**TCVN** TIÊU CHUẨN QUỐC GIA

# TCVN 10295: 2014

# ISO/IEC 27005:2011

Xuất bản lần 1

# CÔNG NGHỆ THÔNG TIN – CÁC KỸ THUẬT AN TOÀN – QUẢN LÝ RỦI RO AN TOÀN THÔNG TIN

***Information technology – Security techniques – Information security risk management***

HÀ NỘI – 2014

**Mục lục**

## Lời nói đầu

TCVN 10295:2014 hoàn toàn tương đương với ISO/IEC 27005:2011.

TCVN 10295:2014 do Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam biên soạn, Bộ Thông tin và Truyền thông đề nghị, Tổng cục Tiêu chuẩn Đo lường Chất lượng thẩm định, Bộ Khoa học và Công nghệ công bố.

# Công nghệ thông tin - Các kỹ thuật an toàn - Quản lý rủi ro an toàn thông tin

*Information technology - Security techniques - Information security risk management*

## 1 Phạm vi áp dụng

Tiêu chuẩn này đưa ra các hướng dẫn về quản lý rủi ro an toàn thông tin.

Tiêu chuẩn này giải thích một số khái niệm cơ bản được sử dụng trong TCVN ISO/IEC 27001:2009 và được xây dựng để hỗ trợ cho việc triển khai an toàn thông tin dựa trên phương pháp tiếp cận quản lý rủi ro.

Để có thể hiểu đầy đủ hơn về nội dung tiêu chuẩn này cần tham khảo thêm các kiến thức về các khái niệm, mô hình, quy trình và các thuật ngữ được trình bày trong TCVN ISO/IEC 27001:2009 và TCVN ISO/IEC 27002:2011.

Tiêu chuẩn này có thể áp dụng cho nhiều loại hình tổ chức (như các doanh nghiệp thương mại, các cơ quan chính phủ, các tổ chức phi lợi nhuận) nhằm mục đích quản lý những rủi ro có thể gây hại tới an toàn thông tin của tổ chức.

## 2 Tài liệu viện dẫn

Các tài liệu viện dẫn sau đây là cần thiết để áp dụng tiêu chuẩn này. Đối với các tài liệu viện dẫn ghi năm công bố thì áp dụng bản được nêu. Đối với các tài liệu viện dẫn không ghi năm công bố thì áp dụng phiên bản mới nhất, bao gồm cả các sửa đổi, bổ sung (nếu có).

ISO/IEC 27000, Information technology – Security techniques – Information security management systems – Overview and vocabulary *(Công nghệ thông tin – Các kỹ thuật an toàn – Hệ thống quản lý an toàn thông tin – Tổng quan và từ vựng)*

TCVN ISO/IEC 27001:2009 Công nghệ thông tin – Các kỹ thuật an toàn – Hệ thống quản lý an toàn thông tin – Các yêu cầu

## 3 Thuật ngữ và định nghĩa

Tiêu chuẩn này áp dụng các thuật ngữ và định nghĩa trong tiêu chuẩn ISO/IEC 27000 và các thuật ngữ và định nghĩa dưới đây.

CHÚ THÍCH: Sự khác nhau trong các thuật ngữ và định nghĩa giữa tiêu chuẩn ISO/IEC 27005:2008 và tiêu chuẩn này được nêu ở Phụ lục G.

3.1

**Hậu quả** (consequence)

Kết quả của một **sự kiện** (3.3) gây ảnh hưởng đến các mục tiêu của tổ chức

[TCVN 9788:2013]

CHÚ THÍCH 1: Một sự kiện có thể dẫn đến một loạt các hậu quả.

CHÚ THÍCH 2: Một hậu quả có thể chắc chắn hoặc không chắc chắn xảy ra và trong bối cảnh an toàn thông tin thì thường mang nghĩa tiêu cực.

CHÚ THÍCH 3: Hậu quả có thể được thể hiện dưới dạng định tính hoặc định lượng.

CHÚ THÍCH 4: Hậu quả ban đầu có thể gây ảnh hưởng leo thang đến các hậu quả tiếp theo.

3.2

**Biện pháp kiểm soát** (control)

Biện pháp sẽ làm thay đổi **rủi ro** (3.9)

[TCVN 9788:2013]

CHÚ THÍCH 1: Biện pháp kiểm soát an toàn thông tin bao gồm bất kỳ quy trình, chính sách, thủ tục, hướng dẫn, phương pháp hoặc cấu trúc tổ chức trong các lĩnh vực hành chính, kỹ thuật, pháp lý hoặc quy định để thay đổi rủi ro an toàn thông tin.

CHÚ THÍCH 2: Biện pháp kiểm soát thay đổi rủi ro không phải lúc nào cũng phát huy tác dụng như mong đợi hoặc như giả định.

CHÚ THÍCH 3: Biện pháp kiểm soát cũng được sử dụng với nghĩa là biện pháp bảo vệ hoặc biện pháp đối phó.

3.3

**Sự kiện** (event)

Sự xuất hiện hoặc sự thay đổi của một tập hợp các tình huống cụ thể

[TCVN 9788:2013]

CHÚ THÍCH 1: Một sự kiện có thể xảy ra một hay nhiều lần và có thể do nhiều nguyên nhân.

CHÚ THÍCH 2: Một sự kiện có thể bao gồm cả những sự việc không xảy ra.

CHÚ THÍCH 3: Một sự kiện đôi khi có thể được dùng theo nghĩa "sự cố" hay "sự rủi ro".

3.4

**Bối cảnh bên ngoài** (external context)

Môi trường bên ngoài, nơi mà tổ chức theo đuổi để đạt được các mục tiêu của mình.

[TCVN 9788:2013]

CHÚ THÍCH: Bối cảnh bên ngoài có thể bao gồm:

- môi trường văn hóa, xã hội, chính trị, pháp lý, quy định, tài chính, công nghệ, kinh tế, môi trường tự nhiên và môi trường cạnh tranh, trong phạm vi quốc tế, quốc gia, khu vực hoặc địa phương;

- những xu hướng và động lực chính tác động đến những mục tiêu của tổ chức;
- những mối quan hệ với các bên liên quan bên ngoài tổ chức, và những nhận thức, giá trị của các bên liên quan đó.

**3.5**

**Bối cảnh nội bộ** (internal context)

Môi trường nội bộ nơi mà tổ chức theo đuổi để đạt được các mục tiêu của mình

[TCVN 9788:2013]

CHÚ THÍCH: Bối cảnh nội bộ có thể bao gồm:

- quản trị, cơ cấu tổ chức, vai trò và trách nhiệm giải trình;
- những chính sách, mục tiêu và chiến lược của tổ chức được đưa ra để đạt được mục đích;
- năng lực, được hiểu như là các nguồn lực và tri thức (Ví dụ như nguồn vốn, thời gian, con người, các quy trình, các hệ thống và các công nghệ);
- các hệ thống thông tin, luồng thông tin và quy trình đưa ra quyết định (cả chính thức và không chính thức);
- những mối quan hệ với các bên liên quan bên trong tổ chức và những nhận thức và giá trị về các bên liên quan bên trong tổ chức đó;
- văn hóa của tổ chức;
- những tiêu chuẩn, hướng dẫn và mô hình mà tổ chức chấp nhận;
- hình thức và phạm vi của những mối quan hệ bằng hợp đồng.

**3.6**

**Mức rủi ro** (level of risk)

Tính chất nghiêm trọng của **rủi ro** (3.9), được hiểu theo nghĩa là sự kết hợp giữa **hậu quả** (3.1) và **khả năng xảy ra** (3.7) của một sự kiện.

[TCVN 9788:2013]

**3.7**

**Khả năng xảy ra** (likelihood)

Cơ hội xảy ra một sự kiện

[TCVN 9788:2013]

CHÚ THÍCH 1: Trong thuật ngữ quản lý rủi ro, từ "khả năng xảy ra" thường được dùng để chỉ cơ hội xảy ra một sự kiện, có thể được định nghĩa, được đo lường hay được xác định một cách chủ quan hay khách quan, dưới dạng định tính hay định lượng và được mô tả bằng cách sử dụng thuật ngữ chung hoặc bằng toán học (như xác suất hoặc tần suất trong một khoảng thời gian nhất định).

CHÚ THÍCH 2: Thuật ngữ "khả năng xảy ra" có nghĩa tương đương với thuật ngữ "xác suất". Tuy nhiên thuật ngữ "xác suất" thường chỉ hiểu theo nghĩa hẹp như là thuật ngữ toán học. Do đó, trong thuật ngữ quản lý rủi ro, "khả năng xảy ra" thường được sử dụng với mục đích giải thích như thuật ngữ "xác suất".

**3.8**

**Rủi ro tồn đọng** (residual risk)

**Rủi ro** (3.9) còn lại sau khi **xử lý rủi ro** (3.17)

[TCVN 9788:2013]

CHÚ THÍCH 1: Rủi ro tồn đọng có thể gồm rủi ro chưa được nhận biết.

CHÚ THÍCH 2: Rủi ro tồn đọng cũng có thể được gọi là "rủi ro được giữ lại".

**3.9**

**Rủi ro** (risk)

Ảnh hưởng sự không chắc chắn đến các mục tiêu

[TCVN 9788:2013]

CHÚ THÍCH 1: Một ảnh hưởng là một sự sai lệch so với kỳ vọng – kết quả ảnh hưởng có thể là tích cực hay tiêu cực.

CHÚ THÍCH 2: Những mục tiêu có thể có những khía cạnh khác nhau (như khía cạnh về tài chính, y tế và an toàn, an toàn thông tin và những mục tiêu về môi trường) và có thể áp dụng ở các mức khác nhau (như chiến lược, tổ chức mở rộng, dự án, sản phẩm và quy trình).

CHÚ THÍCH 3: Rủi ro thường được đặc trưng bởi các sự kiện (3.3) và hậu quả (3.1) tiềm ẩn hoặc là sự kết hợp giữa chúng.

CHÚ THÍCH 4: Rủi ro an toàn thông tin thường được thể hiện bằng sự kết hợp giữa hậu quả của một sự kiện an toàn thông tin và khả năng xảy ra kèm theo.

CHÚ THÍCH 5: Sự không chắc chắn là tình trạng thiếu thông tin liên quan tới việc hiểu biết hoặc nhận thức về một sự kiện, hậu quả hay khả năng xảy ra kèm theo.

CHÚ THÍCH 6: Rủi ro an toàn thông tin liên quan đến những vấn đề tiềm ẩn mà những mối đe dọa có thể khai thác những điểm yếu của một hoặc một nhóm tài sản thông tin và do đó gây ra thiệt hại đối với tổ chức.

**3.10**

**Phân tích rủi ro** (risk analysis)

Quá trình tìm hiểu bản chất của rủi ro và xác định **mức rủi ro** (3.6)

[TCVN 9788:2013]

CHÚ THÍCH 1: Phân tích rủi ro cung cấp cơ sở cho việc ước lượng rủi ro và quyết định cách xử lý rủi ro.

CHÚ THÍCH 2: Phân tích rủi ro bao gồm cả ước đoán rủi ro.

**3.11**

**Đánh giá rủi ro** (risk assessment)

Quy trình tổng thể bao gồm **nhận biết rủi ro** (3.15), **phân tích rủi ro** (3.10) và **ước lượng rủi ro** (3.14)

[TCVN 9788:2013]

**3.12**

***Truyền thông và tư vấn rủi ro*** (risk communication and consultation)

Những quy trình liên tục và lặp đi lặp lại mà tổ chức tiến hành để cung cấp, chia sẻ hay thu nhận thông tin và tiến hành đối thoại với **những bên liên quan** (3.18) về quản lý **rủi ro** (3.9)

[TCVN 9788:2013]

CHÚ THÍCH 1: Thông tin có thể liên quan đến sự tồn tại, bản chất, hình thức, khả năng xảy ra, tầm quan trọng, việc ước lượng, khả năng chấp nhận và xử lý rủi ro.

CHÚ THÍCH 2: Tư vấn là một quy trình truyền thông hai chiều giữa tổ chức đó với những bên liên quan về một vấn đề trước khi đưa ra quyết định hoặc xác định định hướng về vấn đề đó. Tư vấn là:

- một quy trình tác động đến quyết định thông qua những ảnh hưởng hơn là thông qua quyền lực;
- là đầu vào để ra quyết định, nhưng không tham gia vào quá trình ra quyết định.

**3.13**

**Tiêu chí rủi ro** (risk criteria)

Điều khoản tham chiếu mà dựa vào đó để ước lượng mức nghiêm trọng của **rủi ro** (3.9)

[TCVN 9788:2013]

CHÚ THÍCH 1: Tiêu chí rủi ro dựa vào những mục tiêu, bối cảnh nội bộ và bối cảnh bên ngoài của tổ chức.

CHÚ THÍCH 2: Tiêu chí rủi ro có thể được bắt nguồn từ những tiêu chuẩn, luật, chính sách và các yêu cầu khác.

**3.14**

**Ước lượng rủi ro** (risk evaluation)

Quy trình so sánh kết quả của việc **phân tích rủi ro** (3.10) với các **tiêu chí rủi ro** (3.13) để xác định xem rủi ro đó và/hoặc mức nghiêm trọng của rủi ro đó có thể chấp nhận hay chịu đựng được hay không.

[TCVN 9788:2013]

CHÚ THÍCH: Ước lượng rủi ro hỗ trợ việc quyết định cách xử lý rủi ro.

**3.15**

**Nhận biết rủi ro** (risk identification)

Quy trình tìm kiếm, nhận dạng và mô tả rủi ro

[TCVN 9788:2013]

CHÚ THÍCH 1: Nhận biết rủi ro bao gồm nhận biết về nguồn gốc của rủi ro, các sự kiện, những nguyên nhân và hậu quả tiềm ẩn của chúng.

CHÚ THÍCH 2: Nhận biết rủi ro có thể liên quan đến dữ liệu trong quá khứ, phân tích lý thuyết, thông tin và ý kiến chuyên môn và nhu cầu của các bên liên quan.

**3.16**

**Quản lý rủi ro** (risk management)

Các hoạt động phối hợp về vấn đề rủi ro để điều hành và kiểm soát tổ chức

[TCVN 9788:2013]

CHÚ THÍCH: Tiêu chuẩn này sử dụng thuật ngữ "quy trình" để mô tả tổng quan việc quản lý rủi ro. Các yếu tố bên trong quy trình quản lý rủi ro được gọi là "các hoạt động".

**3.17**

**Xử lý rủi ro** (risk treatment)

Quá trình điều chỉnh rủi ro

[TCVN 9788:2013]

CHÚ THÍCH 1: Xử lý rủi ro có thể liên quan đến việc:

- tránh rủi ro bằng cách quyết định không bắt đầu hoặc tiếp tục việc hoạt động làm tăng thêm rủi ro;
- chấp nhận hoặc làm tăng rủi ro để theo đuổi một cơ hội;
- loại bỏ nguồn gốc rủi ro;
- thay đổi khả năng xảy ra;
- thay đổi hậu quả;
- chia sẻ rủi ro với một bên hay nhiều bên khác (bao gồm cả hợp đồng và gây quỹ bồi thường rủi ro)
- Duy trì rủi ro bằng lựa chọn có hiểu biết.

CHÚ THÍCH 2: Xử lý rủi ro để giải quyết các hậu quả tiêu cực đôi khi được gọi là "giảm nhẹ rủi ro", "loại bỏ rủi ro", "ngăn chặn rủi ro" và "giảm bớt rủi ro".

CHÚ THÍCH 3: Xử lý rủi ro có thể tạo ra những rủi ro mới hoặc làm thay đổi những rủi ro hiện có.

**3.18**

**Bên liên quan** (stakeholder)

Cá nhân hay tổ chức có thể gây ảnh hưởng, bị ảnh hưởng, hoặc nhận thấy bị ảnh hưởng bởi một quyết định hay một hành động

[TCVN 9788:2013]

CHÚ THÍCH: Người đưa ra quyết định có thể là một bên liên quan.

## 4 Cấu trúc của tiêu chuẩn

Tiêu chuẩn này bao gồm những mô tả về quy trình và hoạt động quản lý rủi ro an toàn thông tin.

Thông tin cơ bản được cung cấp tại điều 5.

Tổng quan về quy trình quản lý rủi ro an toàn thông tin được trình bày tại điều 6.

Tất cả các hoạt động quản lý rủi ro an toàn thông tin được nêu tại điều 6 sẽ được tiếp tục mô tả chi tiết từ điều 7 đến điều 12:

- Thiết lập bối cảnh trong điều 7,
- Đánh giá rủi ro trong điều 8,
- Xử lý rủi ro trong điều 9,
- Chấp nhận rủi ro trong điều 10,
- Truyền thông rủi ro trong điều 11,
- Giám sát và soát xét rủi ro trong điều 12.

Thông tin bổ sung cho những hoạt động quản lý rủi ro an toàn thông tin sẽ được trình bày trong các phụ lục. Nội dung thiết lập bối cảnh cho an toàn thông tin của tổ chức sẽ được hướng dẫn theo Phụ lục A (xác định phạm vi và giới hạn của quy trình quản lý rủi ro an toàn thông tin). Việc nhận biết, định giá tài sản và đánh giá tác động được đề cập tại Phụ lục B. Phụ lục C đưa ra các ví dụ về các mối đe dọa điển hình và Phụ lục D đề cập tới các điểm yếu và những phương pháp để đánh giá các điểm yếu. Các ví dụ về phương pháp tiếp cận đánh giá rủi ro an toàn thông tin được trình bày trong Phụ lục E.

Các ràng buộc về thay đổi rủi ro được trình bày trong Phụ lục F.

Sự khác nhau trong các định nghĩa giữa ISO/IEC 27005:2008 và TCVN 10295:2014 sẽ được đưa ra trong Phụ lục G.

Tất cả hoạt động quản lý rủi ro từ điều 7 đến điều 12 được trình bày theo cấu trúc như sau:

**Đầu vào:** Nhận biết bất kỳ thông tin cần thiết để thực hiện hành động.

**Hành động:** Mô tả hoạt động

**Hướng dẫn triển khai:** Cung cấp hướng dẫn thực hiện hành động. Một vài hướng dẫn có thể chưa hoàn toàn phù hợp cho mọi hoàn cảnh và do đó các cách thực hiện hành động khác có thể phù hợp hơn.

**Đầu ra:** Nhận biết bất kỳ thông tin thu được sau khi thực hiện hoạt động.

## 5 Thông tin cơ bản

Một phương pháp tiếp cận có tính hệ thống nhằm quản lý rủi ro an toàn thông tin là cần thiết để nhận biết được những nhu cầu của tổ chức về những yêu cầu an toàn thông tin và tạo ra một hệ thống quản lý an toàn thông tin (ISMS) có hiệu quả. Phương pháp tiếp cận quản lý rủi ro an toàn thông tin phải phù hợp với môi trường của tổ chức và đặc biệt phải phù hợp với định hướng chung về quản lý rủi ro của tổ chức. Các nỗ lực an toàn thông tin cần giải quyết những rủi ro theo một cách thức hiệu quả và kịp thời tại địa điểm và thời điểm cần thiết. Quản lý rủi ro an toàn thông tin là một bộ phận không thể thiếu của các hoạt động quản lý an toàn thông tin và có thể áp dụng cho cả triển khai và vận hành liên tục hệ thống ISMS.

Quản lý rủi ro an toàn thông tin là một quy trình liên tục. Quy trình này cần thiết phải thiết lập bối cảnh nội bộ và bối cảnh bên ngoài của tổ chức, đánh giá rủi ro và xử lý rủi ro theo kế hoạch xử lý rủi ro để

triển khai những khuyến nghị và quyết định. Quản lý rủi ro phân tích những gì có thể xảy ra và hậu quả có thể gặp phải, trước khi quyết định thực những việc cần phải làm và khi nào làm để giảm rủi ro tới mức chấp nhận được.

