BSI Vietnam

Hội thảo kỹ thuật

Tiếp cận Đánh giá và Xử lý Rủi ro hiệu quả theo hướng dẫn của Tiêu chuẩn ISO/IEC 27005:2022 trong quản lý rủi ro An toàn **Thông tin”**

Chương trình

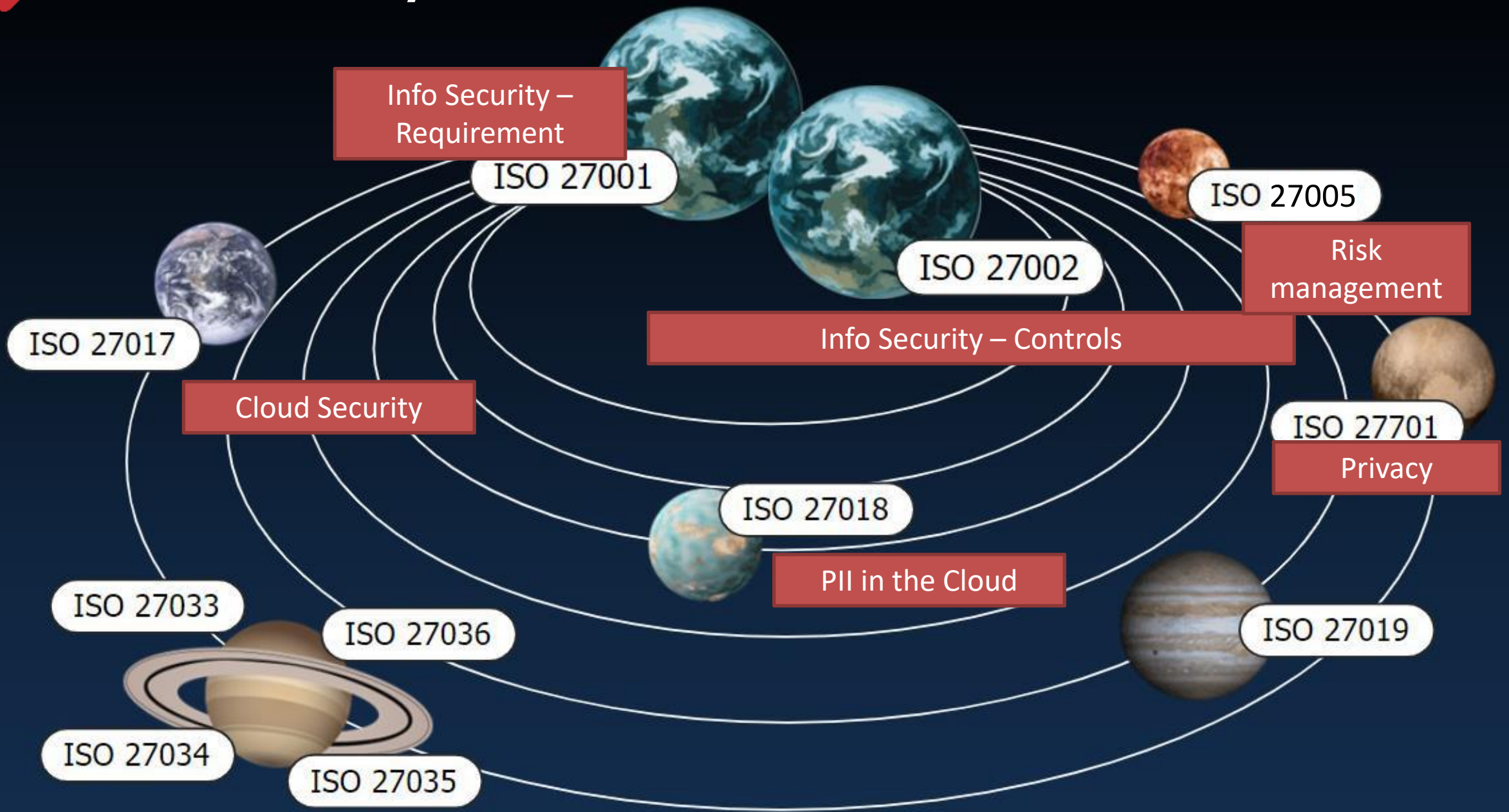
- Chào mừng và giới thiệu
- 1. Cấu trúc và cách tiếp cận ISO/IEC 27005:2022
- 2. Quản lý rủi ro an toàn thông tin
- 3. Thiết lập bối cảnh
- 4. Quá trình đánh giá rủi ro an toàn thông tin – Xác định rủi ro an toàn thông tin
- 5. Quá trình đánh giá rủi ro an toàn thông tin – Phân tích, Định lượng rủi ro an toàn thông tin
- 6. Quá trình xử lý rủi ro an toàn thông tin
- Câu hỏi & Trả lời

Hội thảo này sẽ giúp bạn:

- Xác định các lợi ích chính liên quan đến việc sử dụng ISO/IEC 27005:2022 để bảo vệ tài sản thông tin, nâng cao hiệu quả hệ thống quản lý an toàn thông tin (ISMS)
- Hiểu các phương pháp quản lý rủi ro tốt nhất có trong ISO/IEC 27005:2022
- Hiểu lý do cơ bản đằng sau các quá trình, cách sử dụng và triển khai chúng
- Thiết lập mức độ rủi ro có thể chấp nhận được đối với tài sản thông tin của bạn dựa trên kiến thức và hiểu biết về những rủi ro mà tổ chức của bạn gặp phải
- Phát triển các quá trình đánh giá nhiều rủi ro khác nhau liên quan đến tài sản thông tin của tổ chức bạn

1. Cấu trúc và cách tiếp cận ISO/IEC 27005:2022

ISO 27000 Family



Tiêu chuẩn ISO/IEC 27005:2022

Giới thiệu các khái niệm về kịch bản rủi ro

An toàn thông tin, an ninh mạng và bảo vệ quyền riêng tư - Hướng dẫn quản lý rủi ro an toàn thông tin

