Risk Management: Controlling Risk

Nội dung chính

I. Giới thiệu

II. Phân tích, đánh giá rủi ro

III. Chiến lược kiểm soát rủi ro

IV. Quản lý rủi ro

V. Tính khả thi và phân tích lợi ích – Chi phí

VI. Thực hành kiểm soát rủi ro

I. Giới thiệu

Để theo kịp sự cạnh tranh, các tổ chức phải tạo ra một môi trường an toàn trong quy trình và thủ tục kinh

Môi trường phải duy trì tính bảo mật và quyền riêng tư cũng như đảm bảo tính toàn vẹn và tính sẵn có của dữ liệu tổ chức

I. Giới thiệu

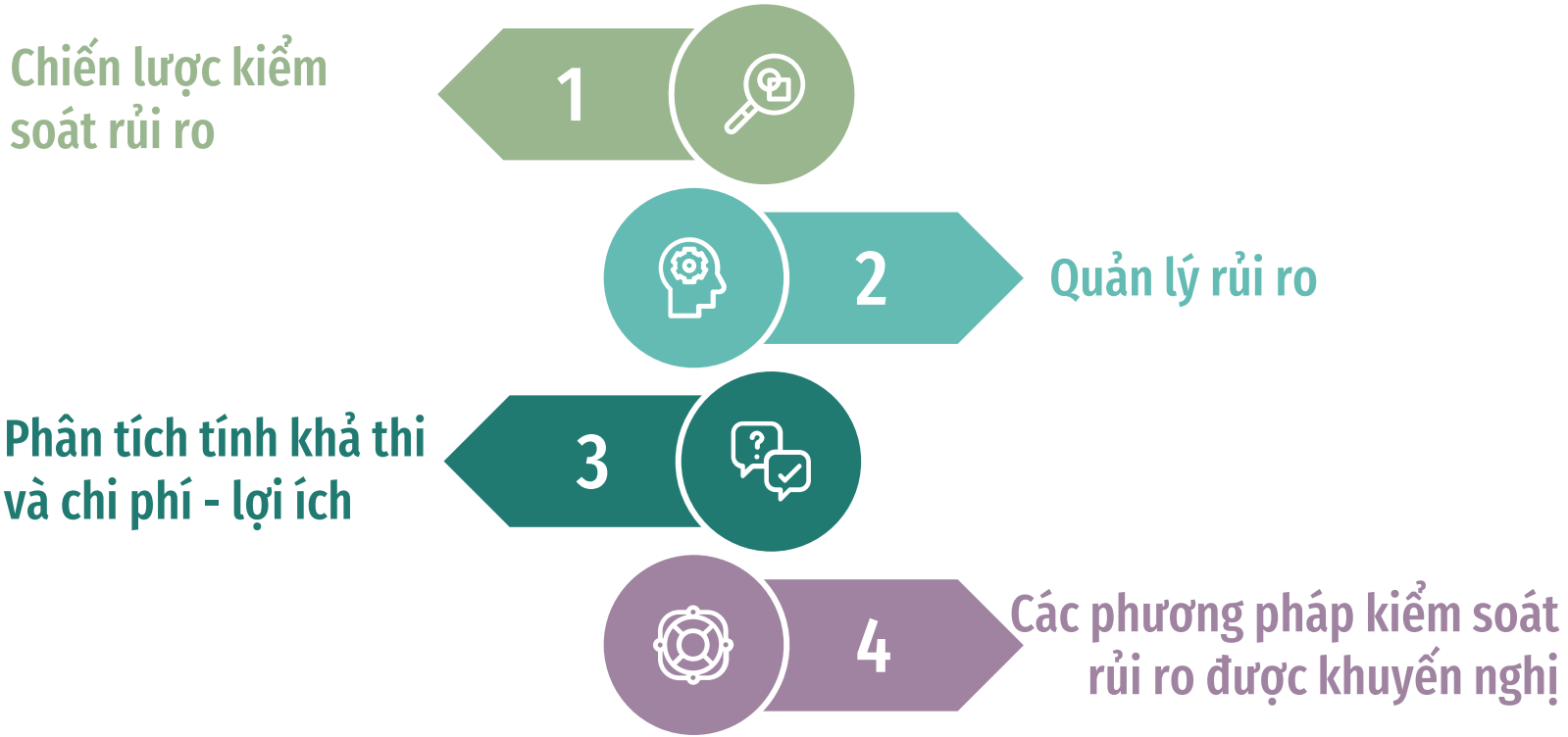
Quản lý rủi ro (Risk management): là quá trình xác định rủi ro và đánh giá mức độ tương đối của nó, đồng thời thực hiện các bước kiểm soát để đưa rủi ro về mức có thể chấp nhận được.

Ta có 3 mục quan trọng trong việc quản lý rủi ro:

1. Đánh giá rủi ro (Risk assessment): là việc xác định mức độ rủi ro mà tài sản thông tin của tổ chức phải chịu.
2. Xác định rủi ro (Risk identification): là việc liệt kê, dự đoán và lập danh sách về các rủi ro đối với tài sản thông tin của tổ chức.
3. Kiểm soát rủi ro (Risk control): là việc áp dụng các biện pháp kiểm soát nhằm giảm mức độ thiệt hại của rủi ro tới tài sản thông tin của tổ chức xuống mức có thể chấp nhận được.

Ở báo cáo này, chúng ta tập trung phân tích và tìm hiểu Risk Management: Controlling Risk, và cách thức hoạt động của nó.

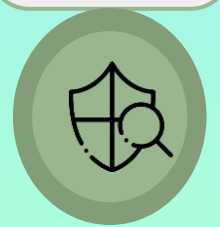
II. Nội dung chính



1. Chiến lược kiểm soát rủi ro

Phòng thủ

Áp dụng các biện pháp bảo vệ để loại bỏ hoặc giảm thiểu rủi ro không thể kiểm soát



Chuyển giao

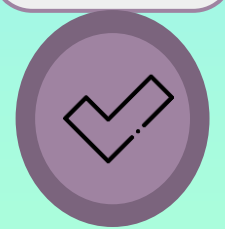
Chuyển các rủi ro sang khu vực khác hoặc các tổ chức bên ngoài

Giảm thiểu

Giảm các tác động đến nội dung thông tin nếu kẻ tấn công khai thác lỗ hổng thành công

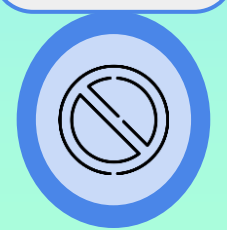
Chấp nhận

Hiểu được hậu quả của việc không kiểm soát được rủi ro và ghi nhận rủi ro vẫn tồn tại mà không cố gắng kiểm soát



Chấm dứt

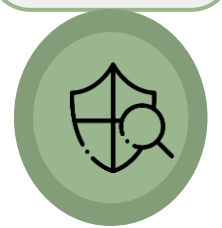
Xóa bỏ hoặc ngừng cung cấp nội dung thông tin từ môi trường hoạt động của tổ chức



1. Chiến lược kiểm soát rủi ro

Phòng thủ

Áp dụng các biện pháp bảo vệ để loại bỏ hoặc giảm thiểu rủi ro không thể kiểm soát



Là chiến lược kiểm soát rủi ro cố gắng loại bỏ hoặc giảm thiểu bất kỳ rủi ro không bị kiểm soát, còn lại sẽ thông qua việc áp dụng các biện pháp kiểm soát và biện pháp bảo vệ bổ sung.

Có 3 phương pháp phòng thủ rủi ro phổ biến:

- **Áp dụng chính sách:** việc áp dụng chính sách cho phép tất cả các cấp quản lý bắt buộc phải tuân theo 1 quy trình nhất định.
- **Giáo dục và đào tạo:** truyền đạt chính sách mới cho nhân viên không đảm bảo rằng họ sẽ tuân thủ. Nhận thức, đào tạo và giáo dục là điều thiết yếu để tạo nên 1 môi trường tổ chức an toàn và có kiểm soát hơn, và để đạt được những thay đổi cần thiết về hành vi của nhân viên.
- **Ứng dụng công nghệ:** ngày nay, các kỹ thuật kiểm soát và biện pháp bảo vệ thường được sử dụng để giảm thiểu rủi ro một cách hiệu quả.