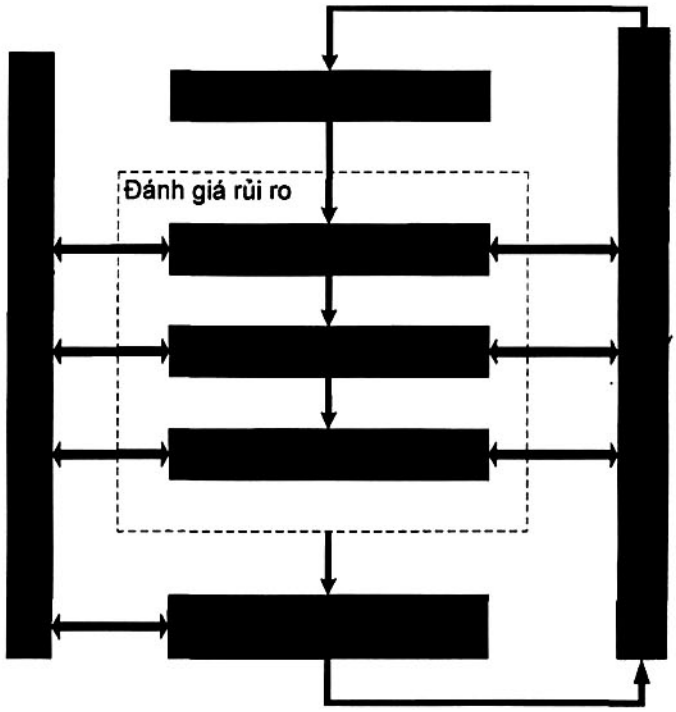
Quản lý rủi ro an toàn thông tin phải đóng góp trong những hoạt động sau:

- Nhận biết rủi ro
- Đánh giá rủi ro về hậu quả của các rủi ro đối với hoạt động nghiệp vụ của tổ chức và khả năng có thể xảy ra
- Truyền thông và nhận thức rõ các khả năng xảy ra và hậu quả của các rủi ro
- Thiết lập thứ tự ưu tiên để xử lý rủi ro
- Ưu tiên cho các hành động nhằm làm giảm rủi ro đang xảy ra
- Các bên liên quan được tham gia quyết định về quản lý rủi ro và luôn được thông báo về trạng thái quản lý rủi ro
- Tăng hiệu quả của hoạt động giám sát xử lý rủi ro
- Giám sát và soát xét thường xuyên các rủi ro và quy trình quản lý rủi ro
- Thu thập thông tin để cải tiến phương pháp tiếp cận quản lý rủi ro
- Đào tạo cho cán bộ quản lý và đội ngũ nhân viên về những rủi ro và các hành động nhằm giảm nhẹ các rủi ro

Quy trình quản lý rủi ro an toàn thông tin có thể áp dụng cho toàn bộ tổ chức hoặc cho bất kỳ bộ phận nào của tổ chức (ví dụ như một phòng ban, một địa điểm, một dịch vụ), hay cho bất kỳ hệ thống thông tin nào, đã tồn tại hoặc đã được lập kế hoạch, hoặc trong những khía cạnh cụ thể của biện pháp kiểm soát (như kế hoạch liên tục trong nghiệp vụ).

## 6 Tổng quan về quy trình quản lý rủi ro an toàn thông tin

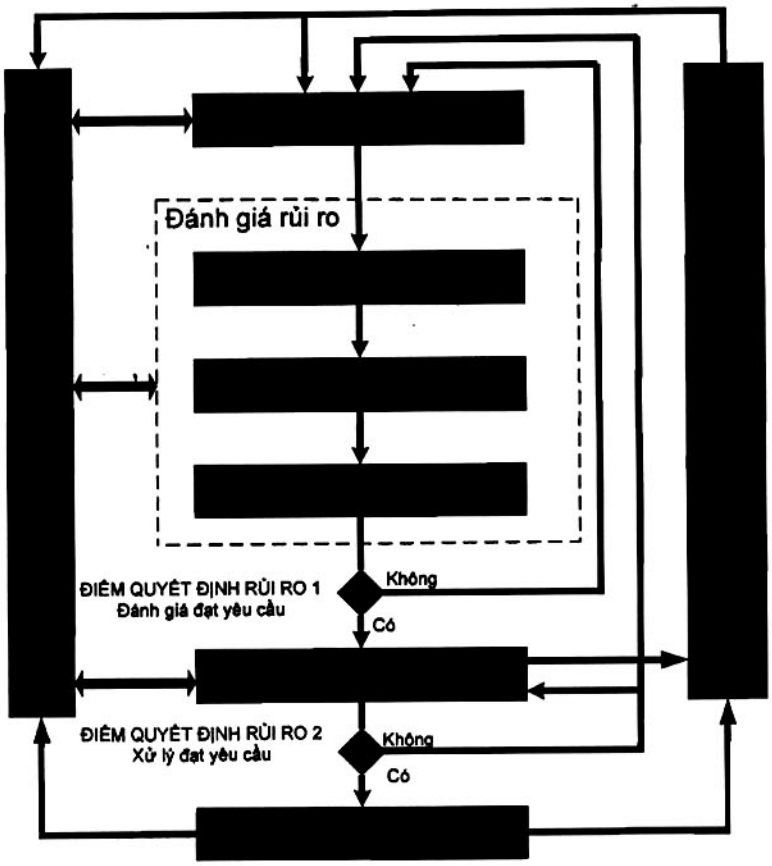
Quy trình quản lý rủi ro được xác định trong ISO 31000 được trình bày trong Hình 1.




**Hình 1 – Quy trình quản lý rủi ro**

Hình 2 thể hiện cách tiêu chuẩn này đã áp dụng quy trình quản lý rủi ro nêu trên như thế nào.

Quy trình quản lý rủi ro an toàn thông tin bao gồm: thiết lập bối cảnh (điều 7), đánh giá rủi ro (điều 8), xử lý rủi ro (điều 9), chấp nhận rủi ro (điều 10), truyền thông và tư vấn rủi ro (điều 11), giám sát và soát xét rủi ro (điều 12).




**Hình 2 – Minh họa về quy trình quản lý rủi ro an toàn thông tin**

Như minh họa tại Hình 2, quy trình quản lý rủi ro an toàn thông tin là quy trình lặp đối với các hoạt động đánh giá rủi ro, xử lý rủi ro. Một phương pháp tiếp cận lặp để tiến hành đánh giá rủi ro có thể làm việc đánh giá tăng theo chiều sâu và chi tiết hơn sau mỗi lần lặp. Phương pháp tiếp cận lặp đi lặp lại này sẽ tạo ra một sự cân bằng tốt giữa việc tối ưu thời gian và việc nỗ lực nhận biết các kiểm soát, trong khi vẫn đảm bảo những rủi ro cao đã được đánh giá một cách phù hợp.

Bối cảnh được thiết lập đầu tiên, sau đó sẽ tiến hành đánh giá rủi ro. Nếu việc đánh giá này cung cấp đầy đủ thông tin để xác định một cách hiệu quả các hoạt động cần thiết để thay đổi rủi ro tới mức có thể chấp nhận được thì lúc đó nhiệm vụ đánh giá rủi ro được coi là đã hoàn thành và tiếp sau đó là tiến hành xử lý rủi ro. Nếu thông tin không đầy đủ thì sẽ lặp lại đánh giá rủi ro với bối cảnh đã được soát xét lại (ví dụ như tiêu chí ước lượng rủi ro, tiêu chí chấp nhận rủi ro hoặc tiêu chí tác động), việc lặp lại đánh giá có thể chỉ tiến hành theo một số phần hạn chế trên toàn bộ phạm vi (xem Hình 2, Điểm Quyết định Rủi ro 1).

Hiệu quả của việc xử lý rủi ro phụ thuộc chặt chẽ vào kết quả của việc đánh giá rủi ro.

Chú ý việc xử lý rủi ro bao gồm một quy trình theo chu kỳ gồm:

- đánh giá một kết quả xử lý rủi ro
- quyết định các mức rủi ro còn tồn đọng có thể chấp nhận được không.
- đưa ra một phương pháp xử lý rủi ro mới nếu các mức rủi ro không thể chấp nhận được
- đánh giá hiệu quả của xử lý rủi ro đó

Việc xử lý rủi ro có thể sẽ không lập tức đạt được mức rủi ro tồn đọng theo yêu cầu (có thể chấp nhận được). Trong trường hợp này, nếu cần thiết, phải tiến hành đánh giá lại rủi ro với các điều chỉnh về các điều kiện của bối cảnh (như đánh giá rủi ro, mức chấp nhận rủi ro hoặc tiêu chí tác động), tiếp sau đó là bước xử lý rủi ro (xem Hình 2, Điểm Quyết định Rủi ro 2).

Hoạt động chấp nhận rủi ro phải đảm bảo các rủi ro tồn đọng phải được sự đồng ý cụ thể của ban quản lý của tổ chức. Điều này đặc biệt quan trọng trong trường hợp việc triển khai các biện pháp kiểm soát bị bỏ qua hoặc bị trì hoãn vì các lý do khác nhau như thiếu kinh phí, nhân lực...

Trong suốt toàn bộ quy trình quản lý rủi ro an toàn thông tin thì việc thông báo kết quả đánh giá rủi ro và xử lý rủi ro tới các cán bộ quản lý và nhân viên vận hành thích hợp là rất quan trọng. Ngay cả trước khi xử lý rủi ro, những thông tin về các rủi ro đã được nhận biết có thể rất quan trọng trong việc quản lý sự cố và có thể giúp giảm thiểu các ảnh hưởng xấu có thể xảy ra. Nhận thức của cán bộ quản lý và nhân viên về những rủi ro, bản chất của các biện pháp để giảm nhẹ rủi ro và những phạm vi mà tổ chức quan tâm sẽ giúp xử lý các sự cố và các sự kiện không mong muốn một cách hiệu quả nhất. Cần phải tài liệu hóa chi tiết kết quả của tất cả quy trình quản lý rủi ro an toàn thông tin và hai điểm quyết định rủi ro (xem Hình 2).

TCVN ISO/IEC 27001:2009 chỉ ra các biện pháp được triển khai trong phạm vi, giới hạn và bối cảnh của ISMS cần phải căn cứ vào rủi ro. Việc ứng dụng một quy trình quản lý rủi ro an toàn thông tin có thể đáp ứng được yêu cầu này. Có nhiều phương pháp tiếp cận để triển khai thành công quy trình này trong một tổ chức. Tổ chức có thể sử dụng bất cứ phương pháp tiếp cận nào phù hợp nhất với hoàn cảnh của mình cho mỗi một ứng dụng cụ thể của quy trình.

Trong một ISMS, thiết lập bối cảnh, đánh giá rủi ro, phát triển kế hoạch xử lý rủi ro và chấp nhận rủi ro là tất cả các bước cần thực hiện của giai đoạn "Lập kế hoạch". Trong giai đoạn "Thực hiện" của ISMS, các hoạt động và biện pháp kiểm soát cần thiết để giảm rủi ro tới mức chấp nhận được được tiến hành theo kế hoạch xử lý rủi ro. Trong giai đoạn "Kiểm tra" của ISMS, ban quản lý sẽ phải xác định sự cần thiết trong việc duyệt lại kết quả đánh giá rủi ro và xử lý rủi ro dựa trên các sự cố xảy ra và những thay đổi về hoàn cảnh. Trong giai đoạn "Hành động", triển khai tất cả các hoạt động cần thiết và cả các hoạt động bổ sung của quy trình quản lý rủi ro an toàn thông tin.

Bảng dưới đây sẽ tổng hợp các hoạt động quản lý rủi ro an toàn thông tin liên quan đến bốn giai đoạn của quy trình ISMS như sau:

**Bảng 1 - ISMS và quy trình quản lý rủi ro an toàn thông tin**

| Quy trình ISMS | Quy trình quản lý rủi ro an toàn thông tin |
|---|---|
| **Lập kế hoạch** | Thiết lập bối cảnh<br>Đánh giá rủi ro<br>Phát triển kế hoạch xử lý rủi ro<br>Chấp nhận rủi ro |
| **Thực hiện** | Triển khai kế hoạch xử lý rủi ro |
| **Kiểm tra** | Liên tục giám sát và soát xét rủi ro |
| **Hành động** | Duy trì và cải tiến quy trình quản lý rủi ro an toàn thông tin |

## 7 Thiết lập bối cảnh

### 7.1 Xem xét chung

**Đầu vào**: Toàn bộ thông tin về tổ chức liên quan tới thiết lập bối cảnh quản lý rủi ro an toàn thông tin.

**Hành động**: Cần phải thiết lập bối cảnh nội bộ và bối cảnh bên ngoài tổ chức cho các hoạt động quản lý rủi ro an toàn thông tin, trong đó bao gồm việc thiết lập tiêu chí cơ bản cần thiết cho hoạt động quản lý rủi ro an toàn thông tin (7.2), định nghĩa phạm vi và giới hạn (7.3) và thiết lập một tổ chức thích hợp để vận hành hoạt động quản lý rủi ro an toàn thông tin (7.4).

**Hướng dẫn triển khai**: Cần thiết phải xác định mục đích của việc quản lý rủi ro an toàn thông tin bởi vì điều này ảnh hưởng đến toàn bộ quy trình và việc thiết lập bối cảnh cụ thể. Mục đích này có thể là:

- Hỗ trợ cho hệ thống quản lý an toàn thông tin (ISMS)
- Tuân thủ pháp luật và bằng chứng thẩm định
- Chuẩn bị một kế hoạch liên tục trong nghiệp vụ
- Chuẩn bị một kế hoạch ứng cứu sự cố
- Mô tả về những yêu cầu an toàn thông tin đối với một sản phẩm, một dịch vụ hoặc một cơ chế.

Hướng dẫn triển khai cho các yếu tố thiết lập bối cảnh cần thiết để hỗ trợ cho hệ thống ISMS được đề cập thêm tại 7.2, 7.3 và 7.4 dưới đây.

CHÚ THÍCH: TCVN ISO/IEC 27001:2009 không sử dụng thuật ngữ "bối cảnh". Tuy nhiên, điều 7 liên quan đến các yêu cầu "xác định phạm vi và giới hạn của ISMS" [4.2.1 a)], "xác định chính sách của ISMS" [4.2.1 b)] và "xác định phương pháp tiếp cận đánh giá rủi ro" [4.2.1 c)] cụ thể trong TCVN ISO/IEC 27001:2009.

**Đầu ra** : Đặc tả kỹ thuật về tiêu chí cơ bản, phạm vi và giới hạn và tổ chức thực hiện quy trình quản lý rủi ro an toàn thông tin.

### 7.2 Tiêu chí cơ bản

#### 7.2.1 Phương pháp tiếp cận quản lý rủi ro

Tùy thuộc vào phạm vi và mục tiêu quản lý rủi ro mà có thể áp dụng nhiều phương pháp tiếp cận khác nhau. Phương pháp tiếp cận cũng có thể khác nhau đối với từng chu trình lặp lại.

Một phương pháp tiếp cận quản lý rủi ro thích hợp cần phải được lựa chọn hoặc phát triển để giải quyết tiêu chí cơ bản như: tiêu chí ước lượng rủi ro, tiêu chí về tác động, tiêu chí chấp nhận rủi ro.

Ngoài ra, tổ chức cần phải đánh giá xem những nguồn lực cần thiết có sẵn có hay không để:

- Thực hiện đánh giá rủi ro và thiết lập kế hoạch xử lý rủi ro
- Định nghĩa và triển khai các chính sách và thủ tục, bao gồm việc triển khai các biện pháp kiểm soát đã được lựa chọn
- Giám sát các kiểm soát
- Giám sát quy trình quản lý rủi ro an toàn thông tin

CHÚ THÍCH: Xem thêm TCVN ISO/IEC 27001:2009 (5.2.1) liên quan tới điều khoản về các nguồn lực cho hoạt động triển khai và vận hành một hệ thống ISMS

#### 7.2.2 Tiêu chí ước lượng rủi ro

Tiêu chí ước lượng rủi ro cần phải được phát triển để ước lượng rủi ro an toàn thông tin của tổ chức liên quan đến:

- Giá trị chiến lược của quy trình thông tin nghiệp vụ
- Mức quan trọng đối với tài sản thông tin có liên quan
- Các yêu cầu về pháp lý và quy định và các trách nhiệm về hợp đồng
- Tầm quan trọng của tính sẵn sàng, tính bí mật và tính toàn vẹn trong các hoạt động mang tính nghiệp vụ và vận hành
- Những nhận thức và mong muốn của các bên liên quan và những hậu quả xấu đối với danh tiếng và uy tín của tổ chức

Ngoài ra, tiêu chí ước lượng rủi ro có thể được sử dụng để xác định ưu tiên cho việc xử lý rủi ro.

#### 7.2.3 Tiêu chí tác động

Tiêu chí tác động cần phải được xác định và phát triển theo mức thiệt hại hoặc các khoản chi phí đối với tổ chức mà nguyên nhân gây ra là từ các sự kiện an toàn thông tin mà có liên quan đến:

- Mức phân loại tài sản thông tin bị tác động
- Vi phạm an toàn thông tin (làm giảm tính bí mật, tính toàn vẹn và tính sẵn sàng)
- Yếu kém trong vận hành (nội bộ hoặc các bên thứ ba)
- Tổn hại về giá trị nghiệp vụ và tài chính
- Phá vỡ các kế hoạch và thời hạn
- Thiệt hại về uy tín
- Vi phạm các yêu cầu về pháp lý, quy định hoặc các cam kết theo hợp đồng

CHÚ THÍCH: Xem thêm TCVN ISO/IEC 27001:2009, 4.2.1 d) 4) liên quan tới việc xác định tiêu chí tác động làm giảm tính bí mật, tính toàn vẹn và tính sẵn sàng.

### 7.2.4 Tiêu chí chấp nhận rủi ro

Tiêu chí chấp nhận rủi ro cần phải được xác định và phát triển. Tiêu chí chấp nhận rủi ro thường phụ thuộc vào các chính sách, mục đích, mục tiêu của tổ chức và các lợi ích của các bên liên quan.

Mỗi tổ chức cần phải xác định mức chấp nhận rủi ro của riêng tổ chức mình. Trong suốt quy trình phát triển cần phải xem xét các vấn đề sau:

- Tiêu chí chấp nhận rủi ro có thể bao gồm nhiều ngưỡng, dựa theo mức mục tiêu mong muốn về rủi ro, nhưng phụ thuộc vào từng điều kiện thực tế cụ thể để cán bộ quản lý cao cấp có thể chấp nhận mức rủi ro
- Tiêu chí chấp nhận rủi ro có thể được thể hiện như tỉ lệ lợi nhuận ước lượng (hoặc các lợi ích nghiệp vụ khác) trên rủi ro được ước lượng
- Các tiêu chí chấp nhận rủi ro khác nhau có thể được áp dụng cho nhiều loại rủi ro khác nhau, ví dụ như những rủi ro mà có thể dẫn tới việc không tuân thủ pháp lý hoặc quy định có thể không được chấp nhận, trong khi việc chấp nhận các rủi ro ở mức cao lại có thể được phép nếu việc chấp nhận này được xác định như là các yêu cầu của hợp đồng.
- Tiêu chí chấp nhận rủi ro có thể bao gồm những yêu cầu cho việc xử lý bổ sung trong tương lai, ví dụ: một rủi ro có thể được chấp nhận thông qua với cam kết sẽ có hành động làm giảm rủi ro tới mức có thể chấp nhận được trong một khoảng thời gian nhất định

Tiêu chí chấp nhận rủi ro có thể khác nhau tùy theo thời gian dự tính tồn tại của rủi ro, ví dụ: rủi ro có thể liên quan đến một hoạt động ngắn hạn hoặc tạm thời. Tiêu chí chấp nhận rủi ro được thiết lập như sau:

- Tiêu chí nghiệp vụ
- Khía cạnh pháp lý và các quy định
- Sự vận hành
- Công nghệ
- Tài chính
- Các yếu tố về xã hội và con người.

CHÚ THÍCH: Tiêu chí chấp nhận rủi ro tương tự với "tiêu chí chấp nhận rủi ro và nhận biết mức rủi ro có thể chấp nhận được" và được quy định rõ trong TCVN ISO/IEC 27001:2009, xem 4.2.1 c) 2).

Thông tin chi tiết được trình bày trong Phụ lục A.

## 7.3 Phạm vi và giới hạn

Tổ chức cần phải xác định rõ phạm vi và giới hạn cho quản lý rủi ro an toàn thông tin.

Phạm vi của quy trình quản lý rủi ro an toàn thông tin cần được xác định rõ để đảm bảo toàn bộ tài sản liên quan phải được quan tâm xem xét trong quy trình đánh giá rủi ro. Ngoài ra, cần phải nhận biết các giới hạn [xem TCVN ISO/IEC 27001:2009, 4.2.1 a)] để giải quyết những rủi ro có thể phát sinh thêm ngoài giới hạn đã có.

Cần phải thu thập những thông tin về tổ chức để xác định môi trường mà tổ chức hoạt động và sự liên quan của tổ chức đó tới quy trình quản lý rủi ro an toàn thông tin.

Khi xác định phạm vi và giới hạn, tổ chức cần phải xem xét tới những thông tin sau:

- Những mục tiêu, chiến lược và chính sách nghiệp vụ mang tính chiến lược của tổ chức
- Những quy trình nghiệp vụ
- Tổ chức bộ máy và chức năng của tổ chức
- Pháp lý, quy định và các cam kết cần áp dụng cho tổ chức
- Chính sách an toàn thông tin của tổ chức
- Phương pháp tiếp cận tổng thể của tổ chức đối với việc quản lý rủi ro
- Các tài sản thông tin
- Vị trí và đặc điểm địa lý của tổ chức
- Những ràng buộc ảnh hưởng đến tổ chức
- Kỳ vọng của các bên liên quan
- Môi trường văn hóa - xã hội
- Các giao diện (trao đổi thông tin với môi trường)

Thêm vào đó, tổ chức phải cung cấp bằng chứng cho các trường hợp ngoại lệ.