So sánh cách tiếp cận dựa trên sự kiện và dựa trên tài sản

Hỗ trợ các yêu cầu ISO 27001 liên quan đến các hành động nhằm giải quyết rủi ro an toàn thông tin

Phù hợp với ISO 27001:2022 và ISO 31000:2018

Thực hiện các hoạt động quản lý rủi ro an toàn thông tin

Lợi ích của ISO/IEC 27005:2022

Phương pháp thực hành tốt nhất có cấu trúc

Mang lại sự nhất quán và độ tin cậy

Lợi ích của ISO/IEC 27005:2022

- Hỗ trợ triển khai ISO/IEC 27001
- Phù hợp với ISO 31000
- Có thể được sử dụng như một quá trình quản lý rủi ro độc lập
- Có thể được sử dụng bởi bất kỳ tổ chức nào

Các điều khoản chính của ISO/IEC 27005:2022

- Điều 5: Quản lý rủi ro an toàn thông tin
- Điều 6: Thiết lập bối cảnh
- Điều 7: Quá trình đánh giá rủi ro an toàn thông tin
- Điều 8: Quá trình xử lý rủi ro an toàn thông tin
- Điều 9: Hoạt động
- Điều 10: Tận dụng các quá trình ISMS liên quan

Rủi ro là gì?

Rủi ro là 'tác động của sự không chắc chắn đến các mục tiêu'

Độ lệch so với dự kiến, có thể là tích cực và/hoặc tiêu cực

Mục tiêu có thể có những khía cạnh khác nhau

Thường đề cập đến các sự kiện và hậu quả tiềm ẩn

Sự kết hợp giữa hậu quả và khả năng xảy ra

Rủi ro là gì? - Ví dụ

Một sự kiện là tập hợp các tình huống có thể bị lợi dụng bởi một mối đe dọa

Để một cửa sổ mở có thể là một điểm yếu về an toàn

Sự kiện: Nếu ai đó lợi dụng điều này để vào tòa nhà bằng cửa sổ

Hậu quả: Là tình trạng được tạo ra bởi một sự kiện dẫn đến sự cố

Một sự cố là một sự kiện an toàn có hậu quả

Quản lý rủi ro là gì?

- Xác định, kiểm soát và loại bỏ các sự kiện không chắc chắn
- Các hoạt động phối hợp để chỉ đạo và kiểm soát
- Đạt được thông qua khuôn khổ hoặc chương trình
- Rủi ro và quá trình cần được xem xét thường xuyên

Thuật ngữ và định nghĩa chính

ISO 31000
ISO/IEC 27000
ISO/IEC Guide 73:2009

Thuật ngữ	Định nghĩa
Chủ sở hữu rủi ro Risk Owner	Người hoặc tổ chức có trách nhiệm và thẩm quyền quản lý rủi ro
Kịch bản rủi ro Risk scenario	Trình tự hoặc sự kết hợp của các sự kiện dẫn từ nguyên nhân ban đầu đến hậu quả không mong muốn
Khẩu vị rủi ro Risk appetite	Số lượng hoặc loại rủi ro mà tổ chức sẵn sàng theo đuổi hoặc duy trì
Rủi ro tồn dư Residual risk	Rủi ro còn lại sau khi xử lý rủi ro
Đánh giá rủi ro Risk assessment	Quá trình tổng thể về Xác định rủi ro, phân tích rủi ro và Định lượng rủi ro
Xác định rủi ro Risk identification	Quá trình tìm kiếm, nhận biết và mô tả rủi ro
Phân tích rủi ro Risk analysis	Quá trình để hiểu bản chất của rủi ro và xác định mức độ rủi ro
Xử lý rủi ro Risk treatment	Quá trình điều chỉnh rủi ro

2. Quản lý rủi ro an toàn thông tin

Chúng ta có ý gì khi nói 'an toàn thông tin'?

Bảo mật

Thuộc tính mà thông tin không được cung cấp hoặc tiết lộ cho các cá nhân, tổ chức hoặc quá trình trái phép

Toàn vẹn

Tài sản bảo vệ tính chính xác và đầy đủ của tài sản

Sẵn sàng

Thuộc tính có thể truy cập và sử dụng được theo yêu cầu của tổ chức được uỷ quyền

Chúng ta cần bảo vệ điều gì?

Tài sản chính:

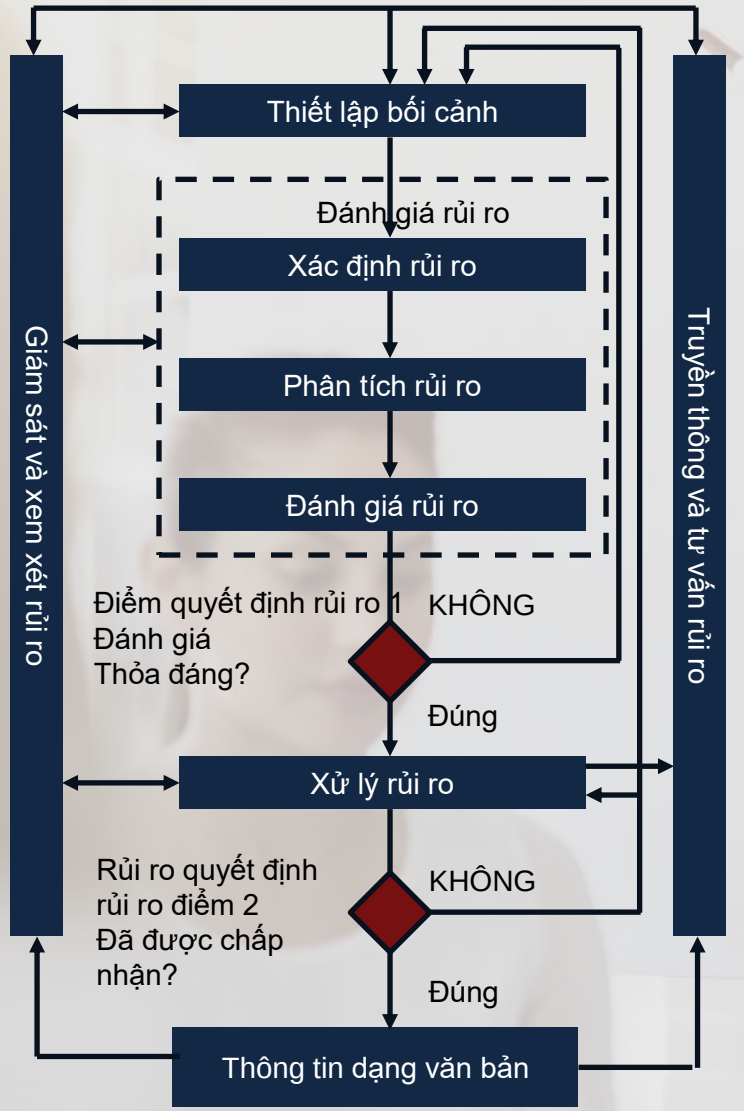
- Thông tin
- Quá trình và hoạt động kinh doanh