1. Chiến lược kiểm soát rủi ro

Chuyển giao

Chuyển các rủi ro sang khu vực khác hoặc các tổ chức bên ngoài

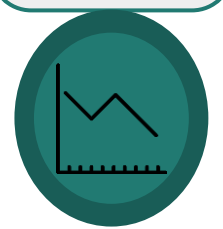
Chiến lược kiểm soát rủi ro chuyển giao cố gắng chuyển rủi ro sang tài sản, quy trình hoặc tổ chức khác. Các kiểm soát này được thực hiện bằng cách cân nhắc cách cung cấp dịch vụ, sửa đổi mô hình triển khai, thuê các tổ chức bên ngoài, mua bảo hiểm hoặc ký hợp đồng dịch vụ với nhà cung cấp.

Các tổ chức nên cân nhắc kỹ trước khi mở rộng hoạt động của mình, bao gồm quản lý thông tin và hệ thống, và thậm chí cả về an toàn thông tin. Khi 1 tổ chức không có đủ kinh nghiệm quản lý và điều hành an ninh, họ nên thuê các cá nhân hoặc những nhà cung cấp có chuyên môn trong lĩnh vực đó.

1. Chiến lược kiểm soát rủi ro

Giảm thiểu

Giảm các tác động đến nội dung thông tin nếu kẻ tấn công khai thác lỗ hổng thành công



Chiến lược kiểm soát rủi ro giảm thiểu là cách cố gắng giảm thiểu thiệt hại do 1 sự cố hoặc thảm họa gây ra đến mức tối thiểu.

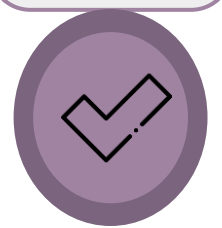
Chiến lược này gồm 3 kế hoạch dự phòng:

- **Kế hoạch ứng phó trước sự cố (IR):** là các hành động mà tổ chức nên thực hiện trong khi sự cố đang diễn ra. Kế hoạch IR cho phép tổ chức thực hiện các hành động phối hợp được xác định trước hoặc đặc biệt cần thiết.
- **Kế hoạch khắc phục hậu quả (DR):** là quy trình phổ biến nhất trong các kế hoạch giảm thiểu, kế hoạch DR bao gồm tất cả các bước chuẩn bị cho quá trình khôi phục, các chiến lược nhằm hạn chế thiệt hại và các bước chi tiết cần làm sau đó.
- **Kế hoạch kinh doanh liên tục (BC):** là kế hoạch chiến lược dài hạn nhất trong 3 kế hoạch. Kế hoạch BC bao gồm các bước cần thiết để đảm bảo sự tiếp tục hoạt động của tổ chức khi phạm vi hoặc quy mô của sự cố vượt quá khả năng khôi phục của kế hoạch DR, thông thường sẽ là di dời các chức năng kinh doanh quan trọng đến 1 địa điểm khác thay thế.

1. Chiến lược kiểm soát rủi ro

Chấp nhận

Hiểu được hậu quả của việc không kiểm soát được rủi ro và ghi nhận rủi ro vẫn tồn tại mà không cố gắng kiểm soát



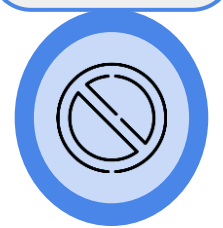
Như đã nói ở trên, giảm thiểu là 1 cách tiếp cận kiểm soát nhằm giảm tác động của 1 lỗ hổng bị khai thác bằng cách chuẩn bị phòng bị nếu và khi nó xảy ra. Ngược lại, **chiến lược kiểm soát rủi ro chấp nhận là việc quyết định không làm gì để bảo vệ thông tin khỏi rủi ro và chấp nhận kết quả từ bất kỳ hoạt động khai thác nào.** Việc chấp nhận rủi ro 1 cách vô thức không phải là cách tiếp cận khả thi để kiểm soát rủi ro. Việc chấp nhận chỉ có tác dụng khi tổ chức có:

- Xác định mức độ rủi ro đối với tài nguyên thông tin
- Đánh giá xác suất tấn công và khả năng khai thác lỗ hổng thành công
- Ước tính thiệt hại hoặc tổn thất có thể xảy ra do các cuộc tấn công
- Các biện pháp kiểm soát tiềm năng đã được sử dụng từng loại để đánh giá tính khả thi
- Phân tích kỹ lưỡng chi phí - lợi ích (CBA)
- Xác định rõ chi phí để kiểm soát rủi ro đối với 1 chức năng, dịch vụ, thu thập dữ liệu hoặc tài nguyên thông tin cụ thể vượt quá chi phí thực hiện và duy trì các biện pháp kiểm soát

1. Chiến lược kiểm soát rủi ro

Chấm dứt

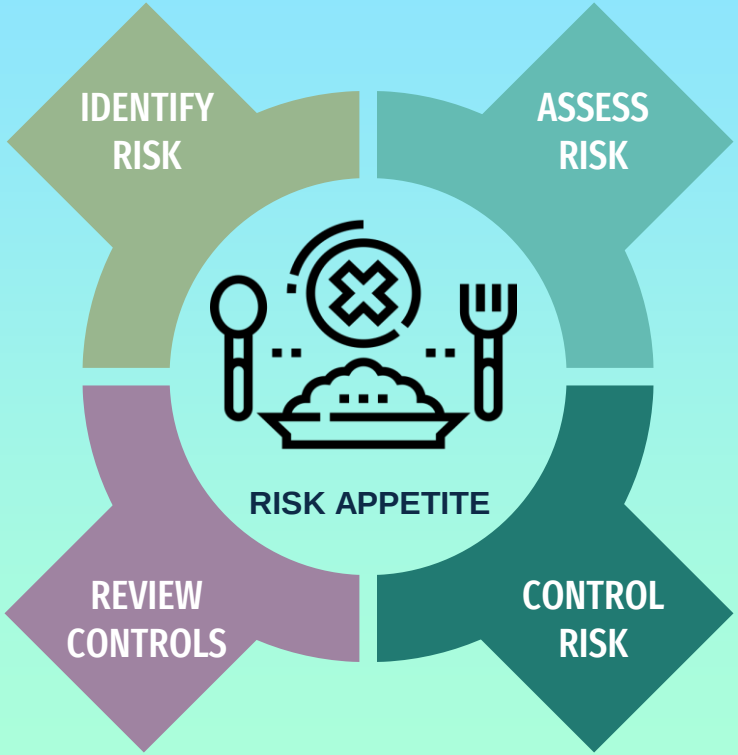
Xóa bỏ hoặc ngừng cung cấp nội dung thông tin từ môi trường hoạt động của tổ chức



Cũng như chiến lược chấp nhận, chiến lược kiểm soát rủi ro chấm dứt dựa trên nhu cầu của tổ chức hoặc sự lựa chọn không bảo vệ tài nguyên. Tuy nhiên, ở đây tổ chức không muốn tài nguyên thông tin tiếp tục gặp rủi ro, do đó sẽ loại bỏ nó khỏi môi trường rủi ro.

Đôi khi, chi phí bảo vệ một tài sản còn lớn hơn giá trị của nó. Trong những trường hợp khác, việc bảo vệ tài sản có thể quá khó khăn hoặc tốn kém so với giá trị hoặc lợi ích mà nó mang lại cho công ty. Do vậy, việc chấm dứt không chỉ là 1 quyết định đơn giản mà còn cần những điều kiện kỹ thuật đầy đủ để được chấp nhận.

Risk appetite – Khẩu vị rủi ro



Ta có khái niệm Risk appetite – "khẩu vị rủi ro" hay còn gọi là "khả năng chấp nhận rủi ro (thiệt hại)" là thuật ngữ để chỉ mức rủi ro mà một nhà đầu tư, doanh nghiệp, công ty, cá nhân,… có thể chấp nhận được, được cho phép để theo đuổi mục tiêu, chiến lược đã đề ra. Nếu 1 công ty, tổ chức có mức khẩu vị rủi ro cao thì sẽ mang lại nhiều lợi ích tiềm năng hơn.