Các ví dụ về phạm vi quản lý rủi ro có thể là một ứng dụng công nghệ thông tin, cơ sở hạ tầng công nghệ thông tin, một quy trình nghiệp vụ, hoặc một bộ phận đã được định rõ của tổ chức.

CHÚ THÍCH: Phạm vi và giới hạn của hoạt động quản lý rủi ro an toàn thông tin liên quan tới phạm vi và giới hạn của hệ thống ISMS được quy định trong TCVN ISO/IEC 27001:2009, xem 4.2.1 a).

Thông tin chi tiết hơn có thể tìm thấy trong Phụ lục A.

### 7.4 Tổ chức quản lý rủi ro an toàn thông tin

Cần phải thiết lập và duy trì tổ chức cũng như những trách nhiệm của tổ chức đối với quy trình quản lý rủi ro an toàn thông tin. Dưới đây sẽ đưa ra vai trò và trách nhiệm chính của tổ chức đối với quy trình quản lý rủi ro an toàn thông tin :

- Phát triển quy trình quản lý rủi ro an toàn thông tin phù hợp cho tổ chức.
- Nhận biết và phân tích về các bên liên quan
- Xác định rõ vai trò và trách nhiệm của tất cả các bên, kể cả nội bộ và bên ngoài tổ chức
- Thiết lập những mối quan hệ cần thiết giữa tổ chức với các bên liên quan quản lý rủi ro an toàn thông tin, cũng như những giao diện đối với các chức năng quản lý rủi ro ở mức cao của tổ chức (ví dụ như quản lý rủi ro trong vận hành), cũng như những giao diện đối với những dự án hay các hoạt động có liên quan khác
- Vạch rõ hướng quyết định tiếp theo
- Đặc điểm kỹ thuật của hồ sơ cần được lưu trữ

Tổ chức phải được chấp thuận bởi những người quản lý thích hợp của tổ chức.

CHÚ THÍCH: TCVN ISO/IEC 27001:2009 yêu cầu phải xác định các nguồn lực dự trữ cần thiết để tiến hành thiết lập, triển khai, vận hành, giám sát, soát xét, duy trì và cải tiến một hệ thống ISMS, xem 5.2.1 a). Tổ chức thực hiện các hoạt động quản lý rủi ro có thể được xem như là một trong các nguồn lực cần thiết trong TCVN ISO/IEC 27001:2009.

# 8 Đánh giá rủi ro an toàn thông tin

## 8.1 Mô tả chung về đánh giá rủi ro an toàn thông tin

CHÚ THÍCH: Hoạt động đánh giá rủi ro an toàn thông tin được nói đến như là quy trình trong TCVN ISO/IEC 27001:2009.

**Đầu vào**: Các tiêu chí cơ bản, phạm vi và giới hạn và tổ chức thực hiện quy trình quản lý rủi ro an toàn thông tin được thiết lập.

**Hành động**: Các rủi ro cần phải được nhận biết được mô tả định tính hoặc định lượng và sắp xếp mức ưu tiên theo các tiêu chí ước lượng rủi ro và các mục tiêu liên quan tới tổ chức.

**Hướng dẫn triển khai:**

Một rủi ro là một sự kết hợp các hậu quả do những sự kiện không mong muốn và khả năng xuất hiện của các sự kiện đó. Việc đánh giá rủi ro định lượng hoặc mô tả định tính về rủi ro và cho phép những người quản lý đặt ra mức ưu tiên cho những rủi ro dựa trên nhận thức của họ về mức nghiêm trọng hoặc các tiêu chí đã được thiết lập khác.

Đánh giá rủi ro bao gồm các hoạt động sau:

- Nhận biết rủi ro (8.2)
- Phân tích rủi ro (8.3)
- Ước lượng rủi ro (8.4)

Đánh giá rủi ro nhằm xác định giá trị của các tài sản thông tin, nhận biết các đe dọa có thể xảy ra và các điểm yếu vẫn còn tồn tại (hoặc có thể tồn tại), nhận biết các biện pháp kiểm soát hiện có và hiệu quả của các biện pháp đó trong việc nhận biết rủi ro, xác định các hậu quả tiềm ẩn và cuối cùng là phân loại và sắp xếp thứ tự ưu tiên các rủi ro đã tìm được dựa vào bộ tiêu chí đánh giá rủi ro trong quy trình thiết lập bối cảnh.

Đánh giá rủi ro thường được tiến hành tối thiểu hai lần. Lần đầu tiên tiến hành đánh giá sơ bộ để xác định các rủi ro nguy hiểm đang tiềm ẩn, tạo điều kiện cho các bước đánh giá tiếp theo. Bước tiếp theo có thể đánh giá sâu hơn các rủi ro tiềm ẩn đã bộc lộ trong lần đánh giá trước đó. Nếu không có đầy đủ thông tin để đánh giá rủi ro thì sẽ có thể tiến hành phân tích chi tiết bằng phương pháp khác trên một phần hoặc toàn bộ phạm vi.

Mỗi tổ chức cần phải chọn phương pháp tiếp cận riêng để đánh giá rủi ro dựa trên các mục tiêu và mục đích của đánh giá rủi ro.

Các phương pháp tiếp cận đánh giá rủi ro an toàn thông tin được trình bày chi tiết trong Phụ lục E.

**Đầu ra** : Một danh sách những rủi ro đã được đánh giá được sắp xếp theo thứ tự ưu tiên phù hợp với các tiêu chí đánh giá rủi ro.

## 8.2 Nhận biết rủi ro

### 8.2.1 Giới thiệu về nhận biết rủi ro

Mục đích của nhận biết rủi ro là xác định nguyên nhân có thể gây ra thiệt hại tiềm ẩn và hiểu được lý do, phương thức, thời điểm, không gian mà thiệt hại có thể xảy ra. Các bước mô tả trong 8.2.2 đến 8.2.6 sẽ thu thập thông tin làm dữ liệu đầu vào cho hoạt động phân tích rủi ro.

Nhận biết rủi ro có thể bao gồm nhận biết nguồn phát sinh rủi ro, đặt nguồn gốc phát sinh rủi ro dưới sự kiểm soát của tổ chức mặc dù nguồn hoặc nguyên nhân phát sinh này có thể không rõ ràng.

CHÚ THÍCH: Các hoạt động được mô tả trong các mục dưới đây có thể được tiến hành theo thứ tự khác nhau tùy theo từng phương pháp luận được áp dụng.

### 8.2.2 Nhận biết về tài sản

**Đầu vào**: Phạm vi và giới hạn của đánh giá rủi ro được tiến hành, danh sách các thành phần (tài sản) liên quan cùng thông tin về những người sở hữu tài sản, vị trí, chức năng,...

**Hành động**: Cần phải nhận biết rõ các tài sản trong phạm vi đã được thiết lập (xem thêm TCVN ISO/IEC 27001:2009, 4.2.1 d) 1)).

**Hướng dẫn triển khai**:

Tài sản là bất kì thứ gì có giá trị đối với tổ chức và do đó cần được bảo vệ. Nhận biết tài sản cần phải xem xét trong khuôn khổ hệ thống thông tin, trong đó không chỉ bao gồm phần cứng và phần mềm.

Nhận biết tài sản phải được thực hiện ở mức chi tiết phù hợp để cung cấp đầy đủ thông tin cho hoạt động đánh giá rủi ro. Mức chi tiết được sử dụng trong quy trình nhận biết tài sản sẽ ảnh hưởng đến toàn bộ lượng thông tin được thu thập trong suốt quy trình đánh giá rủi ro. Mức chi tiết này có thể được cải tiến trong các bước lặp đi lặp lại của quy trình đánh giá rủi ro.

Cần phải nhận biết rõ người sở hữu tài sản đối với mỗi tài sản, để quy định nghĩa vụ và trách nhiệm đối với tài sản. Người sở hữu tài sản có thể không có quyền sở hữu đối với tài sản đó, nhưng lại có trách nhiệm trong việc sản xuất, phát triển, duy trì, sử dụng và đảm bảo an toàn phù hợp. Người sở hữu tài sản thường là người thích hợp nhất để xác định giá trị của tài sản đối với tổ chức (xem 8.3.2 về định giá tài sản).

Giới hạn cho việc soát xét là tập hợp tất cả các tài sản của tổ chức đã được nhận biết được quản lý bởi quy trình quản lý rủi ro an toàn thông tin.

Thông tin cho việc nhận biết và định giá tài sản liên quan tới an toàn thông tin được trình bày trong Phụ lục B.

**Đầu ra**: Một danh sách các tài sản cần được quản lý rủi ro và danh sách các quy trình nghiệp vụ liên quan đến các tài sản và các vấn đề liên quan khác.

### 8.2.3 Nhận biết về mối đe dọa

Đầu vào: Thông tin về các mối đe dọa thu được từ việc soát xét sự cố, người sở hữu tài sản, người sử dụng tài sản và các nguồn thông tin khác, kể cả danh mục về các mối đe dọa từ bên ngoài.

Hành động: Cần phải nhận biết các mối đe dọa và nguồn gốc phát sinh các mối đe dọa (liên quan tới TCVN ISO/IEC 27001:2009, xem 4.2.1 d) 2)).

Hướng dẫn triển khai:

Một mối đe dọa có khả năng gây thiệt hại cho các tài sản như: thông tin, các quy trình nghiệp vụ, các hệ thống và tổ chức. Các mối đe dọa có thể xuất phát từ những lý do khách quan hay chủ quan, cũng có thể là do cố ý hoặc vô ý. Dù mối đe dọa bắt nguồn từ lý do nào cũng đều phải được nhận biết rõ. Một mối đe dọa có thể phát sinh từ bên trong hoặc bên ngoài tổ chức. Những mối đe dọa này phải được nhận biết một cách tổng quát và theo loại (ví dụ: hành động bất hợp pháp, phá hủy về vật lí, lỗi về công nghệ) và nếu phù hợp là theo từng mối đe dọa riêng trong các phân loại cụ thể. Điều này có nghĩa là không được bỏ sót bất cứ mối đe doạ nào, kể cả trong những trường hợp khó xảy ra, nhưng cần phải giới hạn khối lượng công việc cần thực hiện.

Một số mối đe dọa có thể gây ảnh hưởng đồng thời lên nhiều tài sản. Trong trường hợp này, chúng có thể gây ra các tác động khác nhau tùy thuộc vào tài sản nào bị ảnh hưởng.

Đầu vào cho việc nhận biết đe dọa và việc ước lượng các khả năng xảy ra (8.3.3) có thể thu thập được từ: người quản lý hay người sử dụng tài sản, đội ngũ nhân viên, chuyên gia quản lý phương tiện và chuyên gia an toàn thông tin, các chuyên gia an toàn vật lí, bộ phận pháp lý và các tổ chức khác bao gồm: các cơ quan luật pháp, cơ quan dự báo thời tiết, công ty bảo hiểm và các cơ quan quản lý của chính phủ. Ngoài ra, khi giải quyết các mối đe dọa cũng cần phải quan tâm đến khía cạnh môi trường và văn hóa.

Cần phải tham khảo kinh nghiệm nội bộ thu được từ những sự cố đã xảy ra và kết quả đánh giá các đe dọa đã gặp phải trước khi tiến hành các đánh giá ở hiện tại. Những kinh nghiệm này rất hữu ích khi tra cứu các danh mục về các mối đe dọa khác nhau (có thể chi tiết đối với từng tổ chức hay nghiệp vụ), để hoàn thiện danh sách các mối đe dọa có đặc điểm chung. Danh mục các mối đe dọa và số liệu thống kê có thể tham khảo từ các cơ quan như: các cơ sở nghiên cứu, các hiệp hội, công ty bảo hiểm, các cơ quan quản lý nhà nước về công nghệ thông tin, viễn thông...

Khi sử dụng danh mục về các mối đe dọa hoặc các kết quả đánh giá trước đó về các mối đe dọa, cần phải chú ýrằng luôn luôn có những thay đổi liên quan đến các đe dọa, đặc biệt là những thay đổi về môi trường nghiệp vụ hay môi trường hệ thống thông tin.

Thông tin chi tiết về các loại đe dọa được trình bày ở trong Phụ lục C.

Đầu ra: Một danh sách các mối đe dọa cùng với những thông tin nhận biết về kiểu và nguồn gốc của các mối đe dọa.

### 8.2.4 Nhận biết về các biện pháp kiểm soát hiện có

**Đầu vào**: Tài liệu về các biện pháp kiểm soát, các kế hoạch triển khai xử lý rủi ro.

**Hành động**: Nhận biết các biện pháp kiểm soát hiện có hoặc đã có kế hoạch triển khai.

**Hướng dẫn triển khai**:

Nhận biết các biện pháp kiểm soát hiện có là cần thiết nhằm tránh phải thực hiện nhiều công việc hay đỡ mất chi phí một cách không cần thiết, như trong trường hợp áp dụng các biện pháp kiểm soát trùng lặp. Ngoài ra, khi nhận biết các biện pháp kiểm soát hiện có, cần phải tiến hành việc kiểm tra để đảm bảo các biện pháp kiểm soát này được thực hiện một cách đúng đắn – việc tham khảo các báo cáo kiểm toán hệ thống ISMS có thể giúp hạn chế thời gian thực hiện công việc này. Nếu một biện pháp kiểm soát không được thực hiện đúng như mong muốn, đây có thể là nguyên nhân gây ra các điểm yếu. Cần phải chú ý đến trường hợp nếu một biện pháp (hay chiến lược) đã được chọn lựa bị thất bại khi vận hành thì lúc đó cần phải triển khai các biện pháp kiểm soát bổ sung để giải quyết các rủi ro đã biết một cách hiệu quả. Trong một hệ thống ISMS, theo TCVN ISO/IEC 27001:2009, thì hoạt động này được hỗ trợ bởi việc đánh giá hiệu quả các biện pháp kiểm soát. Một cách để ước lượng tính hiệu quả của một biện pháp kiểm soát là xem xét khả năng giảm thiểu sự xuất hiện các mối đe dọa và sự dễ dàng trong khai thác các điểm yếu hoặc tác hại của các sự cố. Ban quản lý cần phải soát xét và kiểm toán các báo cáo cũng như cung cấp các thông tin về tính hiệu quả của các biện pháp kiểm soát hiện có.

Các biện pháp kiểm soát đang được lập kế hoạch để triển khai theo kế hoạch triển khai xử lý rủi ro cần được xem xét theo cùng một phương pháp giống như các biện pháp đã được triển khai.

Một biện pháp kiểm soát hiện có hoặc đã có kế hoạch triển khai có thể không hiệu quả, không đầy đủ hoặc không thích đáng. Nếu nhận thấy biện pháp kiểm soát này không đầy đủ hoặc không thích đáng thì cần kiểm tra để xác định có loại bỏ hoặc thay thế biện pháp kiểm soát này bằng các biện pháp kiểm soát khác phù hợp hơn hay giữ nguyên vì một số lý do nào đó (ví dụ như: chi phí).

Các hoạt động sau có thể giúp ích cho việc nhận biết các biện pháp kiểm soát hiện có hoặc đã có kế hoạch:

- Soát xét lại các tài liệu chứa thông tin về các biện pháp kiểm soát (ví dụ: các kế hoạch triển khai xử lý rủi ro). Nếu quy trình quản lý an toàn thông tin được tài liệu hóa tốt thì tất cả các biện pháp kiểm soát hiện có hoặc đã được lập kế hoạch và tình hình triển khai của chúng sẽ có sẵn;
- Phối hợp với người chịu trách nhiệm về an toàn thông tin của tổ chức (như chuyên viên an toàn thông tin, chuyên viên an toàn hệ thống thông tin, cán bộ quản lý tòa nhà hoặc cán bộ quản lý vận hành) và những người sử dụng xem xét biện pháp kiểm soát thực sự được triển khai cho hoạt động xử lý thông tin hoặc hệ thống thông tin;
- Tiến hành soát xét tại chỗ các biện pháp kiểm soát vật lí, đối chiếu những biện pháp kiểm soát đã triển khai với danh sách các biện pháp kiểm soát cần phải thực hiện và kiểm tra tính chính xác và hiệu quả của việc triển khai các biện pháp này; hoặc
- Soát xét các kết quả kiểm toán.

Đầu ra: Một danh sách các biện pháp kiểm soát hiện có hoặc đã được lập kế hoạch triển khai; tình hình triển khai và tình trạng sử dụng các biện pháp kiểm soát này.

### 8.2.5 Nhận biết về điểm yếu

Đầu vào: Một danh sách các mối đe dọa đã biết, danh sách các tài sản và các biện pháp kiểm soát hiện có.

Mô tả: Cần phải nhận biết các điểm yếu mà có thể bị khai thác bởi các mối đe dọa về an toàn thông tin, chúng chính là nguyên nhân gây thiệt hại cho các tài sản hoặc cho tổ chức (liên quan tới TCVN ISO/IEC 27001:2009, xem 4.2.1 d) 3)).

Hướng dẫn triển khai:

Có thể nhận biết các điểm yếu trong các lĩnh vực sau:

- Tổ chức
- Các thủ tục và quy trình
- Thủ tục quản lý
- Nhân sự
- Môi trường vật lí
- Cấu hình hệ thống thông tin
- Phần cứng, phần mềm hoặc thiết bị truyền thông
- Sự phụ thuộc vào các thành phần bên ngoài

Điểm yếu không tự gây ra thiệt hại, mà cần phải có một mối đe dọa khai thác. Một điểm yếu mà không có mối đe dọa tương ứng thì có thể không cần thiết triển khai biện pháp kiểm soát nào, nhưng các thay đổi cần phải được phát hiện và giám sát chặt chẽ. Cần lưu ý, một biện pháp kiểm soát được thực hiện không đúng cách hoặc sai chức năng, hoặc áp dụng không đúng cũng có thể là một điểm yếu. Một biện pháp kiểm soát có thể hiệu quả hoặc không hiệu quả tùy thuộc vào môi trường vận hành. Ngược lại, một mối đe dọa mà không có điểm yếu tương ứng có thể không gây ra một rủi ro.

Các điểm yếu có thể liên quan đến các thuộc tính của tài sản bị sử dụng khác với mục đích và cách thức khi được mua sắm hoặc chế tạo. Cần phải xem xét các điểm yếu phát sinh từ nhiều nguồn khác nhau, ví dụ như từ bản chất bên trong hoặc bên ngoài của tài sản.

Các ví dụ về các điểm yếu và các phương pháp đánh giá điểm yếu được trình bày trong Phụ lục D.

Đầu ra: Một danh sách các điểm yếu liên quan đến các tài sản, các mối đe dọa và các biện pháp kiểm soát; một danh sách các điểm yếu không liên quan đến bất kì mối đe dọa nào đã được nhận biết để soát xét.

### 8.2.6 Nhận biết về hậu quả

Đầu vào: Một danh sách các tài sản, một danh sách các quy trình nghiệp vụ và một danh sách các điểm yếu và các mối đe dọa, có liên quan đến các tài sản và các vấn đề liên quan.

**Hành động**: Cần nhận biết các hậu quả làm mất đi tính bí mật, tính toàn vẹn và tính sẵn sàng đối với các tài sản (xem TCVN ISO/IEC 27001:2009, 4.2.1 d) 4)).

**Hướng dẫn triển khai**:

Một hậu quả có thể là sự mất đi tính hiệu quả, các bất lợi trong điều kiện vận hành, yếu kém trong hoạt động nghiệp vụ, mất uy tín, gây thiệt hại...

Hoạt động này nhằm nhận biết thiệt hại hay hậu quả đối với tổ chức mà có thể nguyên nhân do kịch bản sự cố gây ra. Một kịch bản sự cố là bản mô tả về một mối đe dọa đang khai thác một hoặc một tập hợp các điểm yếu trong một sự cố an toàn thông tin (xem tham khảo điều 13 trong TCVN ISO/IEC 27002:2011). Tác động của các kịch bản sự cố được xác định theo tiêu chí tác động đã được nhận biết trong hoạt động thiết lập bối cảnh. Những tác động này có thể ảnh hưởng tới một hoặc nhiều tài sản mà cũng có thể chỉ trên một phần của tài sản. Do đó, giá trị tài sản có thể được xem xét dựa vào hai khía cạnh: chi phí tài chính và ảnh hưởng của hoạt động nghiệp vụ nếu tài sản bị thiệt hại hoặc bị xâm phạm. Ảnh hưởng này có thể mang tính chất tạm thời hoặc vĩnh viễn như trường hợp tài sản bị phá hủy hoàn toàn.

CHÚ THÍCH: TCVN ISO/IEC 27001:2009 mô tả sự xuất hiện của các kịch bản sự cố là "các lỗi an toàn".