Tài sản hỗ trợ:

- Phần cứng
- Mạng
- Địa điểm
- Phần mềm
- Nhân viên

ISO/IEC 27005:2022 (A.2.2
Ví dụ về nhận dạng tài sản

Quản lý rủi ro ISO/IEC 27005:2022



Chu trình chiến lược và Chu trình hoạt động

Chu trình chiến lược

- Phát triển do những thay đổi trong bối cảnh tổ chức
- Đầu vào cho cập nhật đánh giá rủi ro tổng thể
- Cập nhật về xử lý rủi ro
- Có thể dùng làm đầu vào để xác định những rủi ro mới

- Tài sản kinh doanh
- Nguồn rủi ro
- Các mối đe dọa
- Các mục tiêu
- Hậu quả của các sự kiện

Chu trình hoạt động

- Dùng làm thông tin đầu vào hoặc thay đổi tiêu chí
- Đánh giá rủi ro bị ảnh hưởng bởi thông tin đó
- Các kịch bản rủi ro có thể cần được xem xét hoặc cập nhật
- Bao gồm xử lý rủi ro tương ứng

3. Thiết lập bối cảnh

Bối cảnh của tổ chức: Những cân nhắc chung

Tổ chức — Một người hoặc một nhóm người có chức năng riêng, có trách nhiệm, quyền hạn và các mối quan hệ để đạt được mục tiêu của mình

Bạn có ý gì khi nói đến tổ chức trong bối cảnh quản lý rủi ro an toàn thông tin?

Có thể là tập hợp con của một thực thể pháp lý trong bối cảnh ISMS

Xem xét quản lý rủi ro trong bối cảnh tổ chức của bạn

- Bên trong
- Bên ngoài

Bối cảnh bên ngoài

Các vấn đề có thể bao gồm các yếu tố hoặc điều kiện tích cực và tiêu cực

Bối cảnh bên ngoài có thể bao gồm: Pháp lý, công nghệ, thị trường, văn hóa, xã hội, v.v.

Bối cảnh bên ngoài (2)

Rủi ro, Tác động của rủi ro và Chấp nhận rủi ro

Định nghĩa phạm vi và ranh giới

Giám sát, soát xét và cải tiến quản lý rủi ro

Nhận dạng tài sản và Định giá tài sản

Xử lý rủi ro

Định lượng rủi ro

Bối cảnh bên trong

Bối cảnh bên trong có thể bao gồm: Giá trị, văn hóa, kiến thức, hiệu suất, v.v.

- Quá trình quản lý rủi ro
- Mục tiêu và tiêu chí
- Cam kết, uy tín, niềm tin và giá trị

Bối cảnh bên trong (2)

- Quản trị, cơ cấu tổ chức, vai trò và trách nhiệm giải trình
- Chính sách, mục tiêu và chiến lược
- Khả năng về nguồn lực và kiến thức
- Mối quan hệ, nhận thức và giá trị của các bên liên quan nội bộ
- Văn hóa tổ chức
- Hệ thống thông tin, luồng thông tin và quá trình ra quyết định
- Tiêu chuẩn, hướng dẫn và mô hình
- Hình thức và mức độ của quan hệ hợp đồng

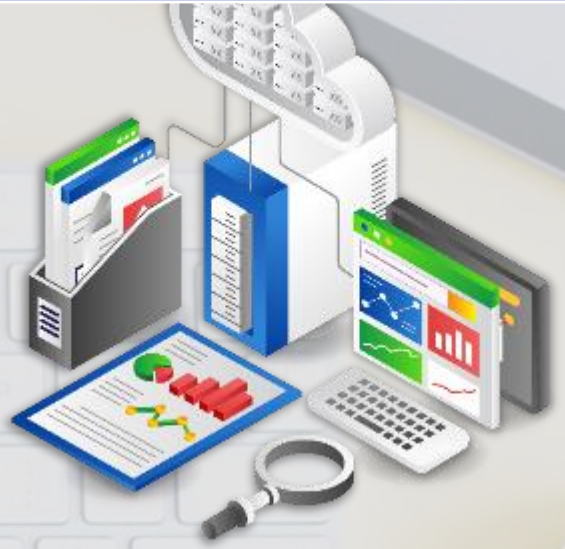
Bối cảnh của Tổ chức

Làm thế nào để một loại vấn đề nhất định ảnh hưởng đến mục tiêu an toàn thông tin?