Ngoài ra khẩu vị rủi ro khi đã được xác định rõ ràng còn giúp đảm bảo cho việc đưa ra các quyết định trong một dự án được phù hợp nhất với những mục tiêu và chiến lược chung trong một tổ chức.

Mục tiêu của InfoSec(Information Security – Bảo mật thông tin) không phải là đưa rủi ro còn lại về 0, mà là nó mang lại rủi ro còn lại phù hợp với khả năng chấp nhận rủi ro của tổ chức.

Residual risk – Rủi ro tồn đọng

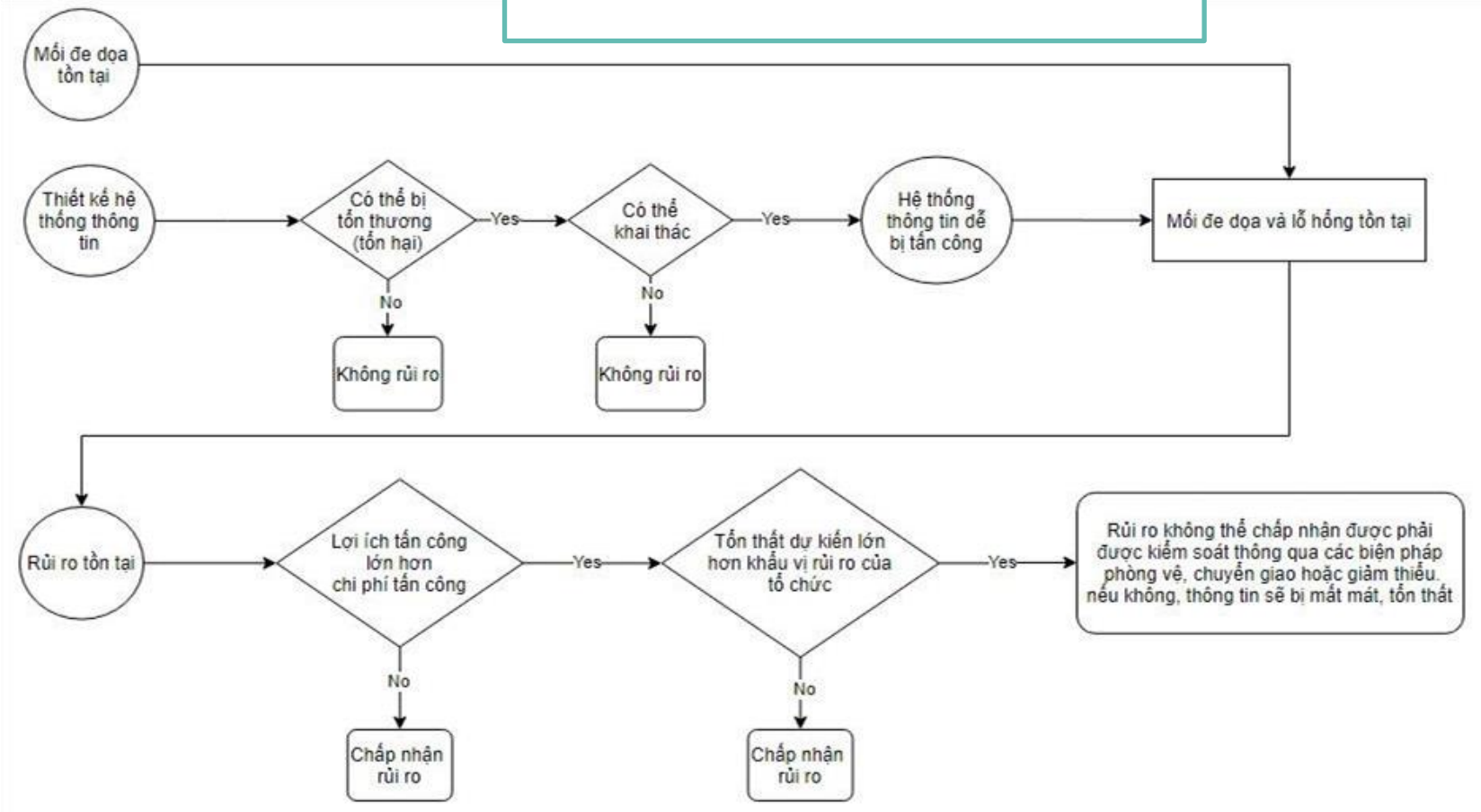
> *Là lượng rủi ro còn sót lại sau khi đã được tăng cường về chính sách bảo mật, giáo dục và đào tạo, đã kiểm soát được về mặt kỹ thuật và được bảo vệ.*

3. Kiểm soát rủi ro

> *Mục tiêu của InfoSec không phải là giảm thiểu lượng rủi ro tồn đọng về 0; thực ra, mục tiêu thực sự là đưa những rủi ro đó trở thành những khẩu vị rủi ro của các doanh nghiệp.*

Kiểm soát rủi ro

Sơ đồ minh họa quá trình của một tổ chức lựa chọn trong số các chiến lược kiểm soát rủi ro



Một số nguyên tắc khi lựa chọn một biện pháp

Khi điểm yếu tồn tại trong một tài sản quan trọng

Tăng cường an ninh để giảm thiểu khả năng điểm yếu bị khai thác

Khi điểm yếu có thể bị khai thác

Áp dụng các lớp bảo vệ, thiết kế kiến trúc hệ thống và quyền kiểm soát của admin để giảm thiểu tối đa rủi ro hoặc ngăn ngừa sự tấn công

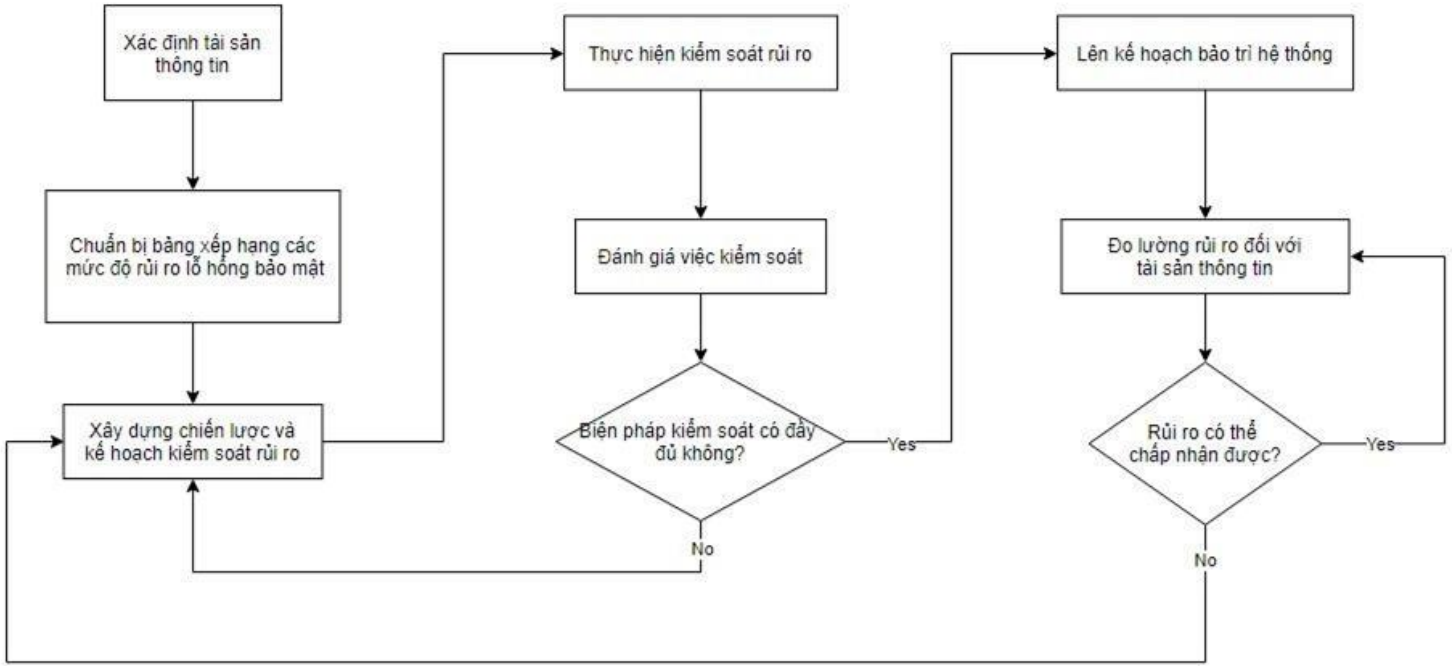
Khi tiềm năng những kẻ tấn công thu được lớn hơn những gì mà chúng bỏ ra