Các tổ chức cần phải nhận biết các hậu quả hoạt động của các kịch bản sự cố về các mặt sau (nhưng không chỉ giới hạn trong những mặt này):

- Việc điều tra nghiên cứu và thời gian khắc phục
- Thời gian (công việc) bị lãng phí
- Cơ hội bị lãng phí
- Sức khỏe và an toàn
- Chi phí tài chính cho từng kĩ năng để khắc phục thiệt hại
- Sự tín nhiệm và danh tiếng.

Chi tiết về đánh giá các điểm yếu thuộc kỹ thuật được trình bày trong Phụ lục B.3 "Đánh giá Tác động".

**Đầu ra**: Một danh sách các kịch bản sự cố cùng với các hậu quả của chúng liên quan đến các tài sản và quy trình nghiệp vụ.

### 8.3 Phân tích rủi ro

#### 8.3.1 Các phương pháp phân tích rủi ro

Phân tích rủi ro có thể được thực hiện theo các mức chi tiết khác nhau phụ thuộc vào mức quan trọng của các tài sản, phạm vi của các điểm yếu đã biết và các sự cố xảy ra trước đây liên quan tới tổ chức. Một phương pháp luận phân tích rủi ro có thể là định lượng hoặc định tính hoặc cả hai, dựa vào từng hoàn cảnh cụ thể. Trong thực tế, phân tích định tính thường được sử dụng đầu tiên để tìm được một biểu thị tổng quan về mức rủi ro và làm bộc lộ các rủi ro chủ yếu. Sau đó, có thể cần thực hiện chi tiết hơn hoặc phân tích định lượng các rủi ro chủ yếu này bởi vì việc thực hiện phân tích định tính thường

ít phức tạp và ít tốn kém hơn so với việc phân tích định lượng. Hình thức phân tích cần phải phù hợp với các tiêu chí ước lượng rủi ro, được phát triển như là một phần của thiết lập bối cảnh.

Chi tiết hơn về hai phương pháp ước lượng được mô tả như sau:

(a) Phương pháp phân tích rủi ro định tính:

Phân tích rủi ro định tính sử dụng một thang đo các thuộc tính chất lượng (thang thuộc tính) để mô tả tính chất nghiêm trọng của các hậu quả tiềm ẩn (ví dụ: Thấp, Trung bình và Cao) và khả năng xảy ra của các hậu quả đó. Ưu điểm của phân tích định tính là giúp các nhân viên có liên quan có thể dễ dàng hiểu được những hậu quả này, trong khi nhược điểm của phương pháp này là sự phụ thuộc vào lựa chọn chủ quan của thang đo thuộc tính.

Các thang đo thuộc tính có thể được thay đổi hoặc điều chỉnh để phù hợp với hoàn cảnh và những mô tả khác nhau có thể được sử dụng cho những rủi ro khác nhau. Phân tích rủi ro định tính có thể được sử dụng:

- Như một hoạt động lọc thô ban đầu để nhận biết những rủi ro, sau đó yêu cầu phân tích chi tiết hơn những rủi ro đó
- Khi mà kiểu phân tích này phù hợp với các quyết định
- Khi mà các dữ liệu số hay tài nguyên số không đủ để thực hiện phân tích rủi ro định lượng

Phân tích định tính cần phải sử dụng các thông tin và dữ liệu thực tế có sẵn.

(b) Phương pháp phân tích rủi ro định lượng:

Phân tích rủi ro định lượng sử dụng thang đo với các giá trị số (thang giá trị số) (chứ không phải là thang mang tính chất mô tả sử dụng trong phân tích rủi ro định tính) cho cả hậu quả và khả năng xảy ra hậu quả. Phân tích rủi ro định lượng sử dụng dữ liệu từ nhiều nguồn khác nhau. Chất lượng của việc phân tích phụ thuộc vào độ chính xác và độ đầy đủ của giá trị số học và giá trị của mô hình đã sử dụng. Trong hầu hết các trường hợp, phân tích rủi ro định lượng thường sử dụng các dữ liệu sự cố trong quá khứ, ưu điểm là có thể liên hệ trực tiếp đến các mục tiêu và mối quan tâm về an toàn thông tin của tổ chức. Nhược điểm của phương pháp này là sự thiếu dữ liệu về các rủi ro mới hoặc các điểm yếu an toàn thông tin. Nhược điểm của phương pháp tiếp cận định lượng xuất hiện khi thiếu các dữ liệu thực tế, có thể kiểm chứng được, từ đó dẫn đến việc tạo ra ảo tưởng về giá trị và tính chính xác của việc đánh giá rủi ro.

Cách thức diễn tả hậu quả và khả năng xảy ra và các cách thức kết hợp hai vấn đề này để tạo ra mức rủi ro sẽ thay đổi theo loại rủi ro và mục đích cho đầu ra của việc đánh giá rủi ro dự tính được sử dụng. Sự không chắc chắn và tính hay thay đổi của cả hậu quả và khả năng xảy ra có thể được xem xét trong quá trình phân tích và truyền thông thông tin một cách hiệu quả.

### 8.3.2 Đánh giá các hậu quả

**Đầu vào**: Một danh sách các kịch bản sự cố liên quan đã được nhận biết, bao gồm nhận biết về các mối đe dọa, các điểm yếu, các tài sản bị ảnh hưởng, những hậu quả đối với tài sản và các quy trình nghiệp vụ.

**Hành động**: Cần phải đánh giá các tác động nghiệp vụ đối với tổ chức mà nguyên nhân gây ra có thể từ những sự cố an toàn thông tin có thể xảy ra hoặc đã xảy ra ở hiện tại và cần phải xem xét các hậu quả do vi phạm an toàn thông tin gây ra như làm ảnh hưởng tới tính bí mật, tính toàn vẹn hay tính sẵn sàng của các tài sản (liên quan tới TCVN ISO/IEC 27001:2009, xem 4.2.1 e) 1)).

**Hướng dẫn triển khai**:

Sau khi nhận biết tất cả các tài sản đang trong quy trình soát xét, các giá trị mà được gắn cho những tài sản này cần phải được xem xét khi đánh giá những hậu quả.

Giá trị tác động nghiệp vụ có thể được thể hiện dưới hai hình thức: mô tả định tính và mô tả định lượng, nhưng nói chung bất kì phương pháp đánh giá giá trị tiền tệ nào cũng có thể cung cấp thêm nhiều thông tin cho việc đưa ra quyết định và do vậy tạo điều kiện thuận lợi cho một quy trình ra quyết định thêm hiệu quả hơn.

Định giá tài sản bắt đầu với việc phân loại các tài sản theo mức rủi ro của tài sản, tầm quan trọng của tài sản đối với việc hoàn thành các mục tiêu nghiệp vụ của tổ chức. Sau đó, việc định giá tài sản sẽ được xác định bằng cách sử dụng hai phương pháp:

- Giá trị thay thế của tài sản, gồm: chi phí khôi phục thông tin và chi phí thay thế thông tin
- Các hậu quả nghiệp vụ do làm mất mát hoặc gây tổn hại tới tài sản, như nghiệp vụ bất lợi tiềm ẩn và/hoặc các hậu quả về pháp lý hay quy định từ sự tiết lộ, thay đổi, tính không sẵn sàng và/hoặc sự phá hoại thông tin và những tài sản thông tin khác

Việc định giá này có thể được xác định từ quy trình phân tích tác động nghiệp vụ. Giá trị mà được xác định bằng hậu quả nghiệp vụ thường cao hơn đáng kể so với chi phí thay thế đơn giản, tùy thuộc vào tầm quan trọng của tài sản đối với tổ chức trong việc đáp ứng các mục tiêu nghiệp vụ của tổ chức đó.

Định giá tài sản là một bước quan trọng trong việc đánh giá tác động của một kịch bản sự cố, bởi vì sự cố có thể ảnh hưởng tới nhiều hơn một tài sản (chẳng hạn như các tài sản phụ thuộc) hoặc chỉ một phần của một tài sản. Các mối đe dọa và điểm yếu khác nhau sẽ có các tác động khác nhau đối với các tài sản, như làm mất đi tính bí mật, tính toàn vẹn hoặc tính sẵn sàng. Vì vậy, việc đánh giá các hậu quả có liên quan đến định giá tài sản dựa trên các phân tích tác động nghiệp vụ.

Các hậu quả hoặc tác động nghiệp vụ có thể được xác định bằng việc mô hình hóa các kết quả của một hoặc một tập hợp các sự kiện, hoặc ngoại suy từ các nghiên cứu thực nghiệm hoặc từ các dữ liệu trong quá khứ.

Các hậu quả có thể được thể hiện theo các tiêu chí tác động về tiền tệ, kỹ thuật hoặc con người, hoặc các tiêu chí khác liên quan đến tổ chức. Trong một số trường hợp, yêu cầu phải có nhiều giá trị số học

để xác định những hậu quả cho những thời điểm, địa điểm, các nhóm hoặc những tình trạng khác nhau.

Các hậu quả về thời gian và tài chính cần phải được đánh giá với cùng một phương pháp tiếp cận được sử dụng để đánh giá khả năng xảy ra mối đe dọa và điểm yếu. Tính nhất quán phải được duy trì trong các phương pháp tiếp cận định tính hay định lượng.

Chi tiết thông tin về định giá tài sản và đánh giá tác động được trình bày trong Phụ lục B.

Đầu ra: Một danh sách các hậu quả của một kịch bản sự cố đã được diễn tả theo tài sản và tiêu chí tác động.

### 8.3.3 Đánh giá khả năng xảy ra sự cố

Đầu vào: Một danh sách các kịch bản sự cố liên quan đã được nhận biết, bao gồm nhận biết về các mối đe dọa, các tài sản bị ảnh hưởng, các điểm yếu bị khai thác và các hậu quả đối với các tài sản và các quy trình nghiệp vụ. Hơn nữa, còn bao gồm các danh sách tất cả các biện pháp kiểm soát hiện có và đã lên kế hoạch triển khai, tính hiệu quả của những biện pháp kiểm soát đó, tình hình triển khai và tình trạng sử dụng các biện pháp kiểm soát này.

Hành động: Khả năng xảy ra của các kịch bản sự cố cần phải được đánh giá (liên quan đến TCVN ISO/IEC 27001:2009, xem 4.2.1 e) 2)).

Hướng dẫn triển khai

Sau khi nhận biết được các kịch bản sự cố thì cần thiết phải đánh giá khả năng xảy ra của từng kịch bản và tác động đang xảy ra, sử dụng các kỹ thuật phân tích định lượng hay định tính. Cần chú ý đến tần suất xuất hiện của các mối đe dọa và cách thức các điểm yếu có thể bị khai thác dễ dàng, xem xét:

- Kinh nghiệm và các số liệu thống kê có thể áp dụng được đối với khả năng xuất hiện mối đe dọa.
- Đối với các nguồn đe dọa có chủ ý: động cơ và khả năng, sẽ thay đổi theo thời gian và các nguồn lực sẵn có của kẻ tấn công, cũng như nhận thức về sự hấp dẫn và điểm yếu của các tài sản đối với kẻ tấn công
- Đối với các nguồn đe dọa khách quan: các yếu tố địa lý, ví dụ như gần nhà máy hóa chất hoặc xăng dầu, điều kiện thời tiết khắc nghiệt và các yếu tố có thể ảnh hưởng đến lỗi của con người và lỗi trang thiết bị
- Các điểm yếu đơn lẻ và tích hợp
- Các biện pháp kiểm soát hiện có và sự hiệu quả của chúng trong việc giảm thiểu các điểm yếu

Ví dụ, một hệ thống thông tin có thể có một điểm yếu đối với các mối đe dọa về giả mạo danh tính người dùng và lạm dụng các tài nguyên. Điểm yếu về giả mạo danh tính người dùng có khả năng xảy ra cao bởi vì sự thiếu xác thực của người dùng. Trái lại, khả năng lạm dụng các tài nguyên có thể xảy ra thấp mặc dù sự thiếu xác thực của người sử dụng, bởi vì cách lạm dụng tài nguyên chỉ có giới hạn.

Tùy thuộc vào sự cần thiết về sự chính xác, các tài sản có thể được nhóm lại, hoặc có thể cần thiết để phân tách tài sản theo từng thành phần của chúng kết nối các kịch bản vào những thành phần này. Ví dụ, dọc theo các vị trí địa lý, bản chất của những mối đe dọa đối với cùng loại tài sản có thể thay đổi, hoặc tính hiệu quả của những biện pháp kiểm soát hiện có có thể biến đổi.

**Đầu ra**: Khả năng xảy ra của các kịch bản sự cố (định lượng hoặc định tính).

### 8.3.4 Xác định mức rủi ro

**Đầu vào**: Một danh sách các kịch bản sự cố cùng với các hậu quả liên quan đến các tài sản và các quy trình nghiệp vụ và khả năng xảy ra các kịch bản đó (định tính hay định lượng).

**Hành động**: Cần phải xác định mức rủi ro cho tất cả các kịch bản sự cố (liên quan tới TCVN ISO/IEC 27001:2009, xem 4.2.1 e)) 4)).

**Hướng dẫn triển khai**:

Phân tích rủi ro sẽ định rõ giá trị cho khả năng xảy ra và những hậu quả của một rủi ro. Các giá trị này có thể là định tính hay định lượng. Phân tích rủi ro được dựa trên các hậu quả đã được đánh giá và khả năng xảy ra. Thêm vào đó, chúng ta cần phải xem xét đến lợi ích về chi phí, các mối quan tâm của những bên liên quan và những biến đổi khác, như sự phù hợp đối với ước lượng rủi ro. Rủi ro được đánh giá là sự kết hợp giữa khả năng xảy ra của một kịch bản sự cố với các hậu quả.

Các ví dụ về những phương pháp tiếp cận hoặc phương pháp phân tích rủi ro an toàn thông tin khác nhau được trình bày trong Phụ lục E.

**Đầu ra**: Một danh sách các rủi ro cùng với các mức giá trị được định rõ.

## 8.4 Ước lượng rủi ro

**Đầu vào**: Một danh sách các rủi ro cùng với các mức giá trị được định rõ và các tiêu chí ước lượng rủi ro.

**Hành động**: Mức rủi ro được đối chiếu dựa vào các tiêu chí ước lượng rủi ro và các tiêu chí chấp nhận rủi ro (liên quan tới TCVN ISO/IEC 27001:2009, xem 4.2.1 e) 4)).

**Hướng dẫn triển khai**:

Bản chất của các quyết định gắn liền với ước lượng rủi ro và các tiêu chí ước lượng rủi ro sẽ được sử dụng để đưa ra những quyết định sẽ được quyết định khi thiết lập bối cảnh. Những quyết định và bối cảnh này cần phải được xem xét lại chi tiết hơn ở bước này khi đã có thêm thông tin về các rủi ro cụ thể đã được nhận biết. Để ước lượng các rủi ro, các tổ chức cần đối chiếu các rủi ro đã được ước đoán (sử dụng các phương pháp hoặc phương pháp tiếp cận đã được chọn như được nêu trong Phụ lục E) với các tiêu chí ước lượng rủi ro được vạch rõ trong suốt quy trình thiết lập bối cảnh.

Các tiêu chí ước lượng rủi ro được sử dụng để đưa ra quyết định cần phải phù hợp với bối cảnh quản lý rủi ro an toàn thông tin trong nội bộ và bên ngoài tổ chức, đồng thời phải xem xét đến các mục tiêu của tổ chức và các quan điểm của các bên liên quan... Các quyết định được thực hiện trong hoạt động

ước lượng rủi ro được dựa vào chủ yếu là mức rủi ro có thể chấp nhận được. Tuy nhiên, cũng cần phải xem xét các hậu quả, khả năng xảy ra và mức tin tưởng trong nhận biết và phân tích rủi ro. Sự kết hợp của các rủi ro thấp và trung bình có thể tạo ra các rủi ro có mức nguy hiểm cao hơn nhiều và cần có biện pháp giải quyết phù hợp.

Xem xét cần phải bao gồm:

- *Các tính chất của an toàn thông tin*: nếu một tiêu chí không liên quan đến tổ chức (ví dụ như mất tính bí mật), thì tất cả các rủi ro tác động đến tiêu chí này có thể cũng không liên quan
- *Sự quan trọng của quy trình nghiệp vụ hoặc các hoạt động được hỗ trợ bởi một tài sản cụ thể hoặc tập hợp các tài sản*: nếu quy trình được xác định là ít quan trọng, các rủi ro liên quan có thể được xem xét ở mức quan tâm thấp hơn so với các rủi ro mà có nhiều quy trình hay hoạt động bị tác động hơn

Ước lượng rủi ro sử dụng những hiểu biết về rủi ro thu được từ phân tích rủi ro để đưa ra quyết định cho các hành động trong tương lai. Các quyết định cần bao gồm:

- Liệu một hoạt động cần được tiến hành hay không
- Các ưu tiên đối với việc xử lý rủi ro xét theo các mức rủi ro đã được đánh giá

Trong suốt giai đoạn ước lượng rủi ro, các yêu cầu về hợp đồng, về pháp lý và quy định là các yếu tố cần phải được xem xét bổ sung thêm vào các rủi ro đã được đánh giá.

Đầu ra: Một danh sách các rủi ro đã được sắp xếp ưu tiên theo các tiêu chí ước lượng rủi ro liên quan đến các kịch bản sự cố mà dẫn đến các rủi ro đó.

## 9 Xử lý rủi ro an toàn thông tin

### 9.1 Mô tả chung về xử lý rủi ro

Đầu vào: Một danh sách các rủi ro đã được phân loại ưu tiên theo các tiêu chí ước lượng rủi ro liên quan đến các kịch bản sự cố mà dẫn đến các rủi ro đó.

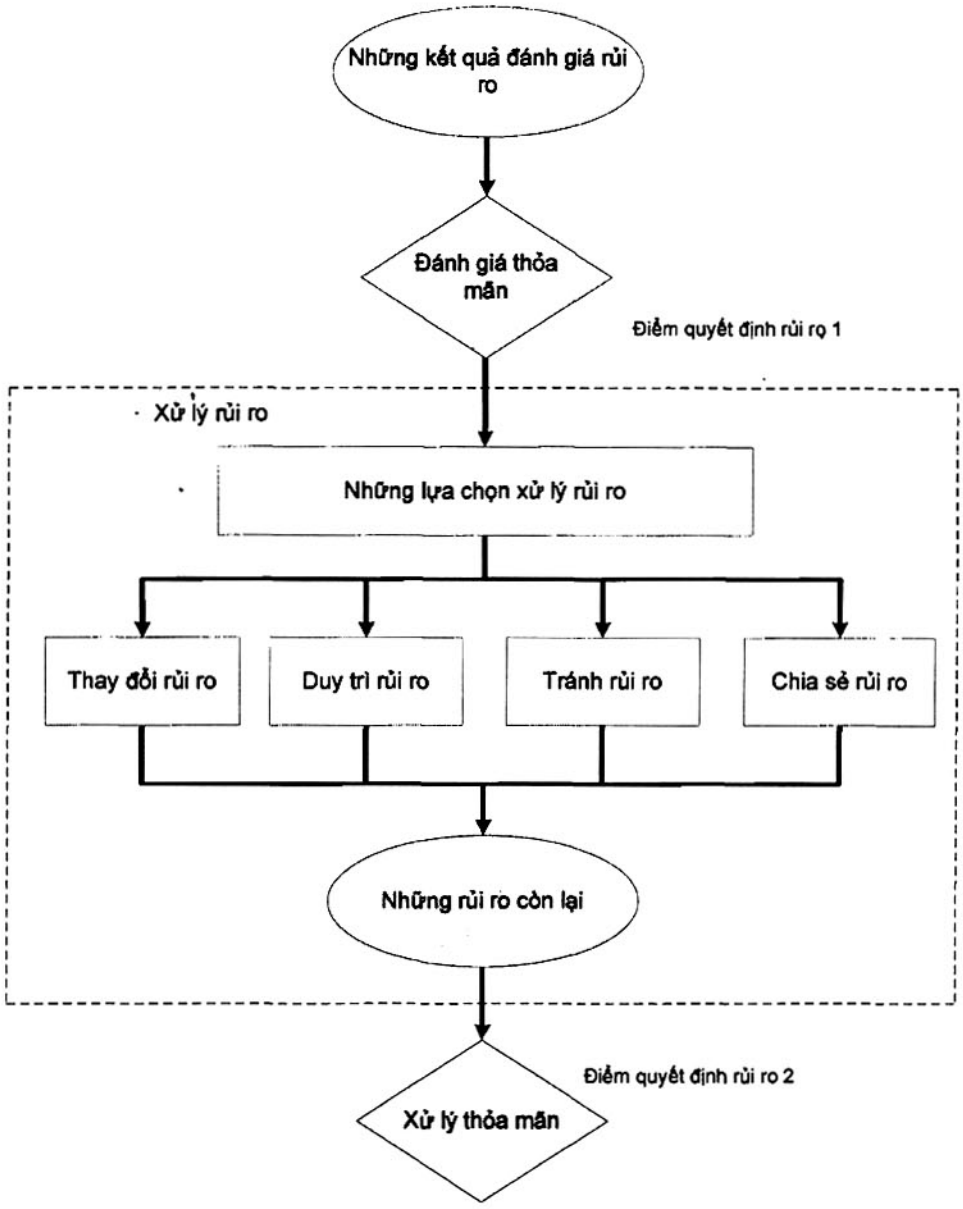
Hành Động: Cần phải lựa chọn các biện pháp kiểm soát để giảm thiểu, duy trì, ngăn ngừa, hoặc chia sẻ những rủi ro và xác định một kế hoạch xử lý rủi ro.