Quản trị và cơ cấu tổ chức

Chính sách, mục tiêu và chiến lược

Hệ thống thông tin và luồng thông tin



Yêu cầu cơ bản của các bên quan tâm

Công dân

Khách hàng

Nhà phân phối

cổ đông

Nhà đầu tư

Những chủ sở hữu

Công ty bảo hiểm

Chính phủ

Nhà làm luật

Nhà cung cấp dịch vụ phục hồi

Tổ chức

Sự quản lý

- Quản lý hàng đầu
- Những người chịu trách nhiệm về chính sách và thực hiện an toàn thông tin

Những người thực hiện và duy trì ISMS

- Những người duy trì ISMS và các thủ tục rủi ro

Nhân viên khác

Nhà thầu

Đối thủ

Phương tiện truyền thông

Bình luận viên

Nhóm thương mại

Người hàng xóm

Các nhóm áp lực

Các dịch vụ khẩn cấp

Các cơ quan ứng phó khác

Dịch vụ vận tải

Người phụ thuộc của nhân viên

ISO/IEC 27001:2022 Clause 4.2

Tài liệu tham khảo liên quan

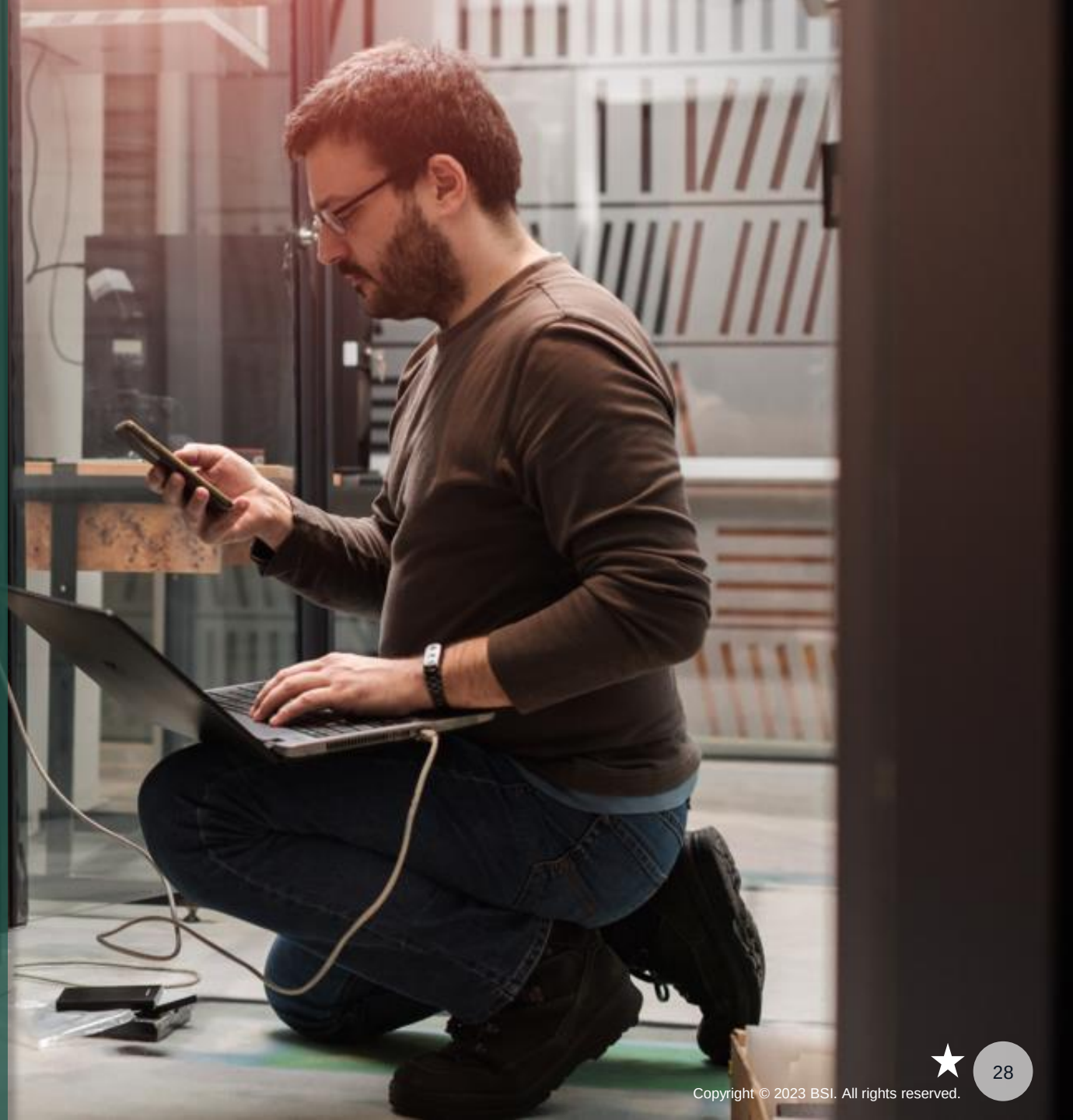
- ISO/IEC 27001:2022 Phụ lục A
- Quy tắc bảo mật và kiểm soát từ hợp đồng
- Tiêu chuẩn bổ sung
- Biện pháp Kiểm soát an toàn
- Tiêu chuẩn cụ thể của ngành
- Luật pháp quốc gia
- Quy định quốc tế/quốc gia

Áp dụng đánh giá rủi ro

Đánh giá rủi ro có thể được nhúng vào các quá trình khác nhau

Cần đề cập đến các vấn đề tổ chức liên quan đến ISMS

Hướng tới các rủi ro và biện pháp kiểm soát nhằm nâng cao khả năng đạt được các mục tiêu của tổ chức



Tiêu chí rủi ro an toàn thông tin

ISO/IEC 27001:2022 yêu cầu các
+ tiêu chí chấp nhận rủi ro và
+ tiêu chí thực hiện đánh giá rủi ro

Loại và bản chất của sự không chắc chắn

Sự nhất quán trong việc sử dụng các phép đo

Năng lực tổ chức

Hậu quả và khả năng xảy ra

Mức độ rủi ro

Các yếu tố

Sự kết hợp và chuỗi của nhiều rủi ro

Định tính và định lượng

Các yếu tố cần xem xét về tiêu chí chấp nhận rủi ro

Nhất quán Consistency

Giữa an toàn thông tin và tiêu chí chấp nhận rủi ro của tổ chức

Sự uỷ quyền Delegation

Cấp quản lý có thẩm quyền ra quyết định

Lưu loát Fluidity

Có thể có nhiều ngưỡng, chấp nhận tuyệt đối hoặc có điều kiện, ngắn hạn và tương lai

