật thông tin chịu trách nhiệm giám sát và đảm bảo thực hiện chính sách này.

6. Luật/Hướng dẫn áp dụng: Chính sách này tuân thủ các luật, quy định liên quan đến an ninh mạng và bảo mật thông tin.

7. Tính hiệu lực: Chính sách an toàn thông tin này có hiệu lực ngay khi được thông báo đến tất cả nhân viên trong công ty ABC.

8. Thông tin và hỗ trợ: Công ty ABC cung cấp các thông tin và hỗ trợ liên quan đến an ninh mạng và bảo mật thông tin cho nhân viên và khách hàng của mình.

9. Phê chuẩn: Chính sách này được phê chuẩn bởi Ban Giám đốc công ty ABC.

10. Tài liệu tham chiếu: Tài liệu tham chiếu cho chính sách an toàn thông tin của công ty ABC bao gồm các hướng dẫn về bảo mật thông tin, quy định về sử dụng và truy cập thông tin, quy trình xử lý thông tin cá nhân, hướng dẫn về phát hiện và giải quyết các vấn đề an ninh mạng, cũng như các tài liệu liên quan khác.

Ngoài ra, chính sách an toàn thông tin của công ty ABC còn bao gồm các biện pháp đảm bảo an toàn thông tin trong việc sử dụng các thiết bị di động, đảm bảo tính bảo mật của dữ liệu khi truyền qua mạng và các biện pháp xử lý các sự cố liên quan đến an ninh mạng và bảo mật thông tin.

Tất cả các nhân viên và bộ phận trong công ty ABC được yêu cầu thực hiện chính sách an toàn thông tin này trong quá trình làm việc của mình. Công ty cũng đảm bảo việc giáo dục và huấn luyện nhân viên về các quy định và biện pháp bảo mật thông tin liên quan đến công việc của họ.

Chính sách an toàn thông tin của công ty ABC được đánh giá và cập nhật định kỳ để đảm bảo tính hiệu lực và phù hợp với các thay đổi về an ninh mạng và bảo mật thông tin. Nếu có bất kỳ vấn đề an ninh mạng hay bảo mật thông tin nào xảy ra, công ty sẽ có các biện pháp khẩn cấp để đối phó và giải quyết vấn đề.

## Ước lượng rủi ro cho một hệ thống.

Chú thích các chữ viết tắt:

V: Giá trị tài sản

P: Khả năng xuất hiện 1 điểm yếu

RR: Rủi ro

R: Mức độ rủi ro được giảm thiểu do các kiểm soát an toàn

U: Mức độ rủi ro do sự không chắc chắn của các tri thức hiện tại về điểm yếu

- Bước 1: Xác định các giá trị sau:

Giá trị của V, P và tính P\*V

Tiếp theo tính:

R = (sự kiểm soát mức độ đạt được là x%) \* PV

Nếu mức độ không đạt được thì lấy 100% - x%

U = (độ ước lượng không chắc chắn y%) \* PV

Nếu độ ước lượng chắc chắn thì lấy 100% - y%

- Bước 2: Tính RR cho từng điểm yếu theo công thức

RR = PV-R+U

- Bước 3: Thứ tự ưu tiên

Cái nào RR càng cao thì viết đầu, vd: ĐY3,ĐY1,ĐY2,...