Áp dụng bảo vệ để tang giá trị của cuộc tấn công lên hay hạn chế những gì mà kẻ tấn công thu được bằng kỹ thuật hay quản lý điều khiển

Khi lượng mất mát đáng kể

Áp dụng các nguyên tắc thiết kế, thiết kế kiến trúc, kỹ thuật bảo vệ để hạn chế mức độ của tấn công, từ đó giảm thiểu mất mát

2. Quản lý rủi ro



Sơ đồ minh họa quá trình của một tổ chức lựa chọn trong số các chiến lược kiểm soát rủi ro

3. Phân tích tính khả thi và chi phí-lợi ích

Trước khi quyết định chiến lược cho một tổ hợp tài sản - lỗ hổng bảo mật - mối đe dọa, tổ chức phải nhận thức được ưu-nhược điểm của chiến lược, nhược điểm có thể gây hậu quả kinh tế và phi kinh tế của việc khai thác lỗ hổng bảo mật khi mối đe dọa gây ra tổn thất về tài sản.

Có rất nhiều cách để xác định ưu điểm của một chiến lược cụ thể, nhưng cách chính là xác định giá trị tài sản thông tin mà nó được thiết kế để bảo vệ.

(*Trong các kĩ thuật sau, một vài kĩ thuật sử dụng các chi phí tính bằng đô la và tiết kiệm từ việc tránh chi phí kinh tế (bằng cách sử dụng chiến lược phòng vệ thông qua việc thực hiện kiểm soát, do đó loại bỏ các phân nhánh tài chính của một sự cố), trong khi các kỹ thuật khác sử dụng các tiêu chí không khả thi về mặt kinh tế.)*

3.1 Phân tích chi phí-lợi ích

Tiêu chí thường được sử dụng nhất là tính khả thi về kinh tế. Quá trình ra quyết định này được gọi là phân tích chi phí - lợi ích (The Cost-Benefit Analysis: CBA) hoặc nghiên cứu khả thi kinh tế.

- **Chi phí:** Cũng như khó xác định giá trị của thông tin, cũng khó xác định chi phí bảo vệ thông tin đó. Các hạng mục ảnh hưởng đến chi phí của việc kiểm soát hoặc biện pháp bảo vệ là:

- **Chi phí phát triển hoặc mua lại** (phần cứng, phần mềm và dịch vụ)
- **Phí đào tạo** (chi phí đào tạo nhân viên)
- **Chi phí thực hiện** (cài đặt, cấu hình và thử nghiệm phần cứng, phần mềm và dịch vụ)
- **Chi phí dịch vụ** (phí bảo trì và nâng cấp của nhà cung cấp)
- **Chi phí bảo trì** (chi phí nhân công để xác minh và liên tục kiểm tra, bảo trì, đào tạo và cập nhật)

- **Lợi ích:** Lợi ích là giá trị đối với tổ chức sử dụng các biện pháp kiểm soát để ngăn ngừa tổn thất liên quan đến một lỗ hổng cụ thể. Kết quả này được biểu thị bằng dự báo tổn thất hàng năm **(ALE).**

3.1 Phân tích chi phí-lợi ích

- **Định giá tài sản:** Định giá tài sản là quá trình ấn định giá trị tài chính hoặc giá trị cho mỗi tài sản thông tin. Giá trị của thông tin khác nhau trong các tổ chức và giữa các tổ chức. Hầu như không thể xác định chính xác giá trị thực của thông tin và tài sản mang thông tin, đó có lẽ là một lý do tại sao các công ty bảo hiểm hiện nay không có bảng định giá chính xác cho tài sản thông tin.

Định giá tài sản là một quá trình phức tạp, các tổ chức phải xác định chính xác cách định giá tài sản thông tin. Các phương pháp thường dùng:

- Giá trị được giữ lại từ chi phí tạo ra tài sản thông tin
- Giá trị được giữ lại từ quá trình bảo trì tài sản thông tin trong quá khứ
- Giá trị bao hàm bởi chi phí thay thế thông tin
- Giá trị từ việc cung cấp thông tin
- Giá trị thu được từ chi phí bảo vệ thông tin
- Giá trị đối với chủ sở hữu
- Giá trị của tài sản trí tuệ
- Giá trị đối với đối thủ
- Mất năng suất trong khi không có tài sản thông tin
- Mất doanh thu trong khi tài sản thông tin không có sẵn

3.2 Tính toán tổn thất tiềm năng từ việc khai thác lỗ hổng

Các tính toán này mang lại ước tính về tổn thất tiềm năng trên mỗi rủi ro.

- Thiệt hại nào có thể xảy ra, và ảnh hưởng tới vấn đề tài chính nào?
- Chi phí để phục hồi sau cuộc tấn công, ngoài tác động tài chính của thiệt hại?
- **Dự báo tổn thất đơn lẻ** cho mỗi rủi ro là bao nhiêu?

Dự báo tổn thất đơn lẻ (SLE) là giá trị được tính toán liên quan đến tổn thất có khả năng xảy ra cao nhất từ một lần xảy ra một cuộc tấn công cụ thể

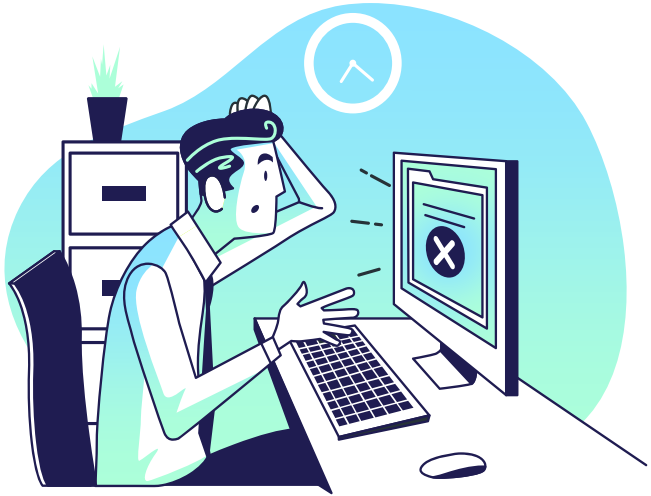
SLE = AV x EF

AV: asset value (Giá trị tài sản)

EF: exposure factor (Phần trăm tổn thất sẽ xảy ra từ một lỗ hổng nhất định bị khai thác)

Ước tính giá trị của thông tin đã khó, ước tính xác suất xuất hiện mối đe dọa hoặc tấn công còn khó hơn. Trong hầu hết các trường hợp, một tổ chức chỉ có thể dựa vào thông tin nội bộ của mình để tính toán mức độ an toàn của các tài sản thông tin của mình.

3.2 Tính toán tổn thất tiềm năng từ việc khai thác lỗ hổng



Xác suất xảy ra mối đe dọa được mô tả dưới dạng bảng cho biết tần suất một cuộc tấn công từ mỗi loại mối đe dọa có khả năng xảy ra trong một khung thời gian nhất, thường được gọi là **tỷ lệ xuất hiện hàng năm (annualized rate of occurrence: ARO)**. ARO chỉ đơn giản cho biết tần suất bạn mong đợi một loại tấn công cụ thể sẽ xảy ra.