Rủi ro khác nhau Differing classes of risk

Không tuân thủ, mất hợp đồng

Doanh thu và lợi nhuận Revenue and profit

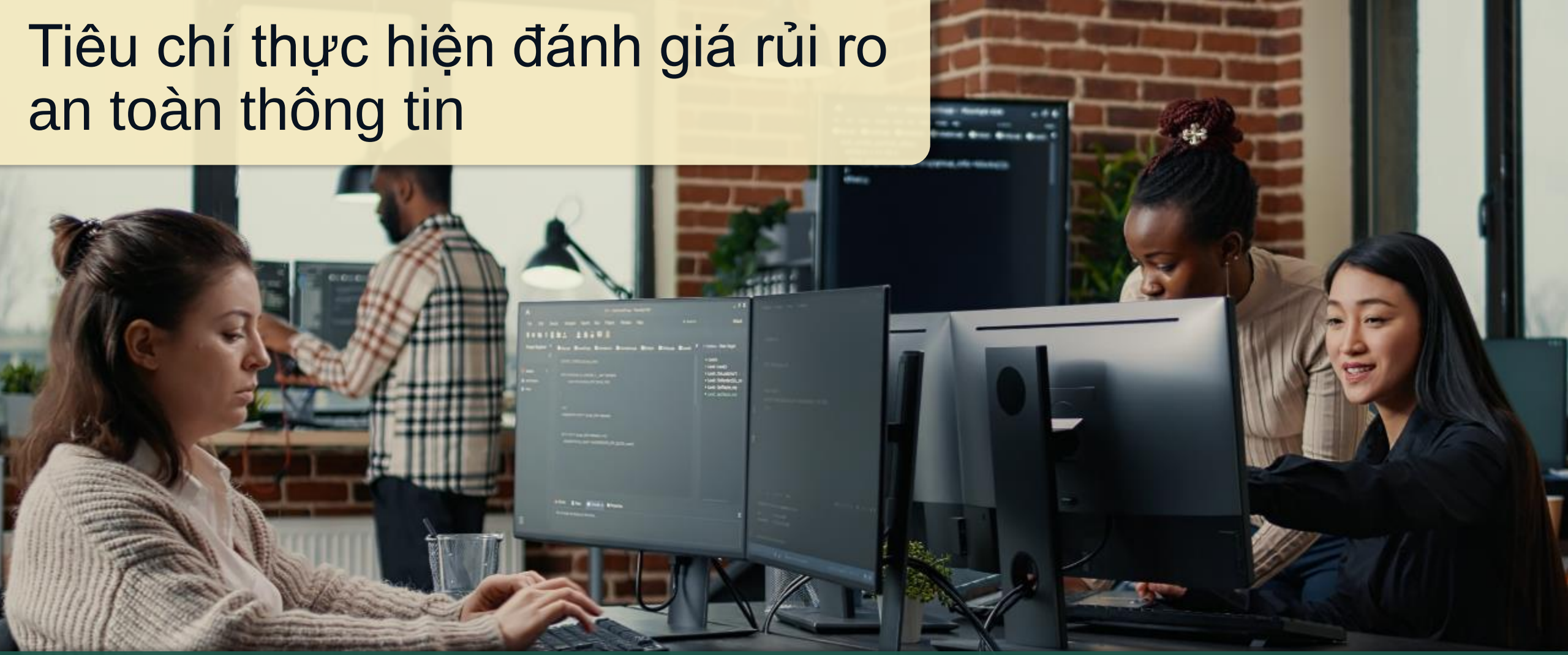
Sự chấp nhận dựa trên khẩu vị rủi ro của tổ chức

Khả năng và hậu quả Likelihood & consequence

Tự mình hay mở rộng để xem xét các yếu tố khác?

Các yếu tố ảnh hưởng đến tiêu chí chấp nhận rủi ro

Tiêu chí thực hiện đánh giá rủi ro an toàn thông tin



Hậu quả

Khả năng

Mức độ rủi ro

Tiêu chí đánh giá rủi ro phải được chuẩn hóa trong toàn tổ chức cho tất cả các loại đánh giá rủi ro, điều này có thể tạo thuận lợi cho việc trao đổi, so sánh và tổng hợp các rủi ro liên quan đến nhiều lĩnh vực kinh doanh

bsi.

Hậu quả

Bảo mật

Toàn vẹn

Sẵn sàng

Xem xét các tiêu chí hậu quả

Ví dụ

Ví dụ 1

Số tiền tối đa mà tổ chức có thể phỉ chi trả trong một năm tài chính và số tiền tối thiểu trong cùng kỳ sẽ buộc tổ chức phải chi trả

Ví dụ 2

Vi phạm dữ liệu

Mất tính bảo mật, tính toàn vẹn hoặc Tính sẵn sàng của thông tin

Không tuân thủ

Tiêu chí Khả năng

Thường biểu diễn dưới dạng xác suất

Sự kiện ngẫu nhiên hoặc tự nhiên

Mức độ phơi nhiễm thông tin hoặc tài sản liên quan đến thông tin trước mối đe dọa

Hành động hoặc thiếu sót của con người

Mức độ lỗ hổng của tổ chức bị khai thác

Thất bại về công nghệ

Xác định mức độ rủi ro

Mức độ vốn có so với mức độ rủi ro hiện tại

Cần thiết để đánh giá rủi ro được phân tích

Hỗ trợ chủ sở hữu rủi ro trong việc ra quyết định

Xác định mức độ rủi ro - Ví dụ

Giá trị bằng tiền của hậu quả hàng năm tính cho năm tiếp theo

Định tính

Định lượng

Các bên quan tâm

Phân tích rủi ro

Định lượng rủi ro

Hiệu chuẩn chính thức định kỳ theo thang đo tham chiếu để đảm bảo tính hợp lệ, tính nhất quán và khả năng so sánh của kết quả