Hướng dẫn triển khai:

Có bốn phương án lựa chọn sẵn có cho việc xử lý rủi ro là: thay đổi rủi ro (9.2), duy trì rủi ro (9.3), ngăn ngừa rủi ro (9.4) và chia sẻ rủi ro (9.5).

CHÚ THÍCH: xem 4.2.1. f) 2) trong TCVN ISO/IEC 27001:2009 sử dụng thuật ngữ "chấp nhận rủi ro" thay cho thuật ngữ "duy trì rủi ro".

Hình 3 minh họa hoạt động xử lý rủi ro trong quy trình quản lý rủi ro an toàn thông tin như đã được trình bày trong Hình 2.




**Hình 3 – Hoạt động xử lý rủi ro**

Những lựa chọn xử lý rủi ro cần phải được chọn lựa dựa trên kết quả của đánh giá rủi ro, chi phí mong muốn cho triển khai các lựa chọn này và các lợi ích mong muốn xuất phát từ những lựa chọn đó.

Cần phải triển khai những lựa chọn khi đạt được những giảm thiểu lớn về rủi ro với chi phí tương đối thấp. Những lựa chọn bổ sung để nâng cấp có thể không mang lại giá trị kinh tế và cần thiết phải thực hiện việc đánh giá để xem xét liệu những lựa chọn đó có hợp lí hay không.

Nhìn chung, những hậu quả tiêu cực của rủi ro cần phải làm thấp đến mức thích hợp và không phân biệt bất kỳ tiêu chí tuyệt đối nào. Những người quản lý cũng cần phải xem xét những rủi ro ít khi xảy ra

nhưng lại là những rủi ro nghiêm trọng. Trong những trường hợp này, các biện pháp kiểm soát mà không hoàn toàn phù hợp với hoàn cảnh kinh tế vẫn cần được triển khai (ví dụ như các biện pháp kiểm soát liên tục trong nghiệp vụ được xem xét để biện pháp kiểm soát các rủi ro mức cao).

Bốn lựa chọn cho việc xử lý rủi ro không loại trừ lẫn nhau. Đôi khi tổ chức có thể được lợi chắc chắn bởi sự kết hợp những lựa chọn như giảm thiểu khả năng xảy ra rủi ro, giảm thiểu hậu quả rủi ro và chia sẻ hoặc duy trì bất kì rủi ro tồn đọng nào.

Một vài xử lý rủi ro có thể giải quyết một cách hiệu quả nhiều rủi ro (ví dụ như đào tạo và nhận thức an toàn thông tin). Một kế hoạch xử lý rủi ro cần phải nhận biết rõ ràng thứ tự ưu tiên để triển khai xử lý rủi ro theo thời gian định sẵn. Các ưu tiên có thể được thiết lập bằng việc sử dụng các kỹ thuật khác nhau, bao gồm xếp loại các rủi ro và phân tích chi phí - lợi nhuận. Đó là trách nhiệm của những người quản lý của tổ chức để quyết định sự cân đối giữa chi phí triển khai các biện pháp kiểm soát với phân bổ ngân sách.

Việc nhận biết các biện pháp kiểm soát hiện có có thể xác định được các biện pháp kiểm soát đó có vượt quá nhu cầu hiện tại hay không, về mặt đối chiếu chi phí, bao gồm cả duy trì. Nếu có xem xét loại bỏ những biện pháp kiểm soát dư thừa hoặc không cần thiết (đặc biệt nếu những biện pháp kiểm soát này có chi phí duy trì cao), những yếu tố về chi phí và an toàn thông tin cần phải được quan tâm. Do các biện pháp kiểm soát có thể ảnh hưởng lẫn nhau, việc loại bỏ các biện pháp kiểm soát dư thừa có thể làm giảm an toàn tổng thể. Thêm vào đó, chi phí có thể sẽ thấp hơn khi vẫn để lại những biện pháp kiểm soát dư thừa hoặc không cần thiết hơn là loại bỏ chúng.

Những lựa chọn xử lý rủi ro có thể quan tâm đến:

- Các bên bị ảnh hưởng nhận thức rủi ro như thế nào
- Cách thích hợp nhất để truyền thông giữa các bên liên quan

Thiết lập bối cảnh (7.2 – Tiêu chí ước lượng rủi ro) sẽ cung cấp những thông tin về các yêu cầu về luật pháp và quy định để tổ chức phải tuân thủ. Rủi ro đối với tổ chức là thất bại trong việc tuân thủ và vì vậy cần phải triển khai các lựa chọn xử lý để giới hạn khả năng xảy ra rủi ro đối với tổ chức. Toàn bộ ràng buộc về mặt tổ chức, kỹ thuật, cấu trúc... đã được nhận biết trong suốt quá trình hoạt động thiết lập bối cảnh cần phải được xem xét trong suốt quy trình xử lý rủi ro.

Một khi kế hoạch xử lý rủi ro được vạch rõ, những rủi ro tồn đọng cũng phải được xác định. Điều này liên quan tới việc cập nhật hoặc lặp lại chu trình đánh giá rủi ro, xem xét những tác động mong muốn của việc xử lý rủi ro đã được đề xuất. Nếu những rủi ro tồn đọng vẫn chưa đáp ứng được các tiêu chí chấp nhận rủi ro của tổ chức, cần thiết phải có thêm một chu trình lặp lại của việc đánh giá rủi ro trước khi đi đến quy trình chấp nhận rủi ro. Thông tin chi tiết được trình bày theo 3.2 trong TCVN ISO/IEC 27002:2011.

Đầu ra: Kế hoạch xử lý rủi ro và những rủi ro tồn đọng tùy thuộc vào quyết định chấp nhận của ban quản lý của tổ chức.

### 9.2 Thay đổi rủi ro

**Hành động**: Mức rủi ro cần phải được quản lý bằng cách đưa ra, loại bỏ hoặc thay thế các biện pháp kiểm soát sao cho các rủi ro tồn đọng có thể được đánh giá lại là chấp nhận được.

**Hướng dẫn triển khai**:

Cần phải lựa chọn các biện pháp kiểm soát thích hợp và đã được minh chứng để đáp ứng những yêu cầu đã được nhận biết bằng việc đánh giá và xử lý rủi ro. Lựa chọn này phải chú ý tới các tiêu chí chấp nhận rủi ro cũng như những yêu cầu về luật pháp, quy định và các yêu cầu theo hợp đồng. Lựa chọn này cần phải xem xét tới chi phí và thời gian triển khai các biện pháp kiểm soát, hoặc các khía cạnh kỹ thuật, môi trường và văn hóa. Nếu những biện pháp kiểm soát an toàn thông tin được lựa chọn một cách đúng đắn thì có thể giảm được toàn bộ chi phí cho các bên sở hữu cùng một hệ thống.

Nói chung, các biện pháp kiểm soát có thể cung cấp một hoặc nhiều loại bảo vệ như sau: hiệu chỉnh, loại bỏ, phòng ngừa, giảm thiểu tác động, ngăn chặn, phát hiện, khôi phục, giám sát và nâng cao nhận thức. Trong suốt quá trình lựa chọn biện pháp kiểm soát, điều quan trọng là phải cân nhắc chi phí để có được, triển khai, quản trị, vận hành, giám sát và duy trì các biện pháp kiểm soát so với giá trị tài sản được bảo vệ. Hơn nữa, lợi nhuận đầu tư do giảm thiểu rủi ro và tiềm năng khai thác những cơ hội nghiệp vụ mới được tạo ra bởi những biện pháp kiểm soát cụ thể cũng cần phải được xem xét. Ngoài ra, cần xem xét đến các kĩ năng chuyên môn cần thiết để nhận biết và triển khai những biện pháp kiểm soát mới hoặc sửa đổi những biện pháp kiểm soát hiện có

TCVN ISO/IEC 27002:2011 cung cấp những hướng dẫn và thông tin chi tiết về các biện pháp kiểm soát.

Có nhiều ràng buộc mà có thể ảnh hưởng tới việc lựa chọn những biện pháp kiểm soát. Những ràng buộc về kỹ thuật như các yêu cầu thực hiện, khả năng quản lý (các yêu cầu hỗ trợ vận hành) và các vấn đề về tính tương thích có thể ngăn cản việc sử dụng các biện pháp kiểm soát hoặc gây ra do lỗi của con người hoặc vô hiệu hóa các biện pháp kiểm soát, dẫn đến nhận thức sai về an toàn hoặc thậm chí làm tăng rủi ro cao đến mức vượt quá tầm kiểm soát (ví dụ như yêu cầu những mật khẩu phức tạp mà thiếu hướng dẫn phù hợp cho người dùng khi đặt mật khẩu). Hơn thế nữa, có thể xảy ra trường hợp biện pháp kiểm soát làm ảnh hưởng tới thực hiện. Những người quản lý phải cố gắng nhận biết một giải pháp để làm thỏa đáng các yêu cầu thực hiện thích hợp trong khi vẫn đảm bảo tốt an toàn thông tin. Kết quả của bước này là một danh sách các biện pháp kiểm soát có thể thực hiện được, với chi phí, lợi ích và mức ưu tiên triển khai của những biện pháp kiểm soát đó.

Những ràng buộc khác nhau phải được xem xét đến khi lựa chọn các biện pháp kiểm soát và trong suốt quy trình triển khai. Điển hình cần quan tâm đến:

- Ràng buộc về thời gian
- Ràng buộc về tài chính
- Ràng buộc về kỹ thuật
- Ràng buộc về vận hành

- Ràng buộc về văn hóa
- Ràng buộc về đạo đức
- Ràng buộc về môi trường
- Ràng buộc về luật pháp
- Sự dễ dàng sử dụng
- Ràng buộc về nhân sự
- Ràng buộc về khả năng hợp nhất giữa các biện pháp kiểm soát mới và các biện pháp kiểm soát hiện có

Thông tin chi tiết về những ràng buộc để thay đổi rủi ro có thể tìm thấy trong Phụ lục F.

### 9.3 Duy trì rủi ro

Hành động: Dựa vào ước lượng rủi ro để ra quyết định giữ lại rủi ro mà không cần thêm bất kì hành động nào nữa.

CHÚ THÍCH: xem 4.2.1 f) 2) của TCVN ISO/IEC 27001:2009 "chấp nhận rủi ro một cách khách quan hay chủ quan với điều kiện chúng hoàn toàn đáp ứng các chính sách và tiêu chí chấp nhận rủi ro của tổ chức" mô tả hoạt động tương tự.

Hướng dẫn triển khai:

Nếu mức rủi ro đáp ứng được các tiêu chí chấp nhận rủi ro thì không cần thực hiện thêm bất kì biện pháp kiểm soát nào và rủi ro có thể được giữ lại.

### 9.4 Tránh rủi ro

Hành động: Cần phải tránh những hoạt động hay hoàn cảnh làm phát sinh các rủi ro.

Hướng dẫn triển khai:

Khi rủi ro được nhận biết ở mức quá cao, hoặc các chi phí triển khai những lựa chọn xử lý rủi ro vượt quá lợi ích, cần phải đưa ra quyết định để tránh hoàn toàn rủi ro, bằng cách rút lại hoạt động hay những hoạt động hiện có hoặc đã được lập kế hoạch, hoặc thay đổi các điều kiện mà theo đó hoạt động được vận hành. Ví dụ, với những rủi ro mà do tự nhiên gây ra thì phương án thay thế hiệu quả nhất là chuyển những phương tiện xử lý thông tin đến nơi rủi ro không tồn tại hoặc nơi có thể kiểm soát/quản lý được.

### 9.5 Chia sẻ rủi ro

Hành động: Rủi ro có thể được chia sẻ với các bên khác, các bên mà có thể quản lý một cách hiệu quả nhất những rủi ro cụ thể tùy thuộc vào quy trình ước lượng rủi ro.

Hướng dẫn triển khai:

Chia sẻ rủi ro là quyết định chia sẻ những rủi ro nào đó với các bên bên ngoài tổ chức. Chia sẻ rủi ro có thể tạo ra những rủi ro mới hoặc làm thay đổi những rủi ro hiện có, đã được nhận biết. Do đó, việc xử lý rủi ro bổ sung là cần thiết.

Chia sẻ có thể được thực hiện bởi sự bảo đảm sẽ hỗ trợ giải quyết những hậu quả rủi ro, hoặc bằng hợp đồng phụ với một đối tác khác, đối tác này sẽ có vai trò giám sát hệ thống thông tin và có hành động ngay lập tức để ngăn chặn kẻ tấn công trước khi chúng gây ra một thiệt hại nhất định.

Cần lưu ý có thể chia sẻ trách nhiệm quản lý rủi ro nhưng sẽ không bình thường nếu chia sẻ trách nhiệm pháp lý đối với một tác động. Khách hàng sẽ thường quy cho việc xuất hiện một tác động bất lợi là do lỗi của tổ chức.

## 10 Chấp nhận rủi ro an toàn thông tin

**Đầu vào**: Kế hoạch xử lý rủi ro và việc đánh giá rủi ro tồn đọng (tức là rủi ro chưa được xử lý hoàn toàn) tùy thuộc vào quyết định chấp nhận của những người quản lý của tổ chức.

**Hành động**: Quyết định để chấp nhận rủi ro và các trách nhiệm đối với quyết định phải được đưa ra và cần phải ghi chép một cách chính thức (vấn đề này liên quan tới TCVN ISO/IEC 27001:2009, xem 4.2.1 h)).

**Hướng dẫn triển khai**:

Các kế hoạch xử lý rủi ro cần phải mô tả được những rủi ro đã được đánh giá được xử lý thế nào để đáp ứng được các tiêu chí chấp nhận rủi ro (xem 7.2 Tiêu chí chấp nhận rủi ro). Điều quan trọng là những người quản lý có trách nhiệm phải xem xét và phê chuẩn các kế hoạch xử lý rủi ro đã được đề xuất và những rủi ro tồn đọng còn lại và ghi chép lại bất kì điều kiện nào có liên quan đến sự phê chuẩn này.

Tiêu chí chấp nhận rủi ro có thể phức tạp hơn so với chỉ xác định xem liệu một rủi ro tồn đọng có nằm trên hoặc dưới một ngưỡng đơn nào đó không

Trong một số trường hợp, mức rủi ro tồn đọng không phù hợp với các tiêu chí chấp nhận rủi ro bởi vì các tiêu chí đang được áp dụng này không xem xét các hoàn cảnh thông thường. Ví dụ: có thể thảo luận để chấp nhận rủi ro vì những lợi ích đi kèm rủi ro rất hấp dẫn, hoặc vì chi phí để thay đổi rủi ro lại quá cao. Những trường hợp trên có thể kết luận các tiêu chí chấp nhận rủi ro là không đầy đủ và cần được xem xét lại nếu có thể. Tuy nhiên, không phải lúc nào cũng có thể xem xét lại các tiêu chí chấp nhận rủi ro một cách kịp thời. Trong trường hợp này, người đưa ra quyết định có thể phải chấp nhận rủi ro mặc dù chúng không đáp ứng được tiêu chí chấp nhận thông thường. Nếu cần thiết thì người ra quyết định nên giải thích rõ ràng cho mỗi rủi ro và có thể đưa ra những chứng minh cho quyết định đó để loại tiêu chí chấp nhận rủi ro thông thường ra một bên.

**Đầu ra**: Một danh sách các rủi ro đã được chấp nhận với các chứng minh đi kèm nếu các rủi ro này không đáp ứng được các tiêu chí chấp nhận rủi ro thông thường của tổ chức.

## 11 Truyền thông và tư vấn rủi ro an toàn thông tin

**Đầu vào**: Toàn bộ thông tin rủi ro thu được từ các hoạt động quản lý rủi ro (xem Hình 2).

Hoạt động: Thông tin về rủi ro phải được truyền thông và/hoặc chia sẻ giữa người ra quyết định và các bên liên quan khác.

Hướng dẫn triển khai:

Truyền thông rủi ro là một hoạt động nhằm đạt được sự nhất trí giữa các bên tham gia về việc làm thế nào để quản lý những rủi ro bằng việc truyền thông và/hoặc chia sẻ thông tin về rủi ro giữa người ra quyết định và các bên liên quan khác. Các thông tin này bao gồm, nhưng không bị giới hạn về tính tồn tại, tính tự nhiên, hình thức, khả năng xảy ra, mức nghiêm trọng, cách xử lý và khả năng chấp nhận rủi ro.

Truyền thông hiệu quả giữa các bên liên quan là quan trọng vì truyền thông có thể có một tác động quan trọng vào việc đưa ra các quyết định cần thiết. Truyền thông sẽ đảm bảo người chịu trách nhiệm của đã đưa ra triển khai quản lý rủi ro và người có quyền lợi cá nhân sẽ hiểu được cơ sở của các quyết định và tại sao cần thiết phải có các hành động cụ thể. Truyền thông có tính hai chiều.

Nhận thức về rủi ro có thể thay đổi do sự khác nhau trong các giả thiết, khái niệm và nhu cầu, các vấn đề và các mối quan tâm của các bên có liên quan đến rủi ro hoặc các vấn đề đang được thảo luận. Các bên liên quan có thể quyết định chấp nhận rủi ro dựa vào nhận thức của họ về rủi ro. Điều này đặc biệt quan trọng để đảm bảo rằng nhận thức về rủi ro của các bên liên quan, cũng như nhận thức của họ về các lợi ích, có thể được nhận biết và được tài liệu hóa và những lý do cơ bản đã được hiểu và được giải quyết một cách rõ ràng.

Truyền thông rủi ro cần phải được tiến hành để đạt được những điều sau:

- Cung cấp sự đảm bảo cho kết quả quản lý rủi ro của tổ chức
- Thu thập thông tin về rủi ro
- Chia sẻ những kết quả từ hoạt động đánh giá rủi ro và đưa ra kế hoạch xử lý rủi ro
- Ngăn ngừa và giảm thiểu sự cố và hậu quả có thể xảy ra của việc vi phạm an toàn thông tin do sự thiếu hiểu biết lẫn nhau giữa người ra quyết định và các bên liên quan
- Hỗ trợ cho việc ra quyết định
- Thu được những hiểu biết mới về an toàn thông tin
- Phối hợp với các bên khác và lập kế hoạch đáp ứng kịp thời nhằm giảm thiểu các hậu quả từ bất kỳ sự cố nào
- Đưa ra ý thức trách nhiệm về rủi ro cho người ra quyết định và các bên liên quan
- Nâng cao nhận thức

Một tổ chức cần phải phát triển các kế hoạch truyền thông rủi ro cho các trường hợp vận hành thông thường cũng như cho các trường hợp khẩn cấp. Vì vậy, hoạt động truyền thông rủi ro phải được thực hiện liên tục và thường xuyên.

Sự phối hợp giữa người ra quyết định chính với các bên liên quan có thể đạt được bằng cách thành lập một ủy ban để tranh luận về những rủi ro, thứ tự ưu tiên của chúng và cách xử lý thích hợp và việc chấp nhận có thể xảy ra.

Một điều quan trọng là phải hợp tác với đơn vị quan hệ công chúng hoặc với đơn vị truyền thông thích hợp trong phạm vi của tổ chức nhằm điều phối tất cả các nhiệm vụ liên quan đến truyền thông rủi ro. Điều này rất quan trọng trong hoạt động truyền thông về khủng hoảng, ví dụ như để đáp ứng với các sự cố cụ thể.

**Đầu ra**: Sự hiểu biết liên tục về quy trình và các kết quả của việc quản lý rủi ro an toàn thông tin của tổ chức.

## 12 Giám sát và soát xét rủi ro an toàn thông tin

### 12.1 Giám sát và soát xét các yếu tố rủi ro

**Đầu vào**: Tất cả các thông tin rủi ro thu được từ những hoạt động quản lý rủi ro (xem Hình 2).

**Hành động**: Rủi ro và các yếu tố rủi ro (như giá trị của các tài sản, những tác động, các mối đe dọa, những điểm yếu, khả năng xảy ra rủi ro) cần phải được giám sát và soát xét để nhận biết bất kì sự thay đổi nào trong bối cảnh của tổ chức ở giai đoạn đầu và để duy trì một tổng thể về bức tranh rủi ro hoàn chỉnh.