Ta có thể tính toán khả năng tổn thất tổng thể trên mỗi rủi ro được biểu thị dưới **dạng dự báo tổn thất hàng năm (annualized loss expectancy: ALE)** bằng cách sử dụng các giá trị ARO và SLE:

ALE = SLE x ARO

VD: với SLE = 100.000 đô la, ARO = 0,5 thì ALE = 100.000 x 0,5 = 50.000 (đô la/năm)

3.2 Tính toán tổn thất tiềm năng từ việc khai thác lỗ hổng

Công thức Phân tích Chi phí-Lợi ích (The Cost-Benefit Analysis (CBA) Formula: CBA) được dùng để xác định lợi ích từ một biện pháp kiểm soát có xứng đáng với chi phí liên quan của việc thực hiện và duy trì kiểm soát hay không. Những phân tích có thể thực hiện trước hoặc sau khi thực hiện việc kiểm soát bảo vệ. Kỹ thuật CBA dễ thực hiện nhất là sử dụng **ALE, ACS** từ các đánh giá trước đó:

CBA = ALE (precontrol) - ALE (postcontrol) - ACS

Với

- **ALE (precontrol):** ALE của rủi ro trước khi thực hiện kiểm soát
- **ALE (postcontrol):** ALE được kiểm tra sau khi kiểm soát đã được thực hiện trong một khoảng thời gian
- **ACS (Annualized cost of a safeguard):** chi phí hàng năm của biện pháp tự vệ.

Một khi các biện pháp kiểm soát được thực hiện, điều quan trọng là phải kiểm tra các lợi ích của chúng liên tục để xác định khi nào chúng phải được nâng cấp, bổ sung hoặc thay thế

3.3 Các phương pháp xác định tính khả thi khác

Bước tiếp theo trong việc đo lường mức độ sẵn sàng của một tổ chức để đưa ra các biện pháp kiểm soát là xác định tính khả thi về tổ chức, hoạt động, kỹ thuật và chính trị của nó.

- Tính khả thi trong hoạt động
- Tính khả thi về kỹ thuật
- Tính khả thi về chính trị

Có nhiều cách phân bổ ngân sách trong các tổ chức khác nhau:

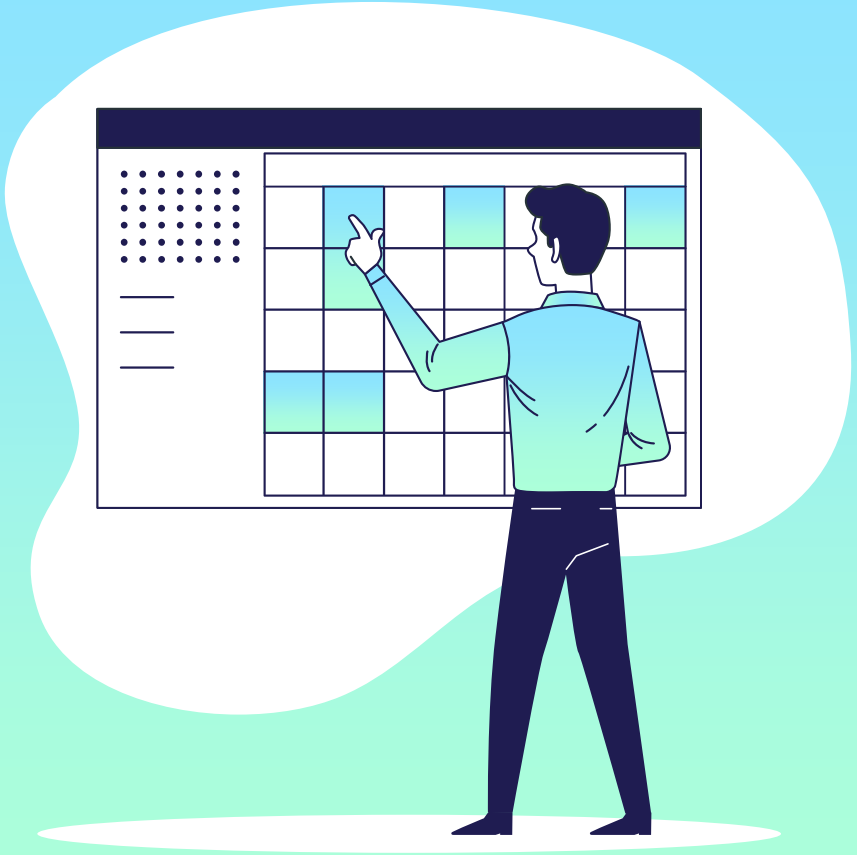
- Cộng đồng InfoSec được chỉ định ngân sách và sử dụng phán đoán riêng để chi tiêu số tiền, phân bổ về các dự án
- Tài nguyên trước tiên được phân bổ cho cộng đồng CNTT quan tâm và nhóm InfoSec phải cạnh tranh để giành được những tài nguyên này.
- Một phương pháp khác để phân bổ ngân sách yêu cầu nhóm InfoSec đề xuất và biện minh cho việc sử dụng các nguồn lực cho các hoạt động và dự án trong bối cảnh của toàn bộ tổ chức.

3.4 Các giải pháp thay thế cho phân tích tính khả thi

Thay vì sử dụng CBA hoặc một số tính toán khả thi khác để biện minh cho các biện pháp kiểm soát rủi ro, một tổ chức có thể tìm đến các mô hình thay thế. Các phương pháp nổi bật:

- **Đo điểm chuẩn** là quá trình tìm kiếm và nghiên cứu các phương pháp thực hành được sử dụng trong các tổ chức khác để tạo ra kết quả mà bạn mong muốn trong tổ chức của mình. Khi đo điểm chuẩn, một tổ chức thường sử dụng các biện pháp dựa trên số liệu hoặc dựa trên quy trình.
- **Sự quan tâm và thẩm định đúng mức xảy ra khi một tổ chức áp dụng một mức độ bảo mật tối thiểu nhất định** — nghĩa là, điều mà bất kỳ tổ chức thận trọng nào cũng sẽ làm trong những trường hợp tương tự.
- **Các phương pháp kinh doanh tốt nhất** được coi là những phương pháp tốt nhất trong ngành, cân bằng giữa nhu cầu tiếp cận thông tin với sự bảo vệ thích hợp.

4. Một số biện pháp kiểm soát rủi ro kiến nghị



4. Một số biện pháp kiểm soát rủi ro kiến nghị

1. **Các biện pháp đánh giá định tính và đánh giá kết hợp**
    a. Đánh giá định tính sử dụng các nhãn như cao, trung bình hoặc thấp.
    b. Đánh giá kết hợp sử dụng các thang đo như 0-10,0-20…
2. **Kỹ thuật Delphi:** Kỹ thuật đánh giá theo nhóm thay vì đánh giá cá nhân
3. **Các phương pháp OCTAVE:** Có ba phiên bản của phương pháp OCTAVE:
    a. OCTAVE là hệ thống nguyên thủy và là cơ sở cho các phiên bản khác trong hệ thống OCTAVE. Hướng tới cơ quan/tổ chức lớn với hơn 300 nhân viên có đủ nguồn lực và khả năng thực hiện các đánh giá an toàn nội bộ.
    b. OCTAVE-S hướng tới cơ quan/tổ chức cỡ nhỏ thường ít hơn 100 nhân viên và cần nhóm 3-5 người có hiểu biết để thực hiện việc đánh giá về tài sản, yêu cầu an toàn, các mối đe dọa, thực hành an toàn.
    c. OCTAVE-Allegro là phiên bản mới nhất hướng tới việc phổ biến rộng rãi việc đánh giá rủi ro an toàn thông tin.