Lựa chọn một phương pháp thích hợp

ISO/IEC 27001:2022 6.1.2 b

- Nhất quán
- Có thể so sánh
- Hiệu lực

4. Quá trình đánh giá rủi ro an toàn thông tin – Xác định rủi ro an toàn thông tin

Quá trình đánh giá rủi ro an toàn thông tin

Hỗ trợ ưu tiên xử lý rủi ro

Bối cảnh, phạm vi và mục đích của việc đánh giá rủi ro

Ba hoạt động chính

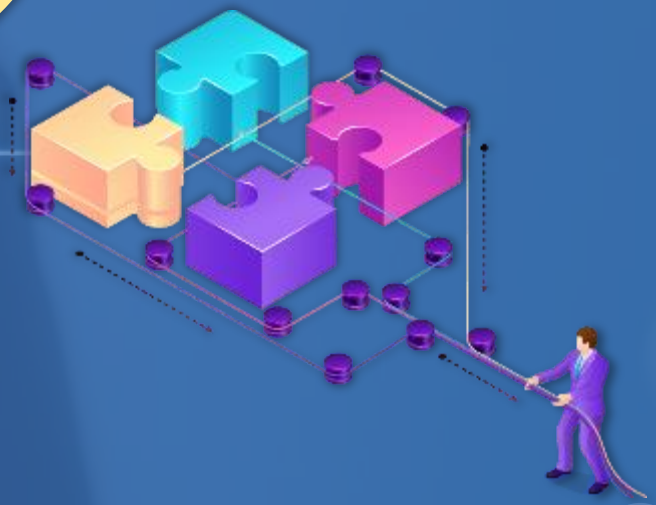
Xác định rủi ro
Risk identification

Phân tích rủi ro
Risk analysis

Định lượng rủi ro
Risk evaluation

Quá trình đánh giá rủi ro an toàn thông tin

Kết quả nhất quán, hợp lệ và có thể lặp lại



Nguồn rủi ro

Tội phạm có tổ chức

Khủng bố

Liên quan đến chính quyền

Các đơn vị chuyên môn

Nghiệp dư

Nhà hoạt động

Kẻ báo thù

Kẻ tấn công bệnh lý

Nhận biết và mô tả rủi ro an toàn thông tin

Tìm kiếm, nhận biết và mô tả rủi ro

Tạo danh sách rủi ro dựa trên việc đạt được các mục tiêu an toàn thông tin

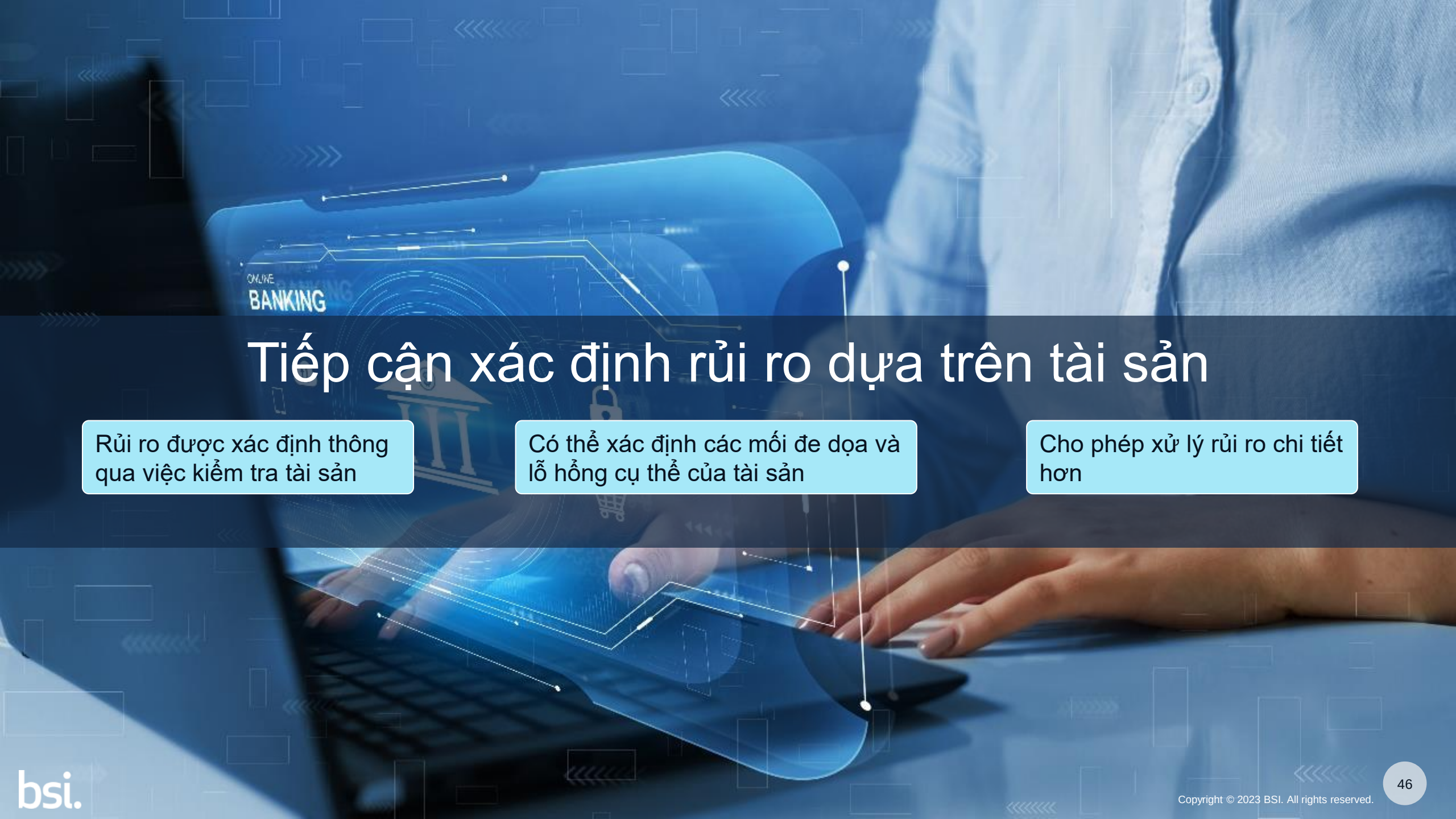
Hai cách tiếp cận phổ biến để xác định rủi ro