**Hướng dẫn triển khai**:

Các rủi ro là không ổn định. Các mối đe dọa, những điểm yếu, khả năng xảy ra hoặc những hậu quả có thể thay đổi bất ngờ mà không có bất kì dấu hiệu nào. Do đó, việc kiểm tra liên tục là cần thiết để phát hiện những thay đổi này. Điều này có thể được hỗ trợ bởi các dịch vụ bên ngoài, những dịch vụ mà cung cấp các thông tin về các mối đe dọa mới hay những điểm yếu.

Các tổ chức cần phải đảm bảo những điều sau phải được kiểm tra liên tục:

- Các tài sản mới đã được đưa vào trong phạm vi quản lý rủi ro
- Những sự thay đổi cần thiết đối với giá trị của tài sản, ví dụ như do những yêu cầu về nghiệp vụ bị thay đổi
- Những mối đe dọa mới mà có thể hoạt động cả bên ngoài và nội bộ tổ chức và vẫn chưa được đánh giá
- Khả năng các điểm yếu mới hoặc gia tăng có thể tạo điều kiện cho các mối đe dọa khai thác các điểm yếu mới hoặc gia tăng này
- Các điểm yếu đã được nhận biết để xác định các điểm yếu đang bị phơi bày cho những mối đe dọa mới hoặc tái xuất hiện
- Tác động tăng lên hay các hậu quả gia tăng của các mối đe dọa, các điểm yếu và những rủi ro tích hợp lại dẫn đến một mức rủi ro không thể chấp nhận được.
- Các sự cố an toàn thông tin

Những mối đe dọa, các điểm yếu hoặc những thay đổi mới về khả năng xảy ra hay những hậu quả có thể làm tăng những rủi ro mà trước đó được đánh giá là thấp. Soát xét các rủi ro ở mức thấp và đã được chấp nhận cần phải xem xét một cách riêng biệt mỗi rủi ro và tất cả các rủi ro này như là một tập hợp, để đánh giá các tác động được tích lũy tiềm ẩn của những rủi ro này. Nếu các rủi ro không rơi vào

loại rủi ro thấp hay rủi ro có thể chấp nhận được thì chúng cần phải được xử lý bằng cách sử dụng một hoặc nhiều tuỳ chọn được xem xét tại điều 9.

Những yếu tố ảnh hưởng đến khả năng xuất hiện và hậu quả của những mối đe dọa xảy ra có thể thay đổi, bởi vì có thể các yếu tố này ảnh hưởng đến tính thích hợp hay chi phí của những lựa chọn xử lý khác nhau. Những thay đổi lớn ảnh hưởng đến tổ chức là lý do để có một sự xem xét cụ thể hơn. Do đó, các hoạt động giám sát rủi ro cần phải được lặp lại một cách thường xuyên và các tùy chọn đã được chọn lọc để xử lý rủi ro phải được xem xét một cách định kỳ.

Kết quả của các hoạt động giám sát rủi ro có thể là đầu vào cho các hoạt động soát xét rủi ro khác. Vì vậy, tổ chức cần phải xem xét tất cả những rủi ro một cách thường xuyên và khi có những thay đổi lớn xảy ra (TCVN ISO/IEC 27001:2009, xem 4.2.3)).

**Đầu ra**: Sự điều chỉnh liên tục của việc quản lý rủi ro với các mục tiêu nghiệp vụ của tổ chức và với các tiêu chí chấp nhận rủi ro.

### 12.2 Giám sát soát xét và cải tiến quản lý rủi ro

**Đầu vào**: Tất cả các thông tin rủi ro thu được từ các hoạt động quản lý rủi ro (xem Hình 2).

**Hành động**: Cần phải giám sát, soát xét và cải tiến liên tục quy trình quản lý rủi ro an toàn thông tin.

**Hướng dẫn triển khai**:

Liên tục giám sát và soát xét là cần thiết để đảm bảo bối cảnh, kết quả của việc đánh giá và xử lý rủi ro, cũng như các kế hoạch quản lý rủi ro vẫn còn có thích đáng và phù hợp với hoàn cảnh.

Tổ chức cần phải chắc chắn quy trình quản lý rủi ro an toàn thông tin và những hoạt động liên quan vẫn còn phù hợp trong hoàn cảnh hiện tại và tương lai sau này. Bất kì sự cải tiến nào đã được chấp nhận cho quy trình hoặc các hành động cần thiết để cải tiến phù hợp với quy trình đó nên được thông báo cho người quản lý thích hợp để đảm bảo không có rủi ro hay yếu tố rủi ro nào bị bỏ qua hoặc bị đánh giá thấp và những hành động cần thiết được thực hiện và các quyết định được đưa ra để cung cấp đầy đủ sự hiểu biết về rủi ro thực tế và khả năng để đáp ứng lại kịp thời.

Ngoài ra, tổ chức cần phải thẩm tra thường xuyên các tiêu chí được sử dụng để đo lường mức rủi ro và các yếu tố của tiêu chí có còn phù hợp với mục tiêu, chiến lược và chính sách nghiệp vụ không và cần phải xem xét một cách đầy đủ những thay đổi đối với bối cảnh nghiệp vụ trong suốt quy trình quản lý rủi ro an toàn thông tin. Hoạt động kiểm tra và soát xét cần phải giải quyết (nhưng không giới hạn):

- Bối cảnh môi trường và pháp lý
- Bối cảnh cạnh tranh
- Phương pháp tiếp cận đánh giá rủi ro
- Các loại tài sản và giá trị tài sản
- Tiêu chí tác động
- Tiêu chí ước lượng rủi ro
- Tiêu chí chấp nhận rủi ro

- Tổng chi phí sở hữu
- Các nguồn lực cần thiết

Tổ chức cần phải đảm bảo các nguồn lực đánh giá và xử lý rủi ro luôn luôn liên tục sẵn sàng để soát xét rủi ro, giải quyết các mối đe dọa hoặc điểm yếu mới hoặc đã bị thay đổi và tư vấn quản lý cho phù hợp.

Giám sát quản lý rủi ro có thể dẫn đến kết quả là sửa đổi hay bổ sung phương pháp tiếp cận, phương pháp luận hoặc những công cụ đã được sử dụng và phụ thuộc vào:

- Những thay đổi đã được nhận biết
- Chu trình lặp đi lặp lại của việc đánh giá rủi ro
- Mục đích của quy trình quản lý rủi ro an toàn thông tin (như quy trình liên tục trong nghiệp vụ, khả năng khôi phục sau sự cố, sự tuân thủ)
- Mục tiêu của quy trình quản lý rủi ro an toàn thông tin (như tổ chức, đơn vị nghiệp vụ, quy trình thông tin, triển khai kỹ thuật, ứng dụng, kết nối internet)

**Đầu ra**: Sự phù hợp liên tục của quy trình quản lý rủi ro an toàn thông tin với mục tiêu nghiệp vụ hoặc sự cập nhật các quy trình của tổ chức.

# Phụ lục A

(Tham khảo)

## Xác định phạm vi và giới hạn của quy trình quản lý rủi ro an toàn thông tin

### A.1 Nghiên cứu về tổ chức

Ước lượng tổ chức: Nghiên cứu về tổ chức là nghiên cứu các yếu tố đặc trưng xác định danh tính của một tổ chức. Đó là: mục đích, nghiệp vụ, nhiệm vụ, giá trị và chiến lược của tổ chức đó. Những vấn đề này phải được nhận biết cùng với các yếu tố đóng góp cho sự phát triển chung (ví dụ như kí kết hợp đồng phụ).

Khó khăn của hoạt động nghiên cứu này là hiểu được một cách chính xác tổ chức được cấu trúc như thế nào. Việc nhận biết cấu trúc thực tế của tổ chức sẽ giúp cho chúng ta hiểu rõ thêm về vai trò và tầm quan trọng của mỗi đơn vị trong việc hoàn thành các mục tiêu của tổ chức.

*Ví dụ, trong thực tế việc người quản lý an toàn thông tin báo cáo với người quản lý cấp cao nhất thay vì báo cáo cho những người quản lý công nghệ thông tin có thể thể hiện sự tham gia của người quản lý cấp cao nhất trong an toàn thông tin.*

Mục đích chính của tổ chức: Mục đích chính của một tổ chức có thể được xác định như là lý do tại sao tổ chức tồn tại (về lĩnh vực hoạt động, thị phần...)

Nghiệp vụ của tổ chức: Nghiệp vụ của tổ chức, được xác định bởi các kỹ thuật và hiểu biết của nhân viên, giúp tổ chức hoàn thành các nhiệm vụ của mình. Đây là nét đặc trưng cho lĩnh vực hoạt động của tổ chức và thường tạo nên văn hóa của tổ chức đó.

Nhiệm vụ của tổ chức: Tổ chức đạt được mục đích bằng cách hoàn thành nhiệm vụ của mình. Để nhận biết các nhiệm vụ của tổ chức, các dịch vụ được cung cấp và/hoặc các sản phẩm được sản xuất phải được nhận biết trong mối quan hệ với những người dùng cuối.

Giá trị của tổ chức: Giá trị là các nguyên tắc chính hoặc là một quy tắc quản lý được xác định tốt được áp dụng cho việc thực hiện nghiệp vụ. Các giá trị này có thể liên quan đến nhân sự, các mối quan hệ với các tác nhân bên ngoài (khách hàng...), chất lượng sản phẩm được đáp ứng hoặc dịch vụ được cung cấp.

*Lấy ví dụ về một tổ chức có mục đích là dịch vụ công cộng, có nghiệp vụ là công việc vận chuyển và có nhiệm vụ là đưa và đón trẻ đến trường học. Những giá trị của tổ chức có thể là đúng giờ và tính an toàn trong suốt quá trình đưa đón.*

Cấu trúc của tổ chức: Tổ chức có những kiểu cấu trúc khác nhau như sau:

- Cấu trúc phòng ban: Mỗi phòng ban được đặt dưới sự giám sát của một cán bộ quản lý có trách nhiệm đối với các quyết định về chiến lược, quản trị và vận hành liên quan đến đơn vị.

- Cấu trúc chức năng: Quyền hạn mang tính chức năng được thực thi dựa trên thủ tục, bản chất công việc và đôi khi là các quyết định hoặc kế hoạch (ví dụ: sản phẩm, IT, các nguồn nhân lực, thương mại...).

Chú ý:

- Một phòng ban trong một tổ chức có cấu trúc phòng ban có thể được thiết lập như một cấu trúc chức năng và ngược lại.
- Một tổ chức có thể được nói là có một cấu trúc ma trận nếu tổ chức đó có các yếu tố của cả hai kiểu cấu trúc trên.
- Trong bất kì cấu trúc tổ chức nào đều phải phân biệt các mức sau đây:
  - mức ra quyết định (xác định các định hướng chiến lược);
  - mức lãnh đạo (điều phối và quản lý);
  - mức vận hành (các hoạt động sản xuất và hỗ trợ).

Biểu đồ của tổ chức: Cấu trúc của tổ chức được trình bày theo mô hình biểu đồ tổ chức. Biểu đồ này cần phải nêu bật được phạm vi quản lý và quyền hạn của người lãnh đạo, nhưng cũng phải bao gồm những mối quan hệ khác, mặc dù những mối quan hệ này không dựa vào bất cứ quyền hạn chính thức nào nhưng vẫn phải thể hiện thông tin rõ ràng.

Chiến lược của tổ chức: Yêu cầu phải có một thể hiện chính thức về các nguyên tắc định hướng của tổ chức. Chiến lược của tổ chức sẽ xác định phương hướng và nhu cầu phát triển để mang lại lợi ích từ những vấn đề đang bấp bênh và những thay đổi chính trong kế hoạch của tổ chức.

### A.2 Danh sách các ràng buộc ảnh hưởng đến tổ chức

Cần phải xem xét toàn bộ các ràng buộc ảnh hưởng đến tổ chức và việc xác định định hướng an toàn thông tin của tổ chức đó. Nguồn của các ràng buộc này có thể ở bên trong tổ chức và trong trường hợp này có vài biện pháp kiểm soát vượt quá ràng buộc hoặc ở bên ngoài tổ chức và do đó nói chung là khó có thể thương lượng. Các ràng buộc về nguồn lực (ngân sách, nhân sự) và những ràng buộc khẩn cấp là những ràng buộc quan trọng nhất.

Tổ chức đặt ra các mục tiêu của mình (liên quan đến nghiệp vụ, hành vi của tổ chức...) cam kết theo một đường lối nhất định, có khả năng là trong một thời gian dài. Tổ chức phải xác định mục tiêu mà tổ chức muốn hướng tới và những phương tiện cần thiết để triển khai. Trong quá trình xác định đường lối này, tổ chức cần xem xét đến sự phát triển về kỹ thuật và hiểu biết, những mong muốn được bày tỏ của những người sử dụng, khách hàng... Mục tiêu này có thể được thể hiện dưới dạng vận hành hoặc trong các chiến lược phát triển với mục đích như cắt giảm chi phí vận hành, cải tiến chất lượng dịch vụ...

Các chiến lược này có thể bao gồm cả thông tin và hệ thống thông tin (IS) mà hỗ trợ cho những ứng dụng của hệ thống. Do đó, những đặc điểm liên quan đến danh tính, nhiệm vụ và các chiến lược của tổ chức là những yếu tố cơ bản trong việc phân tích vấn đề bởi vì sự vi phạm của một khía cạnh an toàn

thông tin dẫn đến việc xem xét lại các mục tiêu chiến lược này. Ngoài ra, điều quan trọng là những đề xuất cho các yêu cầu an toàn thông tin vẫn còn phù hợp với các quy tắc, tập quán và các biện pháp đang có hiệu lực trong tổ chức.

Danh sách các ràng buộc bao gồm (nhưng không giới hạn):

Ràng buộc về bản chất chính trị

Là những ràng buộc có liên quan đến các cơ quan hành chính thuộc chính phủ, các tổ chức hiệp hội cộng đồng hoặc khái quát hơn là bất kì tổ chức nào phải áp dụng các quyết định của chính phủ. Chúng thường là những quyết định liên quan đến các định hướng chiến lược hay vận hành được ban hành bởi một cơ quan thuộc chính phủ hoặc cơ quan chịu trách nhiệm trong việc đưa ra quyết định và phải được áp dụng.

*Ví dụ: việc tin học hóa các hóa đơn chứng từ hay các tài liệu quản lý mở đầu cho các vấn đề an toàn thông tin.*

Ràng buộc về bản chất chiến lược

Các ràng buộc có thể nảy sinh từ những thay đổi có kế hoạch hoặc có thể xảy ra đối với cấu trúc hoặc định hướng của tổ chức. Các ràng buộc này được thể hiện trong các kế hoạch chiến lược hoặc vận hành của tổ chức.

*Ví dụ: hoạt động hợp tác quốc tế trong vấn đề chia sẻ những thông tin nhạy cảm có thể đòi hỏi phải có những thỏa thuận liên quan tới sự truyền thông an toàn.*

Ràng buộc về lãnh thổ

Cấu trúc và/hoặc mục đích của tổ chức có thể đưa ra các ràng buộc đặc trưng như sự phân bố về vị trí trên toàn bộ lãnh thổ của quốc gia hoặc ở nước ngoài.

*Ví dụ bao gồm: các dịch vụ bưu chính, đại sứ quán, ngân hàng, các công ty con của một tập đoàn công nghiệp lớn...*

Ràng buộc nảy sinh từ tình hình kinh tế và chính trị

Hoạt động của một tổ chức có thể bị thay đổi sâu sắc bởi những sự kiện cụ thể như các cuộc đình công hoặc các cuộc khủng hoảng trong phạm vi quốc gia và quốc tế.

*Ví dụ: một vài dịch vụ cần có thể tiếp tục duy trì thậm chí trong một khủng hoảng nghiêm trọng.*

Ràng buộc về cấu trúc

Bản chất cấu trúc của một tổ chức (phân chia theo bộ phận, theo chức năng hay loại khác) có thể dẫn tới một chính sách an toàn thông tin cụ thể và tổ chức an toàn phù hợp với cấu trúc.

*Ví dụ: một cấu trúc quốc tế cần phải có khả năng điều hòa các yêu cầu an toàn đặc trưng theo từng nước.*

Ràng buộc về chức năng

Các ràng buộc về chức năng phát sinh trực tiếp từ các nhiệm vụ chung hay riêng của tổ chức.

*Ví dụ: một tổ chức vận hành theo chu trình cần đảm bảo chắc chắn các nguồn lực của tổ chức đó phải luôn luôn sẵn sàng.*

Ràng buộc liên quan đến vấn đề nhân sự

Tính chất của những ràng buộc này thay đổi một cách đáng kể. Chúng bị chi phối bởi: mức trách nhiệm, tuyển dụng, phẩm chất, đào tạo, nhận thức về an toàn, động cơ, sự sẵn sàng...

*Ví dụ: toàn bộ nhân viên của một tổ chức bảo vệ cần phải có thẩm quyền xử lý thông tin mật ở mức cao.*

Ràng buộc nảy sinh từ lịch công tác (thời gian biểu) của tổ chức:

Những ràng buộc này có thể là kết quả từ việc tái cấu trúc hoặc thiết lập những chính sách mới mang tầm quốc gia hoặc quốc tế trong những thời hạn nhất định.

*Ví dụ: việc tạo ra một bộ phận an toàn.*

Ràng buộc liên quan tới phương pháp

Các phương pháp phù hợp với tri thức của tổ chức sẽ cần được áp dụng cho khía cạnh như là lập kế hoạch dự án, hướng dẫn kỹ thuật, sự phát triển...

*Ví dụ: một ràng buộc điển hình thuộc loại này là nhu cầu hợp nhất các nghĩa vụ hợp pháp của tổ chức thành chính sách an toàn.*

Ràng buộc mang bản chất văn hóa

Trong một vài tổ chức, các thói quen trong công việc hoặc nghiệp vụ chính đã dẫn đến một "văn hóa" đặc trưng trong tổ chức, 'văn hóa' này có thể không phù hợp với các biện pháp kiểm soát an toàn. Văn hóa này là khung tham khảo chung của nhân sự và có thể được quyết định bằng nhiều khía cạnh, bao gồm: giáo dục, học vấn, kinh nghiệm chuyên gia, kinh nghiệm bên ngoài công việc, quan điểm, triết học, lòng tin, địa vị xã hội...

Ràng buộc về ngân sách

Các biện pháp kiểm soát an toàn đã được đề xuất đôi lúc có thể có chi phí áp dụng quá cao. Do đó, cần phải cân nhắc khi áp dụng các biện pháp kiểm soát này vì còn phụ thuộc vào ngân sách của từng tổ chức.

*Ví dụ: trong khu vực tư nhân và một vài tổ chức công cộng, tổng chi phí cho các biện pháp kiểm soát an toàn thông tin cần không vượt quá chi phí xử lý các hậu quả tiềm ẩn của những rủi ro. Do đó, ban quản lý cao nhất cần phải đánh giá và chấp nhận các rủi ro đã được tính toán nếu tổ chức muốn tránh những chi phí an toàn vượt trội.*

### A.3 Danh sách các tài liệu tham khảo về quy định pháp lý có thể áp dụng cho tổ chức

Các yêu cầu quy định áp dụng cho tổ chức cần được nhận biết. Các yêu cầu này có thể là các luật, nghị định, những quy định cụ thể trong lĩnh vực của tổ chức hay các quy định nội bộ và/hoặc bên ngoài. Điều này cũng liên quan đến các hợp đồng, các thỏa thuận và khái quát hơn là bất kì nghĩa vụ nào có tính chất quy phạm pháp lý hoặc quy định.

### A.4 Danh sách các ràng buộc ảnh hưởng đến phạm vi

Thông qua việc nhận biết các ràng buộc, có thể liệt kê các ràng buộc có tác động đến phạm vi và xác định được ràng buộc mà chịu ảnh hưởng của hoạt động. Những ràng buộc này thêm vào và có thể điều chỉnh các ràng buộc của tổ chức đã xác định ở trên. Phần dưới đây đưa ra danh sách chưa hoàn chỉnh về những kiểu ràng buộc.

Ràng buộc nảy sinh từ những quy trình đã có

Các dự án ứng dụng không nhất thiết phải được phát triển một cách đồng thời. Một vài dự án ứng dụng phụ thuộc vào những quy trình đã có. Mặc dù một quy trình có thể bị phân ra thành nhiều quy trình con, quy trình này không nhất thiết phải chịu ảnh hưởng bởi toàn bộ các quy trình con của quy trình khác.