4.3 Các phương pháp OCTAVE

Các bước tiến hành OCTAVE bao gồm:

1. Thiết lập tiêu chuẩn đánh giá rủi ro
2. Xây dựng hồ sơ tài sản thông tin
3. Xác định đối tượng chứa tài sản
4. Xác định lĩnh vực quan tâm
5. Xác định các tình huống đe dọa
6. Xác định rủi ro
7. Phân tích rủi ro
8. Lựa chọn các tiếp cận giảm thiểu

4.4 Phương pháp tiếp cận quản lý rủi ro của Microsoft

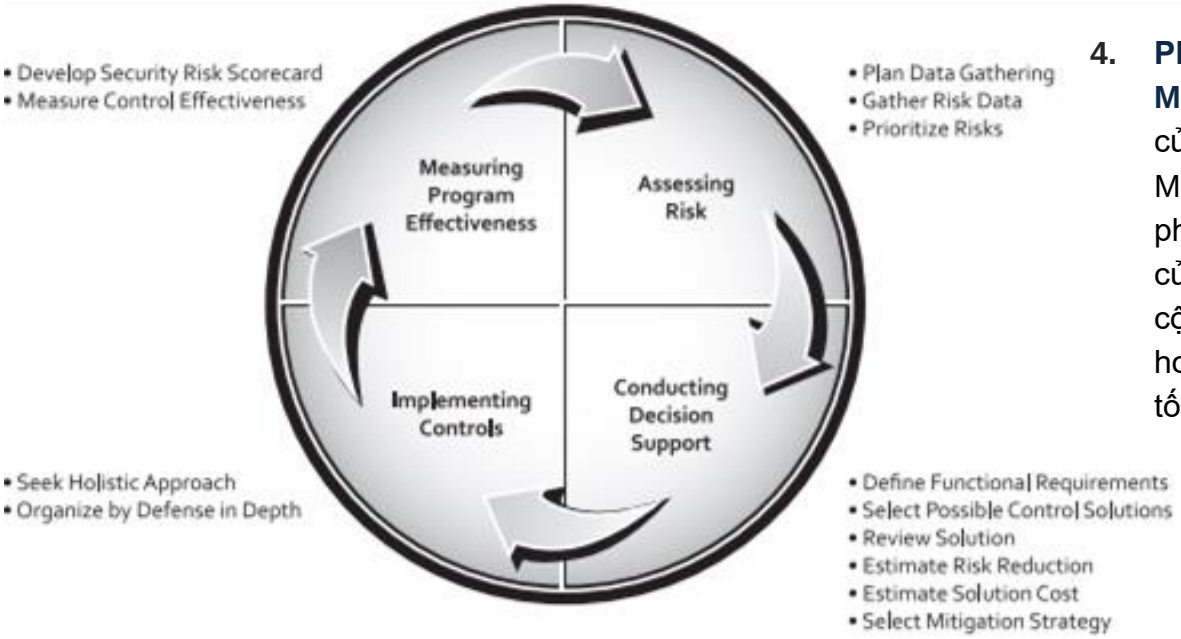


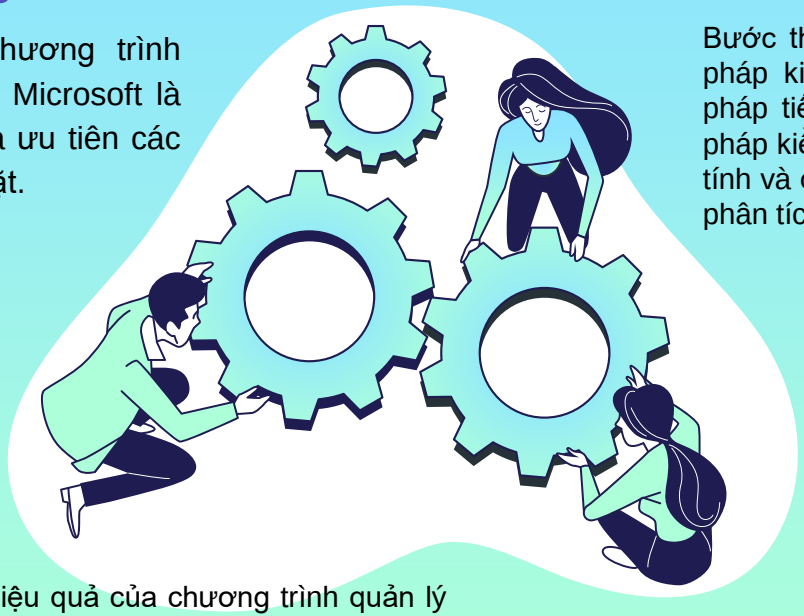
Figure A-1 Security risk management guide

4. **Phương pháp tiếp cận quản lý rủi ro của Microsoft:** Hướng dẫn cung cấp cách tiếp cận của công ty đối với quy trình quản lý rủi ro. Microsoft khẳng định rằng quản lý rủi ro không phải là một chủ đề độc lập và phải là một phần của chương trình quản trị chung để cho phép cộng đồng quản lý chung của tổ chức đánh giá hoạt động của tổ chức và đưa ra các quyết định tốt hơn, sáng suốt hơn:
    a. Đánh giá rủi ro
    b. Thực hiện hỗ trợ quyết định
    c. Thực hiện các biện pháp kiểm soát
    d. Đo lường hiệu quả của chương trình

4.4 Phương pháp tiếp cận quản lý rủi ro của Microsoft

4.4.1: Đánh giá rủi ro

Giai đoạn đầu tiên của chương trình Quản lý rủi ro bảo mật của Microsoft là đánh giá rủi ro - xác định và ưu tiên các rủi ro mà tổ chức phải đối mặt.



4.4.2: Thực hiện hỗ trợ quyết định

Bước thứ hai chỉ là xác định và đánh giá các biện pháp kiểm soát có sẵn cho tổ chức. Các phương pháp tiếp cận được sử dụng để đánh giá các biện pháp kiểm soát có thể bao gồm cả phương pháp định tính và định lượng đã thảo luận trước đó, bao gồm cả phân tích chi phí - lợi ích mà Microsoft nhấn mạnh

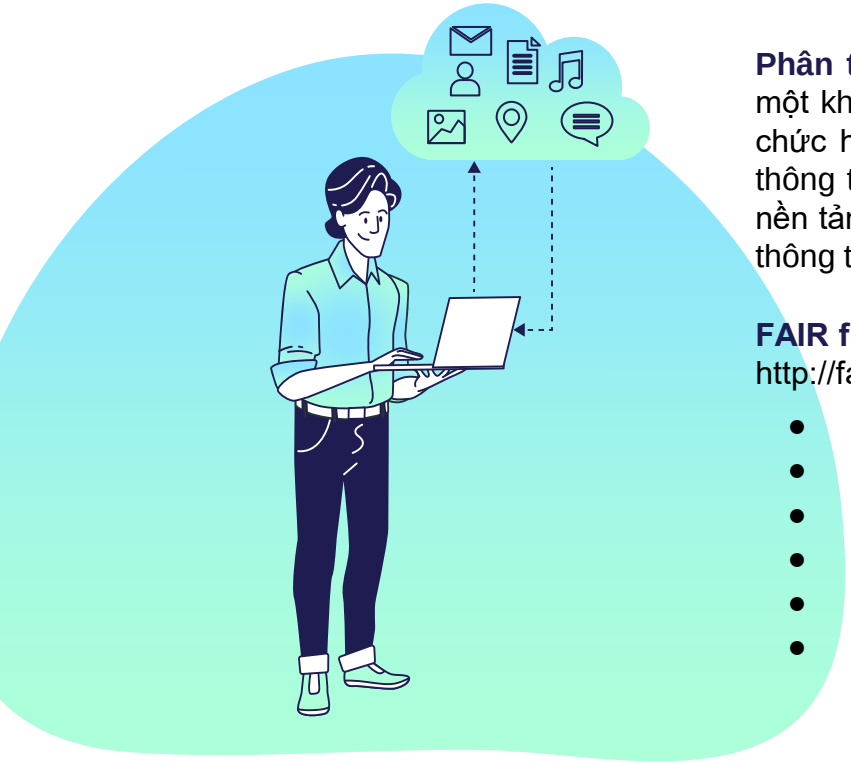
4.4.3: Thực hiện các biện pháp kiểm soát

Bước tiếp theo liên quan đến việc triển khai và vận hành các biện pháp kiểm soát được lựa chọn từ các phân tích lợi ích chi phí và các yếu tố giảm thiểu khác từ bước trước.