Dựa trên sự kiện
Event-based

Dựa trên tài sản
Asset-based

Tiếp cận xác định rủi ro dựa trên sự kiện

- ✓ Có thể liên kết với các vấn đề chiến lược và liên kết với bối cảnh cũng như các mối quan tâm của lãnh đạo cao nhất
- ✓ Kịch bản chiến lược không cần tài sản ở cấp độ chi tiết
- ✓ Có thể cho phép tập trung xử lý rủi ro vào các rủi ro quan trọng



Tiếp cận xác định rủi ro dựa trên tài sản

Rủi ro được xác định thông qua việc kiểm tra tài sản

Có thể xác định các mối đe dọa và lỗ hổng cụ thể của tài sản

Cho phép xử lý rủi ro chi tiết hơn

Chủ sở hữu rủi ro

Lãnh đạo cao nhất

Ban ATTT

Chủ thể quá trình

Chủ thể chức năng

Trưởng bộ phận

Chủ tài sản

5. Quá trình đánh giá rủi ro an toàn thông tin – Phân tích, Định lượng rủi ro an toàn thông tin

Phân tích rủi ro an toàn thông tin

- Chi tiết cao
- Chi tiết TB
- Chi tiết thấp

Rủi ro?

Mục đích phân tích?

Dữ liệu sẵn có?

Thông tin sẵn có?

Nguồn lực sẵn có?

Đánh giá hậu quả tiềm ẩn

Yêu cầu danh sách các sự kiện hoặc kịch bản rủi ro có liên quan đã được xác định

Hậu quả do không bảo đảm đầy đủ tính bảo mật, tính toàn vẹn hoặc Tính sẵn sàng của thông tin cần được xác định và đánh giá.

Cung cấp danh sách các hậu quả tiềm ẩn liên quan đến các kịch bản rủi ro, tài sản hoặc sự kiện

Đánh giá hậu quả tiềm ẩn

Ước tính tổn thất

Ước tính/nhận thức về mức độ nghiêm trọng của hậu quả

Chi phí khôi phục tùy thuộc vào việc việc khôi phục có thể được thực hiện nội bộ hay không

Đánh giá khả năng xảy ra

Các sự kiện hoặc kịch bản rủi ro liên quan và các nguồn lực hiện có

Đánh giá khả năng xảy ra các tình huống có thể xảy ra hoặc thực tế

Xác định thời điểm cần hoàn thành việc đánh giá

Cung cấp danh sách các sự kiện hoặc kịch bản rủi ro được bổ sung theo khả năng xảy ra

Xác định mức độ rủi ro

Kịch bản rủi ro với hậu quả và khả năng xảy ra

Mức độ rủi ro được xác định là sự kết hợp giữa khả năng xảy ra và hậu quả được đánh giá đối với các kịch bản rủi ro liên quan

Mức độ rủi ro quan trọng là rủi ro cần được đánh giá

Cung cấp danh sách rủi ro với các giá trị cấp độ được chỉ định

Định lượng rủi ro an toàn thông tin

Danh sách tiêu chí rủi ro
với mức độ rủi ro được chỉ định

So sánh kết quả phân tích rủi
ro với các tiêu chí rủi ro

Tổ chức nên áp dụng tiêu chí chấp nhận rủi ro của mình để xác định liệu rủi ro có thể được chấp nhận hay không.

Định lượng rủi ro an toàn thông tin

Mức độ rủi ro cần được so sánh với các tiêu chí đánh giá rủi ro, đặc biệt là các tiêu chí chấp nhận rủi ro

quá trình cần thiết để ưu tiên xử lý rủi ro an toàn thông tin

Bất kỳ sự khác biệt nào giữa mức độ rủi ro được đánh giá và mức độ mà chủ sở hữu rủi ro nhận thấy được đều cần được điều tra.

Ưu tiên các rủi ro được phân tích để xử lý rủi ro

Các rủi ro được ưu tiên nên xem xét các mục tiêu của tổ chức, hợp đồng,
các yêu cầu pháp lý và quy định cũng như quan điểm của các bên quan tâm có liên quan

6. Quá trình xử lý rủi ro an toàn thông tin

Xử lý rủi ro an toàn thông tin

Các lựa chọn xử lý rủi ro

- Tránh rủi ro avoidance
- Sửa đổi rủi ro modification
- Duy trì rủi ro retention
- Chia sẻ rủi ro sharing
- thông tin Dạng văn bản

Các phương án xử lý rủi ro được lựa chọn dựa trên kết quả đánh giá rủi ro và chi phí so với lợi ích của việc thực hiện

Xác định các biện pháp kiểm soát để xử lý rủi ro an toàn thông tin

Kiểm tra từng biện pháp kiểm soát cần thiết:

- Có nhiều tập hợp biện pháp kiểm soát để lựa chọn
- Các biện pháp kiểm soát tùy chỉnh có thể được yêu cầu

Giải quyết các rủi ro

Cân bằng giữa chi phí và hậu quả

Nếu biện pháp kiểm soát hoạt động trong phạm vi dung sai cho phép thì không cần cải tiến thêm

So sánh với các biện pháp kiểm soát của Phụ lục A và Tuyên bố về khả năng áp dụng

ISO/IEC 27001:2022, Điều 6.1.3 c)

Kiểm tra an toàn nhằm xác định mọi biện pháp kiểm soát cần thiết còn thiếu từ bất kỳ nguồn nào bằng cách so sánh các biện pháp kiểm soát với các tiêu chuẩn và danh sách kiểm soát khác