Ràng buộc kỹ thuật

Các ràng buộc kỹ thuật, liên quan đến cơ sở hạ tầng của tổ chức, phát sinh khi cài đặt các thiết bị phần cứng hay phần mềm và phát sinh từ phòng hay vị trí diễn ra quy trình:

- Các tập tin (các yêu cầu liên quan đến tổ chức, quản lý phương tiện thông tin, quản lý các quy tắc truy cập...)
- Kiến trúc tổng thể (các yêu cầu liên quan đến kiểu kiến trúc (tập trung, phân tán, khách - máy chủ), kiểu kiến trúc vật lí...)
- Phần mềm ứng dụng (các yêu cầu liên quan đến thiết kế phần mềm đặc trưng, các tiêu chuẩn của thị trường...)
- Gói phần mềm (các yêu cầu liên quan đến các tiêu chuẩn, mức đánh giá, chất lượng, tuân thủ quy chuẩn kỹ thuật, an toàn...)
- Phần cứng (các yêu cầu liên quan đến các tiêu chuẩn, chất lượng, tuân thủ quy chuẩn kỹ thuật... )
- Các mạng truyền thông (các yêu cầu liên quan đến phạm vi truyền thông, các tiêu chuẩn, dung lượng, độ tin cậy...)
- Xây dựng cơ sở hạ tầng (các yêu cầu liên quan đến xây dựng dân dụng, công trình, điện áp cao, điện áp thấp...)

Ràng buộc về tài chính

Việc triển khai các biện pháp kiểm soát an toàn thông tin thường bị giới hạn về ngân sách mà tổ chức có thể cam kết. Tuy nhiên, ràng buộc về mặt tài chính vẫn là ràng buộc cuối cùng cần phải được xem xét bởi vì việc cấp ngân sách cho an toàn thông tin có thể được dàn xếp trên cơ sở nghiên cứu về an toàn thông tin.

Ràng buộc về môi trường

Các ràng buộc về môi trường bắt nguồn từ môi trường địa lý hay kinh tế mà ở đó các quy trình đang được triển khai: đất nước, khí hậu, các rủi ro tự nhiên, điều kiện địa lý, môi trườngkinh tế...

Ràng buộc về thời gian

Thời gian cần thiết cho việc triển khai các biện pháp kiểm soát an toàn thông tin cần phải được xem xét trong mối liên quan đến khả năng nâng cấp của hệ thống thông tin; nếu thời gian triển khai là quá dài, những rủi ro mà biện pháp kiểm soát đã được thiết kế để xử lý chúng có thể đã thay đổi. Thời gian là một yếu tố quyết định cho việc lựa chọn các giải pháp và các ưu tiên.

Ràng buộc liên quan đến các phương pháp

Các phương pháp thích hợp với hiểu biết của tổ chức phải được sử dụng cho việc lập kế hoạch dự án, xác định đặc tính kỹ thuật, phát triển...

Ràng buộc mang tính tổ chức

Các ràng buộc khác nhau có thể xuất phát từ các yêu cầu của tổ chức:

- Vận hành (các yêu cầu liên quan đến thời gian trễ khởi động, cung cấp dịch vụ, theo dõi, giám sát, kế hoạch ứng cứu khẩn cấp, hoạt động vận hành bị xuống cấp...)
- Duy trì (các yêu cầu đối với việc xử lý sự cố, các hành động phòng ngừa, khắc phục nhanh chóng...)
- Quản lý nguồn nhân lực (các yêu cầu liên quan đến việc đào tạo người vận hành và người sử dụng, năng lực đối với những vị trí công tác như là người quản trị hệ thống và người quản trị dữ liệu...)
- Quản lý hành chính (các yêu cầu liên quan đến trách nhiệm...)
- Quản lý phát triển (các yêu cầu liên quan đến các công cụ phát triển, kĩ sư phần mềm máy tính, các kế hoạch chấp nhận, thiết lập tổ chức...)
- Quản lý các mối quan hệ bên ngoài (các yêu cầu liên quan đến việc thiết lập các mối quan hệ với bên thứ ba, ký kết hợp đồng...)

# Phụ lục B

(Tham khảo)

## Nhận biết, định giá tài sản và đánh giá tác động

### B.1 Ví dụ về nhận biết tài sản

Để thực hiện định giá tài sản, trước tiên tổ chức cần phải nhận biết được các tài sản của tổ chức đó (ở một mức chi tiết phù hợp). Tài sản có thể được chia thành hai loại:

- Tài sản cơ bản:
- Hoạt động và quy trình nghiệp vụ
- Thông tin
- Tài sản bổ trợ (là tài sản mà các yếu tố cơ bản của phạm vi dựa vào), gồm các loại:
- Phần cứng
- Phần mềm
- Mạng
- Nhân sự
- Vị trí
- Cấu trúc của tổ chức

#### B.1.1 Nhận biết tài sản cơ bản

Để mô tả phạm vi một cách chính xác hơn, hoạt động này bao gồm việc nhận biết tài sản cơ bản (các quy trình và hoạt động nghiệp vụ, thông tin). Việc nhận biết tài sản này được tiến hành bởi một nhóm người đại diện của quy trình (những người quản lý, các chuyên gia hệ thống thông tin và những người sử dụng).

Tài sản cơ bản thường là những quy trình và thông tin cốt lõi của hoạt động trong phạm vi bối cảnh tổ chức. Những tài sản cơ bản khác như là các quy trình của tổ chức cũng cần phải xem xét, điều này sẽ thích hợp hơn cho việc xây dựng một chính sách an toàn thông tin hay một kế hoạch liên tục trong nghiệp vụ. Tùy thuộc vào từng mục đích, một vài nghiên cứu không yêu cầu một sự phân tích triệt để các yếu tố của phạm vi. Trong những trường hợp này, ranh giới nghiên cứu có thể được giới hạn trong những yếu tố chính của phạm vi.

Tài sản cơ bản gồm hai loại:

1- Các quy trình (hoặc quy trình con) và hoạt động nghiệp vụ, ví dụ:

- Các quy trình mà sự mất mát hoặc xuống cấp của chúng làm mất khả năng thực hiện những nhiệm vụ của tổ chức
- Các quy trình chứa các quy trình bí mật hoặc các quy trình liên quan đến công nghệ độc quyền
- Các quy trình mà nếu bị sửa đổi có thể gây ảnh hưởng lớn đến việc hoàn thành nhiệm vụ của tổ chức
- Các quy trình cần thiết cho tổ chức để tuân thủ các yêu cầu hợp đồng, quy định hoặc yêu cầu pháp lý

2- Tài sản thông tin:

Một cách tổng quát hơn, tài sản thông tin chủ yếu bao gồm:

- Thông tin cần thiết cho việc thực hiện nhiệm vụ hoặc nghiệp vụ của tổ chức
- Thông tin cá nhân, có thể được định nghĩa một cách cụ thể theo luật pháp quốc gia về quyền riêng tư.
- Thông tin chiến lược cần thiết cho việc đạt được các mục tiêu được xác định bởi những định hướng chiến lược.
- Thông tin có chi phí cao mà việc thu thập, lưu trữ, xử lý và truyền dẫn những thông tin đó đòi hỏi một khoảng thời gian dài và/hoặc liên quan tới chi phí mua lại cao.

Các quy trình và những thông tin không được xác định là nhạy cảm sau hoạt động này sẽ không có sự phân loại rõ ràng trong phần còn lại của nghiên cứu. Điều đó có nghĩa là ngay cả khi các quy trình hoặc thông tin này bị gây hại thì tổ chức vẫn hoàn thành nhiệm vụ một cách thành công.

Tuy nhiên, tổ chức sẽ thường xuyên kế thừa những biện pháp kiểm soát mà đã được triển khai để bảo vệ các quy trình và thông tin đã được xác định là nhạy cảm.

### B.1.2 Danh sách và mô tả những tài sản bổ trợ

Phạm vi bao gồm các tài sản cần được nhận biết và mô tả. Các tài sản này có những điểm yếu dễ bị khai thác bởi những mối đe dọa có mục đích làm hư hại các tài sản cơ bản (các quy trình và thông tin). Tài sản bổ trợ gồm nhiều loại khác nhau:

Phần cứng

Loại phần cứng bao gồm tất cả các phần tử vật lí hỗ trợ các quy trình.

Thiết bị xử lý dữ liệu (tích cực)

Thiết bị xử lý thông tin tự động bao gồm các thiết bị có thể vận hành một cách độc lập.

Thiết bị có thể vận chuyển được

Thiết bị máy tính xách tay.

Ví dụ: máy tính xách tay, thiết bị hỗ trợ kỹ thuật số cá nhân (PDA).

Thiết bị cố định

Thiết bị máy tính được sử dụng trong phạm vi tổ chức.

Ví dụ: máy chủ, máy vi tính được sử dụng như một máy trạm.

Thiết bị xử lý ngoại vi

Thiết bị được kết nối tới một máy tính thông qua một cổng truyền thông (liên kết nối tiếp, song song...) để nhập dữ liệu, chuyển dữ liệu hoặc truyền dữ liệu.

Ví dụ: máy in, ổ đọc đĩa.

Phương tiện dữ liệu (thụ động)

Đây là những phương tiện để lưu trữ dữ liệu hoặc các chức năng.

Phương tiện điện tử

Một phương tiện thông tin mà có thể kết nối với một máy tính hoặc mạng máy tính để lưu trữ dữ liệu. Mặc dù chỉ có kích thước nhỏ gọn nhưng các phương tiện thông tin này có thể chứa được một khối lượng lớn dữ liệu. Các thiết bị này có thể được sử dụng với thiết bị điện toán quy chuẩn.

Ví dụ: đĩa mềm, đĩa CD, băng đĩa từ sao lưu, ổ cứng di động, thẻ nhớ, băng từ.

Các phương tiện khác

Phương tiện tĩnh, phi điện tử chứa dữ liệu.

Ví dụ: giấy, slide, tài liệu văn bản, fax.

Phần mềm

Phần mềm bao gồm toàn bộ chương trình đóng góp vào việc vận hành của một bộ xử lý dữ liệu.

Hệ điều hành

Hệ điều hành bao gồm toàn bộ chương trình của một máy tính tạo thành bộ vận hành nền tảng cho các chương trình phần mềm khác chạy (như là các ứng dụng hoặc dịch vụ). Hệ điều hành bao gồm một phần trung tâm và các chức năng hoặc dịch vụ cơ bản. Tùy vào từng kiến trúc, một hệ điều hành có thể là nguyên khối hoặc được tạo ra từ một phần trung tâm rất nhỏ và một tập hợp các dịch vụ hệ thống. Các thành phần chính của hệ điều hành là toàn bộ các dịch vụ quản lý thiết bị (bộ xử lý trung tâm, bộ nhớ máy tính, đĩa và các giao diện mạng), các dịch vụ quản lý nhiệm vụ hoặc quy trình và các dịch vụ quản lý quyền của người sử dụng.

Dịch vụ, phần mềm bảo trì hoặc quản trị

Phần mềm bổ sung trực tiếp cho các dịch vụ hệ điều hành và bổ sung gián tiếp cho các dịch vụ của người dùng hoặc các ứng dụng (mặc dù phần mềm thường là cần thiết hoặc không thể thiếu được đối với toàn bộ hoạt động của hệ thống thông tin).

Gói phần mềm hay phần mềm chuẩn

Phần mềm chuẩn hoặc gói phần mềm được hiểu theo cách thông thường là những sản phẩm trọn vẹn được thương mại hóa (không phải là các phần mềm được phát triển cụ thể hoặc chỉ làm một lần) có phương tiện thông tin, phát hành và duy trì. Các phần mềm này cung cấp các dịch vụ cho người sử dụng và các ứng dụng, nhưng không mang tính cá nhân hoặc cụ thể như các ứng dụng nghiệp vụ.

Ví dụ: phần mềm quản lý cơ sở dữ liệu, phần mềm thư điện tử, phần mềm nhóm, phần mềm danh mục, phần mềm máy chủ web...

Ứng dụng nghiệp vụ

Ứng dụng nghiệp vụ tiêu chuẩn

Đây là phần mềm thương mại được thiết kế để đưa tới cho những người sử dụng sự truy cập trực tiếp đến các dịch vụ và các chức năng mà họ yêu cầu từ hệ thống thông tin trong bối cảnh chuyên môn của họ, có phạm vi rất rộng, không giới hạn về mặt lý thuyết và bao gồm nhiều lĩnh vực.

Ví dụ: phần mềm kế toán, phần mềm điều khiển công cụ máy, phần mềm chăm sóc khách hàng, phần mềm quản lý năng lực cán bộ, phần mềm quản trị...

Ứng dụng nghiệp vụ đặc trưng

Đây là phần mềm mà ở đó các khía cạnh khác nhau (ví dụ như: hỗ trợ, bảo trì, nâng cấp...) được phát triển một cách đặc thù để đưa tới cho những người sử dụng sự truy cập trực tiếp đến các dịch vụ và chức năng mà họ yêu cầu từ hệ thống thông tin của họ. Đây là phạm vi rất rộng, không giới hạn về mặt lý thuyết và đa lĩnh vực.

Ví dụ: quản lý hóa đơn của các khác hàng khai thác viễn thông, ứng dụng giám sát thời gian thực cho việc phóng tên lửa.

Mạng

Mạng bao gồm toàn bộ các thiết bị viễn thông được sử dụng để kết nối nhiều máy tính hay nhiều thành phần của một hệ thống thông tin ở cách xa nhau về điều kiện tự nhiên.

Phương tiện thông tin và sự hỗ trợ

Phương tiện hay thiết bị thông tin và viễn thông được mô tả chủ yếu bởi các đặc điểm về vật lí và kỹ thuật của thiết bị (điểm tới điểm, quảng bá) và bằng các giao thức truyền thông (liên kết hoặc mạng - tầng 2 và 3 theo mô hình mạng OSI 7 tầng).

Ví dụ: mạng điện thoại chuyển mạch công cộng (PSTN), chuẩn Ethernet, Gigabit Ethernet, đường dây thuê bao kỹ thuật số không đối xứng (ADSL), đặc tả giao thức không dây (theo chuẩn WiFi 802.11), chuẩn Bluetooth, chuẩn Firewire.

Bộ chuyển tiếp thụ động hoặc chủ động

Kiểu này bao gồm toàn bộ thiết bị mà không phải là thiết bị kết cuối logic (trong hệ thống thông tin) mà là thiết bị trung gian hoặc thiết bị chuyển tiếp. Các thiết bị chuyển tiếp được mô tả bằng các giao thức truyền thông mạng được hỗ trợ. Ngoài chức năng chuyển tiếp cơ bản, các thiết bị này thường có thêm các chức năng, dịch vụ định tuyến và/hoặc lọc, bộ chuyển mạch và bộ định tuyến với các bộ lọc. Chúng có thể được quản lý từ xa và thường có khả năng tạo ra các bản ghi.

Ví dụ: cầu nối, thiết bị định tuyến, máy chủ truy cập, thiết bị chuyển mạch, tổng đài tự động.

Giao diện truyền thông

Các giao diện truyền thông của các bộ xử lý đều được kết nối tới các bộ xử lý nhưng được mô tả bằng phương tiện thông tin và các giao thức hỗ trợ, bằng các chức năng lọc, ghi vết hoặc phát cảnh báo và dung lượng của chúng và bằng khả năng và yêu cầu quản lý từ xa. Ví dụ: dịch vụ vô tuyến gói tổng hợp (GPRS), bộ tương thích Ethernet.

Nhân sự

Nhân sự bao gồm toàn bộ nhóm người liên quan đến hệ thống thông tin.

Người đưa ra quyết định

Người đưa ra quyết định là người chủ sở hữu các tài sản cơ bản (thông tin và chức năng) và là người quản lý tổ chức hoặc dự án cụ thể.

Ví dụ: người quản lý ở cấp cao nhất, người phụ trách dự án.

Người dùng

Người dùng là những người xử lý các thành phần nhạy cảm trong bối cảnh hoạt động của họ và là người có một trách nhiệm đặc biệt ở lĩnh vực này. Người dùng có quyền truy cập đặc biệt đến hệ thống thông tin để thực hiện các nhiệm vụ hàng ngày của họ.

Ví dụ: người quản lý nguồn nhân lực, người quản lý tài chính, người quản lý rủi ro.

Nhân viên vận hành/bảo trì

Là những người phụ trách việc vận hành và bảo trì hệ thống thông tin. Những nhân viên này có quyền truy cập đặc biệt tới hệ thống thông tin để thực hiện các nhiệm vụ hàng ngày .

Ví dụ: người quản trị hệ thống, người quản trị dữ liệu, văn thư, bộ phận hỗ trợ, người triển khai ứng dụng, các nhân viên bảo vệ.

Nhà phát triển ứng dụng

Người phát triển là người phụ trách phát triển các ứng dụng của tổ chức. Họ có quyền cấp cao để truy cập tới bộ phận của hệ thống thông tin nhưng không đưa ra bất kì hành động nào tới việc sản xuất dữ liệu.

Ví dụ: người phát triển ứng dụng nghiệp vụ.

Trụ sở

Trụ sở bao gồm tất cả các địa điểm chứa toàn bộ phạm vi hoặc một phần của phạm vi và các phương tiện vật chất cần thiết để trụ sở hoạt động.

Địa điểm

Môi trường bên ngoài

Gồm toàn bộ các địa điểm mà ở đó các biện pháp an toàn của tổ chức không thể được áp dụng.

Ví dụ: nhà của nhân viên, cơ sở của các tổ chức khác, môi trường bên ngoài trụ sở (khu vực đô thị, khu vực nguy hiểm).

Cơ sở

Nơi này được giới hạn bởi vành đai của tổ chức và giữ liên hệ trực tiếp với bên ngoài. Cơ sở có thể được bảo vệ bằng việc tạo ra các hàng rào hoặc các phương tiện giám sát xung quanh các tòa nhà.

Ví dụ: cơ sở, các tòa nhà.

Khu vực

Khu vực được hình thành bởi một ranh giới bảo vệ vật lí tạo ra các vách ngăn trong cơ sở của tổ chức. Khu vực có được bằng cách tạo ra các hàng rào vật lí xung quanh các cơ sở hạ tầng xử lý thông tin của tổ chức.

Ví dụ: các phòng ban, khu vực truy cập riêng tư, khu vực an toàn.

Các dịch vụ thiết yếu

Toàn bộ các dịch vụ cần thiết để vận hành các trang thiết bị của tổ chức.

Truyền thông

Các dịch vụ viễn thông và trang thiết bị được cung cấp bởi một doanh nghiệp viễn thông.

Ví dụ: đường dây điện thoại, thiết bị trao đổi PABX, các mạng điện thoại nội bộ.

Các hệ thống tiện ích khác

Các dịch vụ và phương tiện (các nguồn cung cấp và hệ thống mạng dây dẫn) cần thiết cho việc cung cấp điện năng cho các thiết bị công nghệ thông tin và thiết bị ngoại vi.

Ví dụ: nguồn điện áp thấp, bộ biến tần, bảng mạch điện đầu cuối.

Nguồn cung cấp nước

Xử lý chất thải

Các dịch vụ và phương tiện (thiết bị, kiểm soát) cho việc làm mát và lọc không khí.

Ví dụ: các đường ống nước làm mát, các bộ điều hòa không khí.

Tổ chức

Các loại hình tổ chức mô tả cấu trúc tổ chức, bao gồm tất cả các cấu trúc nhân sự của tổ chức đã được phân công nhiệm vụ và các phương pháp quản lý các cấu trúc này.

Cơ quan quyền lực

Đây là những đơn vị có thẩm quyền đối với tổ chức đang xét, có thể là chi nhánh hợp pháp hoặc từ bên ngoài. Các đơn vị này áp đặt những ràng buộc đối với tổ chức đang xét qua các quy định, quyết định và các hành động.

Ví dụ: cơ quan quản trị, văn phòng chính của một tổ chức.

Cấu trúc của tổ chức

Bao gồm nhiều chi nhánh khác nhau của tổ chức, có nhiều chức năng đan xen, hoạt động dưới sự quản lý của ban quản lý của tổ chức đó.

Ví dụ: quản lý các nguồn nhân lực, quản lý công nghệ thông tin, quản lý mua sắm, quản lý kinh doanh, dịch vụ an toàn cho tòa nhà, dịch vụ chữa cháy, quản lý kiểm toán.

Tổ chức dự án hay hệ thống

Liên quan đến việc tổ chức được thành lập cho một dự án hoặc dịch vụ cụ thể.

Ví dụ: dự án phát triển ứng dụng mới, dự án di chuyển hệ thống thông tin.

Nhà thầu phụ / nhà cung cấp / nhà sản xuất

Đây là những đơn vị cung cấp cho tổ chức dịch vụ hoặc các nguồn tài nguyên và bị ràng buộc với tổ chức thông qua hợp đồng.

Ví dụ: công ty quản lý trang thiết bị, công ty thuê ngoài, công ty tư vấn.

### B.2 Định giá tài sản

Bước tiếp theo sau khi nhận biết tài sản là thống nhất thang đo được sử dụng và các tiêu chí để xác định giá trị cụ thể trên thang đo đó cho mỗi tài sản, dựa vào việc định giá. Trong hầu hết các tổ chức, vì tài sản là vô cùng đa dạng nên có khả năng một vài tài sản có giá trị tiền tệ đã được nhận biết sẽ được định giá ngay theo đơn vị tiền tệ địa phương. Trong khi đó, những tài sản khác có giá trị định lượng nhiều hơn thì có thể được gán cho một giá trị trong dải, ví dụ từ "rất thấp" tới "rất cao". Quyết định sử dụng thang đo định lượng hay thang đo định tính là tùy thuộc vào mỗi tổ chức, nhưng phải thích hợp với những tài sản đang được định giá. Cả hai loại định giá có thể được sử dụng cho cùng một loại tài sản.