4.4.4: Đo lường hiệu quả của chương trình

Bước cuối là đánh giá liên tục hiệu quả của chương trình quản lý rủi ro. Khi các biện pháp kiểm soát được sử dụng, tổ chức và môi trường xung quanh thay đổi và phát triển, quá trình phải được giám sát chặt chẽ để đảm bảo các biện pháp kiểm soát tiếp tục cung cấp mức độ bảo vệ mong muốn.

4.5 Phân tích yếu tố rủi ro thông tin



Phân tích yếu tố rủi ro thông tin (Factor Analysis of Information Risk), một khuôn khổ quản lý rủi ro do Jack A. Jones phát triển, có thể giúp các tổ chức hiểu, phân tích và đo lường rủi ro thông tin. Kết quả là quản lý rủi ro thông tin hiệu quả hơn về mặt chi phí, uy tín hơn đối với nghề InfoSec và là nền tảng để từ đó phát triển phương pháp tiếp cận khoa học để quản lý rủi ro thông tin.

FAIR framework được mô tả trên trang
http://fairwiki.riskmanagementinsight.com bao gồm:

- Phân loại rủi ro thông tin
- Danh pháp tiêu chuẩn cho các thuật ngữ rủi ro thông tin
- Khuôn khổ để thiết lập tiêu chí thu thập dữ liệu
- Thang đo lường các yếu tố rủi ro
- Công cụ tính toán để tính toán rủi ro
- Cấu trúc mô hình để phân tích các tình huống rủi ro phức tạp

4.5 Phân tích yếu tố rủi ro thông tin

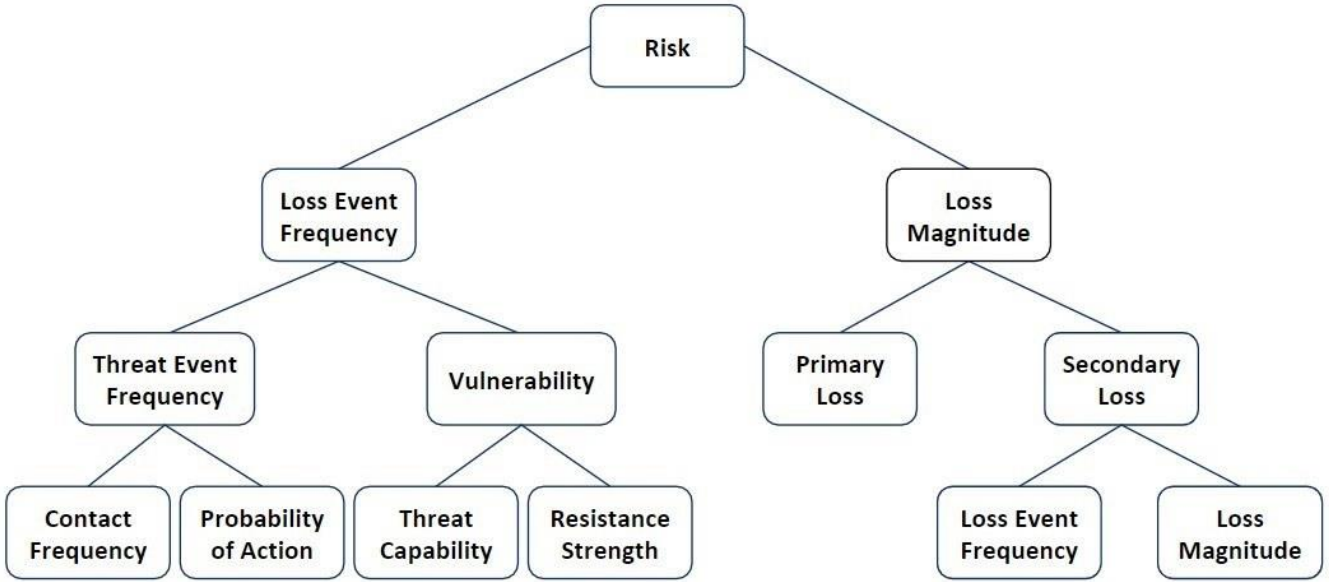
4 Giai đoạn của FAIR:

- **Giai đoạn 1 — Xác định các thành phần kịch bản**
  - Xác định tài sản có rủi ro.
  - Xác định cộng đồng mối đe dọa đang được xem xét.
- **Giai đoạn 2 — Đánh giá tần suất sự kiện mất mát**
  - Ước tính tần suất sự kiện đe dọa có thể xảy ra.
  - Ước tính khả năng đe doạ.
  - Ước tính sức mạnh kiểm soát.
  - Trích dẫn lỗ hổng bảo mật.
  - Trích dẫn sự kiện mất đĩa.
- **Giai đoạn 3 — Đánh giá mức độ tổn thất có thể xảy ra**
  - Ước tính tổn thất trong trường hợp xấu nhất.
  - Ước tính tổn thất có thể xảy ra.
- **Giai đoạn 4 - Phát triển và xác định rủi ro**
  - Trích dẫn và nêu rõ rủi ro.

4.5 Phân tích yếu tố rủi ro thông tin

Không giống như các khuôn khổ quản lý rủi ro khác, FAIR dựa trên đánh giá định tính của nhiều thành phần rủi ro, sử dụng các thang đo với các phạm vi giá trị — ví dụ, từ rất cao đến rất thấp.

Hình sau cho thấy cấu trúc cơ bản của phương pháp FAIR.



4.6 Tiêu chuẩn ISO 27005 về quản lý InfoSec

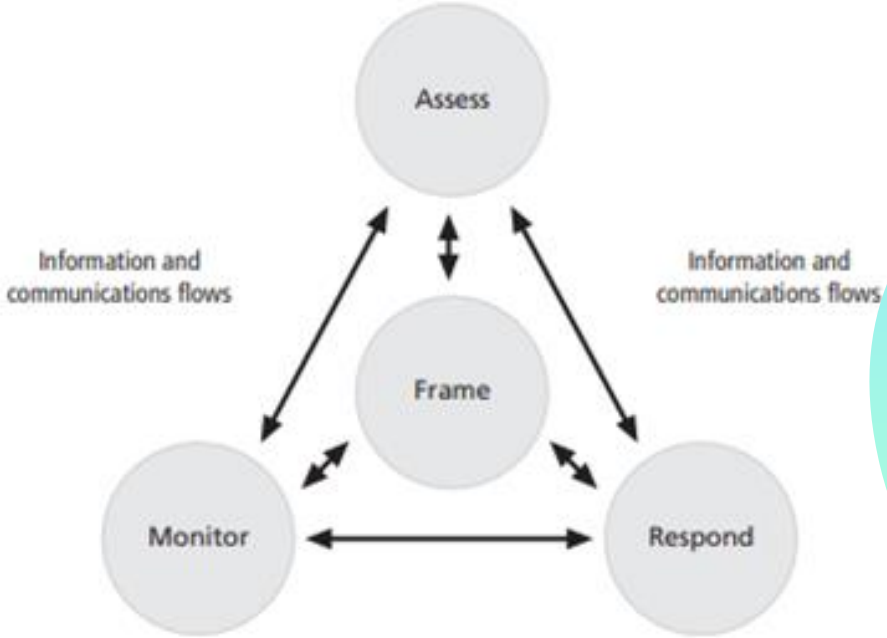
Đây là hệ thống kiểm soát do Tổ chức tiêu chuẩn quốc tế ISO đưa ra nhằm cung cấp các hướng dẫn về các quy trình quản lý rủi ro an toàn thông tin cần thiết cho việc triển khai hệ thống quản lý an toàn thông tin hiệu quả. Bao gồm 6 chủ đề chính

1. Xây dựng ngữ cảnh
2. Đánh giá rủi ro an toàn thông tin
3. Xử lý rủi ro an toàn thông tin
4. Chấp nhận rủi ro an toàn thông tin
5. Truyền thông về rủi ro an toàn thông tin
6. Xem xét lại và giám sát rủi ro an toàn thông tin

ISO 27005 có 3 bước xử lý việc đánh giá rủi ro bao gồm xác định, ước lượng và đánh giá rủi ro.