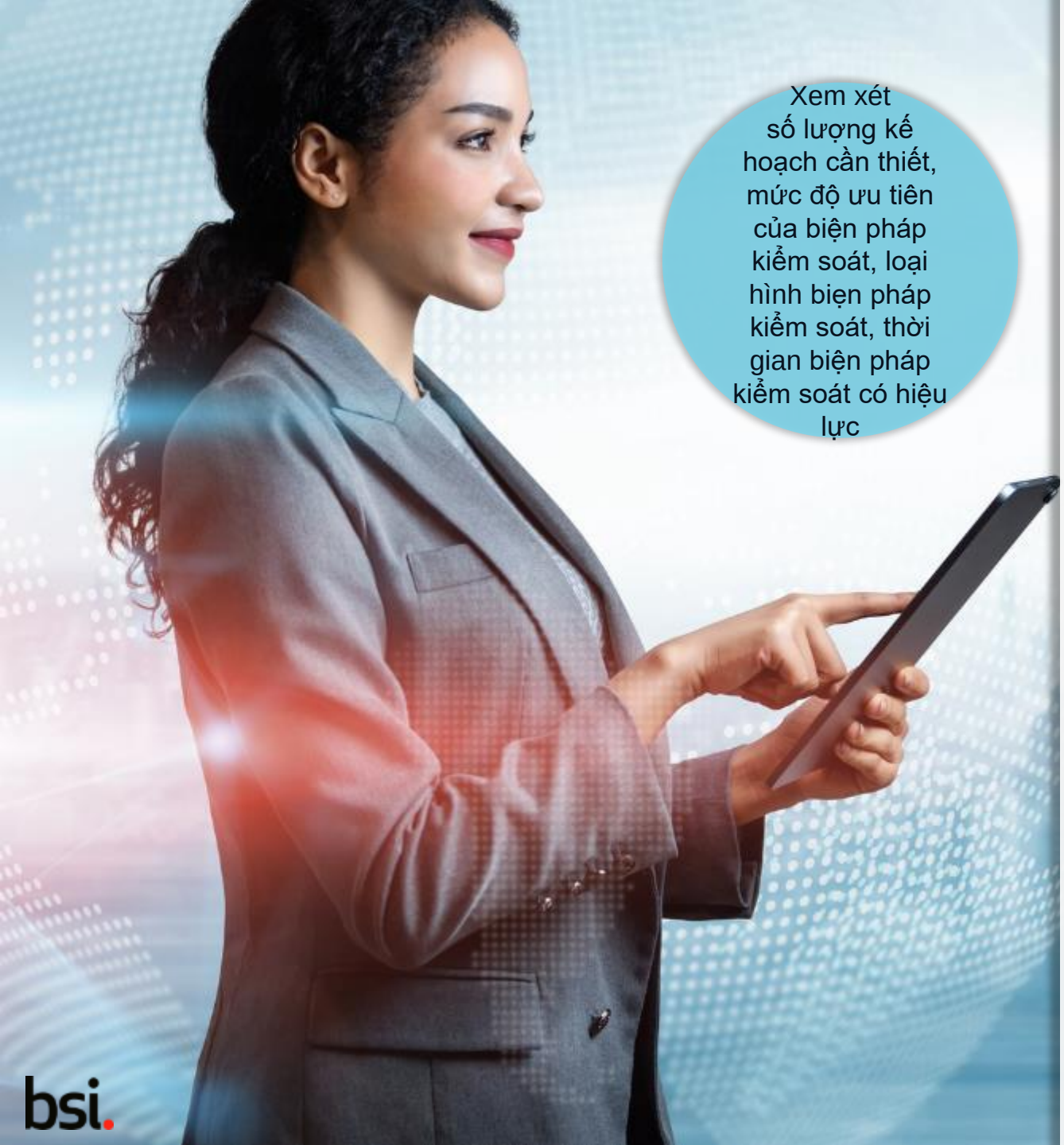
Tuyên bố về khả năng áp dụng

Kế hoạch xử lý rủi ro an toàn thông tin

- Kế hoạch xử lý rủi ro
  - Kế hoạch dự án
    - Hết giá trị sau khi thực hiện
  - Kế hoạch thiết kế
    - Mô tả cách các biện pháp kiểm soát tương tác với môi trường và với nhau

Nội dung của kế hoạch xử lý rủi ro và các vấn đề cần cân nhắc

- Các ưu tiên liên quan đến mức độ rủi ro và tính cấp bách của việc xử lý
- Liệu các loại biện pháp kiểm soát khác nhau hoặc thành phần của chúng có được áp dụng hay không
- Liệu có cần thiết phải đợi giải pháp kiểm soát trước khi bắt đầu triển khai một biện pháp kiểm soát mới trên cùng một nội dung hay không
- Liệu có sự chậm trễ giữa thời điểm biện pháp kiểm soát được thực hiện và thời điểm biện pháp kiểm soát đó có hiệu lực và đi vào hoạt động đầy đủ hay không



Nội dung của kế hoạch xử lý rủi ro và các vấn đề cần cân nhắc

Phê duyệt của chủ sở hữu rủi ro và chấp nhận các rủi ro an toàn thông tin còn lại (tồn dư)

Kế hoạch xử lý rủi ro và chấp nhận rủi ro tồn dư cần được hiểu và phê duyệt

Kế hoạch xử lý rủi ro được đưa vào đánh giá rủi ro tiếp theo

Phê duyệt của chủ sở hữu rủi ro và chấp nhận các rủi ro an toàn thông tin còn lại (tồn dư)

Có thể mất một thời gian để thực hiện kế hoạch xử lý các rủi ro đã đánh giá

Các quyết định chấp nhận rủi ro có thể tính đến các khung thời gian trong kế hoạch xử lý rủi ro

Một số rủi ro có thể thay đổi theo thời gian

- Cảm ơn sự tham gia của Quí vị

Câu hỏi & Trả lời