1. Xác định rủi ro
2. Ước lượng rủi ro
3. Đánh giá rủi ro

4.7 Mô hình quản lý rủi ro NIST



Vào năm 2009, chính phủ Hoa Kỳ thông qua NIST đã thay đổi cách tiếp cận cơ bản để xác nhận hệ thống thông tin liên bang và kiểm định (C&A), đưa chính phủ phù hợp với ngành công nghiệp.

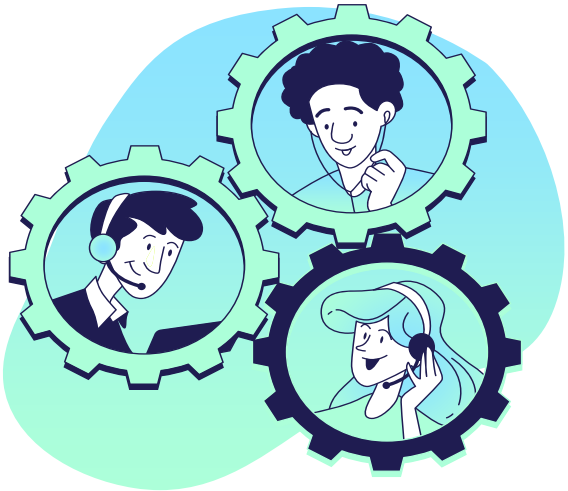
Trọng tâm chuyển từ các hoạt động C&A chính thức sang mô hình vòng đời quản lý rủi ro với việc xuất bản NIST SP 800-37 Rev. 1, “Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach”.

4.8 Các phương pháp khác

Một vài phương pháp được mô tả trong phần này không phải là tất cả. Trên thực tế, có hai tổ chức so sánh các phương pháp và đưa ra các khuyến nghị về các công cụ quản lý rủi ro mà công chúng có thể sử dụng:

- Cơ quan An ninh Mạng và Thông tin Châu Âu (ENISA) —Cơ quan này của Liên minh Châu Âu xếp hạng 12 công cụ sử dụng 22 thuộc tính khác nhau. Nó cũng cung cấp một tiện ích trên trang Web cho phép người dùng so sánh các phương pháp hoặc công cụ quản lý rủi ro (www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory).
- IsecT Ltd của New Zealand — Một công ty phi chính phủ tư vấn về Quản trị và Tuân thủ Rủi ro, IsecT duy trì trang web Bảo mật ISO 27001 tại http://iso27001security.com. Trang web này mô tả một số lượng lớn các phương pháp quản lý rủi ro (www.iso27001security.com/html/risk_mgmt.html).

III. Kết luận



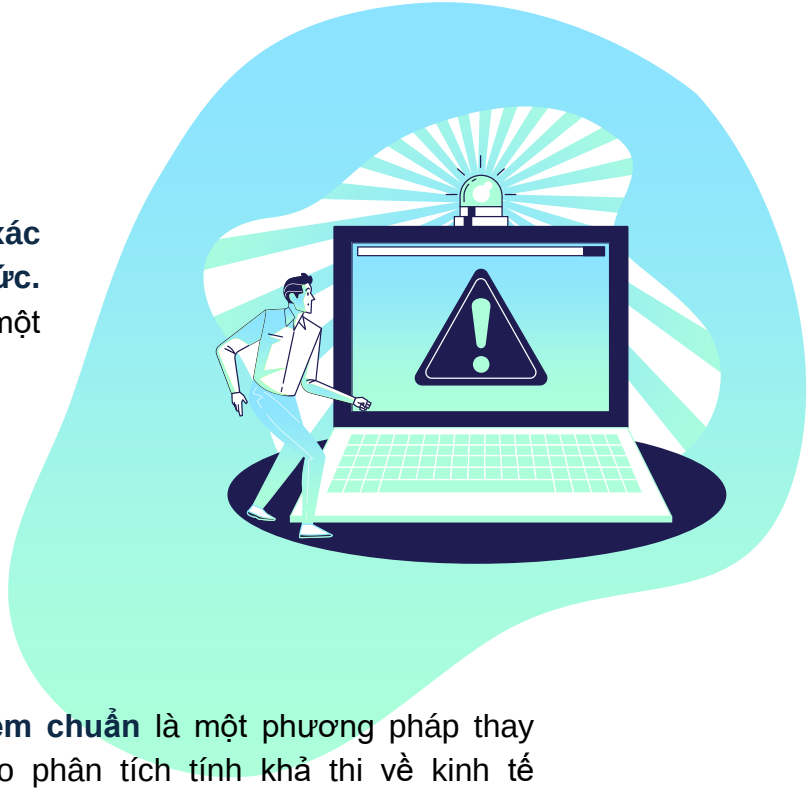
Vai trò của quản lý rủi ro trong tổ chức

- Giúp tổ chức hoạt động ổn định
- Giúp tổ chức thực hiện mục tiêu sứ mạng, chiến lược kinh doanh
- Giúp các nhà quản trị đưa ra các quyết định đúng đắn
- Giúp tăng vị thế, uy tín của doanh nghiệp và nhà quản trị
- Giúp tăng độ an toàn trong các hoạt động của tổ chức
- Giúp doanh nghiệp thực hiện thành công các hoạt động kinh doanh mạo hiểm

Khẩu vị rủi ro xác định số lượng và bản chất của rủi ro mà các tổ chức sẵn sàng chấp nhận khi họ đánh giá sự đánh đổi giữa bảo mật hoàn hảo và khả năng tiếp nhận rủi ro. Rủi ro còn lại là lượng rủi ro chưa được tính đến sau khi áp dụng các biện pháp kiểm soát.

Mục tiêu kiểm soát rủi ro là xác định và giảm thiểu các yếu tố rủi ro tiềm ẩn trong hoạt động của công ty, chẳng hạn như các khía cạnh kỹ thuật và phi kỹ thuật của hoạt động kinh doanh, chính sách tài chính và các vấn đề khác có thể ảnh hưởng đến phúc lợi của công ty.

III. Kết luận



Thành phần quan trọng của chiến lược quản lý rủi ro là xác định, phân loại, và ưu tiên các tài sản thông tin của tổ chức. Khi các lỗ hổng đã được xác định và sắp xếp mức độ nguy hại, một trong 5 chiến lược sau kiểm soát sau phải được lựa chọn:

- Phòng thủ
- Chuyển giao
- Giảm thiểu
- Chấp nhận
- Chấm dứt

Các nghiên cứu khả thi về kinh tế, xác định và so sánh chi phí và lợi ích từ các biện pháp kiểm soát. Các hình thức phân tích khả thi khác bao gồm phân tích dựa trên các yếu tố tổ chức, hoạt động, kỹ thuật và chính trị.

Đo điểm chuẩn là một phương pháp thay thế cho phân tích tính khả thi về kinh tế nhằm tìm ra và nghiên cứu các phương pháp thực tiễn được sử dụng trong các tổ chức khác để tạo ra kết quả mong muốn của chính tổ chức đó.

III. Kết luận

Dự báo tổn thất một lần (SLE) được tính toán từ giá trị tài sản thông tin và tỷ lệ phần trăm tổn thất dự kiến sẽ xảy ra từ cuộc tấn công thành công. Dự báo tổn thất hàng năm (ALE) đại diện cho tổn thất có thể xảy ra mỗi năm

Có thể lặp lại phân tích rủi ro bằng cách sử dụng các ước tính dựa trên đánh giá định tính. Kỹ thuật Delphi có thể được sử dụng để đạt được sự đồng thuận của nhóm về các giá trị đánh giá rủi ro.

Các phương pháp tiếp cận thay thế để quản lý rủi ro bao gồm phương pháp OCTAVE, phương pháp quản lý rủi ro của Microsoft, ISO 27005, phương pháp quản lý rủi ro NIST and FAIR.