Các thuật ngữ điển hình được sử dụng cho việc định giá tài sản theo định tính thường là những từ như: không đáng kể, rất thấp, thấp, trung bình, cao, rất cao và nghiêm trọng. Việc lựa chọn và xếp loại các thuật ngữ cho phù hợp với tổ chức phụ thuộc rất lớn vào nhu cầu an toàn của tổ chức, quy mô của tổ chức và các yếu tố cụ thể khác.

Tiêu chí

Các tiêu chí được sử dụng như là cơ sở cho việc định giá đối với mỗi tài sản cần được viết bằng những thuật ngữ rõ ràng. Đây thường là một trong những khía cạnh khó nhất của việc định giá tài sản, bởi vì giá trị của một số tài sản có thể phải được xác định một cách chủ quan và việc xác định có thể được thực hiện bởi nhiều cá nhân khác nhau. Các tiêu chí thường được sử dụng để xác định giá trị của tài sản bao gồm: chi phí ban đầu, chi phí thay thế hay tạo lập lại hoặc giá trị của tài sản có thể là trừu tượng, ví dụ như: giá trị uy tín của một tổ chức.

Một cơ sở khác cho việc định giá tài sản là các chi phí phải gánh chịu do sự mất đi tính bí mật, tính toàn vẹn và tính sẵn sàng như là kết quả của một sự cố. Tính không chối bỏ, trách nhiệm giải trình, tính xác thực và độ tin cậy cũng phải được xem xét một cách thích hợp. Việc định giá như thế này phải đưa ra những thông số thành phần quan trọng để đánh giá giá trị, bổ sung thêm vào chi phí thay thế, dựa trên các đánh giá đối với các hậu quả nghiệp vụ bất lợi là kết quả của các sự cố an toàn trong những hoàn cảnh đã được giả thiết. Cần phải nhấn mạnh phương pháp tiếp cận này dành cho các hậu quả mà cần thiết đưa hệ số vào việc đánh giá rủi ro.

Nhiều tài sản trong suốt quy trình định giá có thể được gán nhiều giá trị. Ví dụ: một kế hoạch nghiệp vụ có thể được định giá dựa trên số lao động được sử dụng để phát triển kế hoạch, có thể được định giá dựa trên số lao động nhập dữ liệu và có thể được định giá dựa trên giá trị của kế hoạch nghiệp vụ đó đối với một đối thủ cạnh tranh. Mỗi giá trị được gán sẽ có sự khác nhau một cách đáng kể. Giá trị được gán có thể lớn nhất trong số tất cả các giá trị tồn tại hoặc có thể là tổng của một vài hoặc tất cả các giá trị tồn tại. Trong bản phân tích cuối cùng, giá trị hoặc những giá trị nào mà được gán cho một tài sản phải được quyết định một cách cẩn thận bởi vì giá trị cuối cùng sẽ được dùng vào việc xác định các nguồn lực được sử dụng cho việc bảo vệ tài sản.

Giảm nhẹ tới mức chung

Cuối cùng, toàn bộ định giá tài sản cần phải được giảm nhẹ tới một mức chung. Điều này có thể được thực hiện với sự trợ giúp của các tiêu chí được liệt kê ở dưới. Những tiêu chí có thể được sử dụng để đánh giá hậu quả có thể xảy do sự mất đi tính bí mật, tính toàn vẹn, tính sẵn sàng, tính chống chối bỏ, trách nhiệm giải trình, tính xác thực, hoặc độ tin cậy của tài sản là:

- Vi phạm luật pháp và/hoặc quy định
- Làm suy giảm việc thực thi nghiệp vụ
- Mất thiện ý/ảnh hưởng tiêu cực tới uy tín
- Vi phạm liên quan đến thông tin cá nhân
- Gây nguy hiểm đến an toàn cá nhân
- Ảnh hưởng xấu đến việc thi hành pháp luật
- Vi phạm tính bí mật
- Vi phạm trật tự công cộng
- Thiệt hại tài chính
- Ảnh hưởng đến các hoạt động nghiệp vụ
- Đe dọa an toàn môi trường

Những phương pháp tiếp cận khác để đánh giá các hậu quả có thể là:

- Gián đoạn dịch vụ
    - không có khả năng cung cấp dịch vụ
- Đánh mất niềm tin của khách hàng
    - đánh mất độ tin cậy trong hệ thống thông tin nội bộ
    - hủy hại tới uy tín
- Phá vỡ vận hành nội bộ
    - phá vỡ ngay trong chính tổ chức
    - thêm vào chi phí nội bộ
- Phá vỡ hoạt động của một bên thứ ba
    - phá vỡ trong nội bộ của các bên thứ ba có giao dịch với tổ chức
    - các loại thiệt hại khác nhau
- Vi phạm pháp luật / quy định
    - không có khả năng thực hiện các nghĩa vụ pháp lý
- Vi phạm hợp đồng
    - không có khả năng thực hiện các nghĩa vụ theo hợp đồng
- Nguy hiểm đến an toàn của nhân sự / người sử dụng
    - nguy hiểm cho nhân sự của tổ chức và/hoặc người sử dụng
- Tấn công vào cuộc sống riêng tư của người sử dụng
- Thiệt hại về tài chính
- Chi phí tài chính trong trường hợp khẩn cấp hoặc sửa chữa
    - về mặt nhân sự
    - về mặt trang thiết bị
    - về mặt nghiên cứu, báo cáo của các chuyên gia
- Thiệt hại hàng hóa / vốn / tài sản
- Đánh mất khách hàng, đánh mất nhà cung cấp
- Thủ tục tố tụng tư pháp và hình phạt
- Đánh mất lợi thế cạnh tranh
- Đánh mất vị trí dẫn đầu về công nghệ / kỹ thuật
- Mất hiệu quả / sự tin tưởng
- Mất uy tín công nghệ
- Suy giảm năng lực đàm phán

- Khủng hoảng công nghiệp (các cuộc đình công)
- Khủng hoảng chính phủ
- Sự giải tán
- Hư hỏng nguyên vật liệu

Các tiêu chí này là những ví dụ về những vấn đề cần được xem xét cho việc định giá tài sản. Để thực hiện việc định giá, tổ chức cần phải lựa chọn các tiêu chí thích hợp với loại hình nghiệp vụ và các yêu cầu an toàn. Điều đó có nghĩa là một vài trong số các tiêu chí được liệt kê ở trên không thể áp dụng được và một số tiêu chí khác có thể cần được thêm vào danh sách.

Thang đo

Sau khi việc thiết lập các tiêu chí được xem xét, tổ chức cần phải thống nhất một thang đo được sử dụng trong toàn bộ tổ chức. Bước đầu tiên là quyết định số lượng mức được sử dụng. Không có quy tắc nào liên quan đến số lượng mức như thế nào thích hợp nhất. Nhiều mức hơn thì sẽ cung cấp một mức chi tiết lớn hơn, nhưng đôi khi một sự phân biệt quá chính xác sẽ làm cho việc gán tiêu chí nhất quán trong tổ chức khó thực hiện. Thông thường, bất kỳ số lượng mức nào nằm giữa 3 (như thấp, trung bình và cao) và 10 có thể được sử dụng miễn là phù hợp với phương pháp tiếp cận mà các tổ chức đang sử dụng cho toàn bộ quy trình đánh giá rủi ro.

Một tổ chức có thể định nghĩa các giới hạn của mình đối với các giá trị tài sản, như là "thấp", "trung bình", hoặc "cao". Các giới hạn này nên được đánh giá căn cứ theo các tiêu chí đã được lựa chọn (ví dụ như đối với thiệt hại tài chính có thể xảy ra, các giới hạn nên được đưa ra theo các giá trị tiền tệ, nhưng để đánh giá cho những nguy hiểm đến an toàn cá nhân thì việc đánh giá theo giá trị tiền tệ có thể phức tạp và không phù hợp với mọi tổ chức). Cuối cùng, việc quyết định hậu quả như thế nào là "nhỏ" hay "lớn" hoàn toàn phụ thuộc vào tổ chức. Một hậu quả có thể là thảm họa đối với một tổ chức nhỏ nhưng có thể là nhỏ hoặc thậm chí không đáng kể đối với một tổ chức rất lớn.

Sự phụ thuộc

Tài sản càng hỗ trợ thích hợp và nhiều quy trình nghiệp vụ thì giá trị của tài sản càng lớn. Sự phụ thuộc của các tài sản vào các quy trình nghiệp vụ và các tài sản khác cũng cần được nhận biết bởi vì điều này có thể ảnh hưởng đến giá trị tài sản. Ví dụ: tính bí mật của dữ liệu cần được lưu giữ trong suốt vòng đời của dữ liệu, ở tất cả các giai đoạn, bao gồm lưu trữ và xử lý, tức là nhu cầu an toàn của các chương trình xử lý và lưu trữ dữ liệu phải có liên quan trực tiếp đến giá trị đại diện cho tính bí mật của dữ liệu được lưu trữ và xử lý. Cũng như vậy, nếu một quy trình nghiệp vụ dựa vào tính toàn vẹn của dữ liệu được tạo bởi một chương trình thì dữ liệu đầu vào của chương trình này phải đáng tin cậy. Hơn nữa, tính toàn vẹn của thông tin sẽ phụ thuộc vào phần cứng và phần mềm được sử dụng để lưu trữ và xử lý thông tin. Cũng như vậy, phần cứng sẽ phụ thuộc vào việc cung cấp điện năng và điều hòa không khí. Do đó, thông tin về sự phụ thuộc sẽ trợ giúp cho việc nhận biết các mối đe dọa và điểm yếu cụ thể. Thêm vào đó, nó cũng giúp đảm bảo giá trị thực sự của tài sản (thông qua các mối quan hệ phụ thuộc) sẽ được gán cho các tài sản, qua đó chỉ ra mức bảo vệ hợp lý.

Giá trị của tài sản mà các tài sản khác phụ thuộc vào đó có thể được sửa đổi theo cách sau:

- Nếu giá trị của tài sản phụ thuộc (ví dụ: dữ liệu) thấp hơn hoặc bằng giá trị của tài sản được xem xét (ví dụ: phần mềm) thì giá trị của tài sản được xem xét vẫn giữ nguyên
- Nếu giá trị của tài sản phụ thuộc (ví dụ: dữ liệu) lớn hơn thì giá trị của tài sản được xem xét (ví dụ: phần mềm) phải được tăng lên theo tùy thuộc:
    - Mức phụ thuộc
    - Giá trị của các tài sản khác

Một tổ chức có thể có một vài tài sản với số lượng lớn hơn một, như là các bản sao của các chương trình phần mềm hoặc các máy tính cùng loại được sử dụng trong hầu hết các phòng ban. Thực tế này cần thiết phải được xem xét khi tiến hành định giá tài sản. Một mặt, những tài sản này dễ dàng bị bỏ sót, do đó cần phải chú ý để nhận biết tất cả các tài sản đó; mặt khác, chúng có thể được sử dụng để giảm thiểu các vấn đề có sẵn.

Đầu ra

Kết quả cuối cùng của bước này là một danh sách các tài sản và các giá trị của chúng liên quan đến: sự tiết lộ (duy trì tính bí mật), sự thay đổi (duy trì tính toàn vẹn, tính xác thực, tính chống chối bỏ và trách nhiệm giải trình), tính không sẵn sàng và sự phá hủy (duy trì tính sẵn sàng và độ tin cậy) và chi phí thay thế.

### B.3 Đánh giá tác động

Một sự cố an toàn thông tin có thể tác động tới nhiều hơn một tài sản hoặc chỉ một phần tài sản. Tác động có liên quan tới mức thành công của sự cố. Giống như hậu quả, có một sự khác biệt quan trọng giữa giá trị tài sản và tác động được gây ra từ sự cố. Tác động được xem như hoặc có một ảnh hưởng ngay lập tức (về vận hành) hoặc có ảnh hưởng trong tương lai (về nghiệp vụ) mà bao gồm các hậu quả về tài chính và thị trường.

Tác động ngay lập tức (về vận hành) có thể là trực tiếp hoặc gián tiếp.

Trực tiếp:

a) Giá trị thay thế tài chính của tài sản hoặc một phần tài sản bị mất

b) Chi phí thu nhận, cấu hình và cài đặt tài sản mới hoặc sao lưu

c) Chi phí vận hành bị dừng do các sự cố cho đến khi các dịch vụ được cung cấp bởi (các) tài sản được khôi phục

d) Tác động gây ra một sự vi phạm an toàn thông tin

Gián tiếp:

a) Chi phí cơ hội (các nguồn tài chính cần thiết để thay thế hoặc sửa chữa một tài sản lẽ ra đã được sử dụng cho mục đích khác)

b) Chi phí cho các hoạt động bị gián đoạn

c) Tiềm ẩn sự lạm dụng các thông tin thu được thông qua sự vi phạm an toàn thông tin

d) Vi phạm các nghĩa vụ do luật pháp quy định hoặc vi phạm quy định

e) Vi phạm các chuẩn mực đạo đức ứng xử

Như vậy, bước đánh giá đầu tiên (không có bất cứ biện pháp kiểm soát nào) sẽ ước lượng được một tác động mà rất gần với (các) giá trị tài sản có liên quan. Ở bất kì quy trình lặp lại tiếp theo nào đối với (các) tài sản này thì tác động cũng sẽ khác nhau (thường là thấp hơn nhiều) do sự có mặt và hiệu quả của các biện pháp kiểm soát đã được triển khai.

## Phụ lục C

(Tham khảo)

## Ví dụ về những mối đe dọa điển hình

Bảng dưới đây sẽ đưa ra các ví dụ về những mối đe dọa điển hình. Danh sách này có thể được sử dụng trong suốt quy trình đánh giá các mối đe dọa. Các mối đe dọa có thể là do cố ý, vô ý hay do môi trường (tự nhiên) và có thể gây ra ví dụ như sự thiệt hại hay mất mát những dịch vụ cần thiết. Dưới đây liệt kê đối với từng kiểu đe dọa với C (cố ý), V (vô ý), MT (môi trường).

C: được sử dụng cho tất cả các hành động cố ý nhằm tới các tài sản thông tin.

V: được sử dụng cho tất cả các hành động do con người có thể vô ý gây ra thiệt hại lên các tài sản thông tin.

MT: được sử dụng cho tất cả các sự cố không do hành động của con người gây ra.

Các nhóm đe dọa không được sắp xếp theo thứ tự ưu tiên.

| Loại | Các mối đe dọa | Nguồn gốc |
|---|---|---|
| Thiệt hại về vật chất | Cháy/Hỏa hoạn | C, V, MT |
| | Thiệt hại về nguồn nước | C, V, MT |
| | Sự ô nhiễm | C, V, MT |
| | Tai nạn nghiêm trọng | C, V, MT |
| | Sự phá hủy thiết bị hoặc các phương tiện thông tin | C, V, MT |
| | Bụi, ăn mòn, đóng băng | C, V, MT |
| Các sự kiện thiên nhiên | Hiện tượng khí hậu | MT |
| | Hiện tượng địa chấn | MT |
| | Hiện tượng núi lửa | MT |
| | Hiện tượng khí tượng | MT |
| | Lũ lụt | MT |
| Thiệt hại các dịch vụ cần thiết | Lỗi hệ thống điều hòa không khí hay hệ thống cấp nước | C, V |
| | Thất thoát trong cung cấp điện năng | C, V, MT |
| | Hư hỏng các trang thiết bị truyền thông | C, V |
| Nhiễu do bức xạ | Bức xạ điện từ | C, V, MT |
| | Bức xạ nhiệt | C, V, MT |

| | | |
|---|---|---|
| | Xung điện từ | C, V, MT |
| Gây hại tới thông tin | Nghe trộm các tín hiệu nhiễu gây hại tới thông tin | C |
| | Gián điệp từ xa | C |
| | Nghe trộm | C |
| | Lấy trộm phương tiện thông tin hoặc tài liệu | C |
| | Lấy trộm thiết bị | C |
| | Khôi phục thông tin từ phương tiện đã được tái chế hoặc đã bị loại bỏ | C |
| | Tiết lộ thông tin | C, V |
| | Dữ liệu từ các nguồn không đáng tin cậy | C, V |
| | Giả mạo phần cứng | C |
| | Giả mạo phần mềm | C, V |
| | Phát hiện vị trí | C |
| Các lỗi kỹ thuật | Lỗi do thiết bị | V |
| | Sự cố, hỏng thiết bị | V |
| | Trạng thái bão hòa của hệ thống thông tin | C, V |
| | Sự cố phần mềm | V |
| | Vi phạm về bảo trì hệ thống thông tin | C, V |
| Các hành vi trái phép | Sử dụng trái phép thiết bị | C |
| | Sao chép gian lận phần mềm | C |
| | Sử dụng phần mềm giả mạo hoặc đã bị sao chép | C, V |
| | Sửa đổi làm sai hỏng dữ liệu | C |
| | Xử lý dữ liệu không hợp pháp | C |
| Gây hại tới các chức năng | Lỗi trong sử dụng | V |
| | Lạm dụng quyền | C, V |
| | Giả mạo quyền | C |
| | Từ chối hành động | C |
| | Vi phạm tính sẵn sàng của nhân viên | C, V, MT |

Đặc biệt phải chú ý tới các nguồn gốc mối đe dọa mà nguyên nhân là do con người. Những nguồn gốc này được nhóm thành từng nhóm trong bảng dưới đây:

| Nguồn gốc mối đe dọa | Động cơ thực hiện | Các hậu quả có thể xảy ra |
|---|---|---|
| Tin tặc, người bẻ khóa | Thách thức<br>Lòng tự trọng<br>Sự nổi loạn, chống đối<br>Địa vị/danh tiếng<br>Tiền bạc | • Tấn công máy tính<br>• Kỹ thuật lừa đảo<br>• Xâm phạm, tấn công hệ thống<br>• Truy cập hệ thống trái phép |
| Tội phạm máy tính | Phá hủy thông tin<br>Công bố thông tin bất hợp pháp<br>Lợi ích tài chính<br>Thay đổi dữ liệu trái phép | • Tội phạm máy tính (ví dụ: theo dõi trên mạng)<br>• Hành vi gian lận (ví dụ: tái tạo, mạo danh, nghe lén thông tin)<br>• Mua chuộc thông tin<br>• Giả mạo thông tin<br>• Xâm nhập hệ thống |
| Khủng bố | Tống tiền<br>Phá hủy<br>Khai thác<br>Trả thù<br>Lợi ích chính trị<br>Đưa thông tin | • Bom/khủng bố<br>• Chiến tranh thông tin<br>• Tấn công hệ thống (ví dụ: tấn công từ chối dịch vụ phân tán)<br>• Xâm nhập hệ thống<br>• Giả mạo hệ thống |
| Gián điệp công nghiệp (cơ quan tình báo, các công ty, chính phủ nước | Lợi ích cạnh tranh<br>Gián điệp kinh tế | • Lợi ích quốc phòng<br>• Lợi ích chính trị<br>• Khai thác kinh tế<br>• Trộm cắp thông tin<br>• Xâm phạm quyền riêng tư cá nhân<br>• Kỹ thuật lừa đảo |

| | | |
|---|---|---|
| ngoài, các tổ chức quan tâm khác) | | • Xâm nhập hệ thống<br>• Truy cập vào hệ thống trái phép (truy cập đến các thông tin đã phân loại, độc quyền và/hoặc các thông tin liên quan đến công nghệ) |
| Những người trong nội bộ của tổ chức (được đào tạo kém, bất mãn, có ý xấu, cẩu thả, không trung thực, hoặc thôi việc) | Tò mò<br>Lòng tự trọng<br>Tin tức tình báo<br>Lợi ích tài chính<br>Sự trả thù<br>Lỗi và thiếu sót do vô ý (ví dụ: lỗi nhập dữ liệu, lỗi lập trình) | • Tấn công vào chuyên viên<br>• Tống tiền<br>• Xem thông tin độc quyền<br>• Lạm dụng máy tính<br>• Gian lận và trộm cắp<br>• Mua chuộc thông tin<br>• Giả mạo dữ liệu đầu vào, dữ liệu bị hỏng<br>• Nghe trộm<br>• Mã độc (ví dụ như virus, bom logic, Trojan)<br>• Bán thông tin cá nhân<br>• Lỗi hệ thống<br>• Xâm nhập hệ thống<br>• Phá hoại hệ thống<br>• Truy cập hệ thống trái phép |

# Phụ lục D

(Tham khảo)

## Các điểm yếu và các phương pháp đánh giá điểm yếu

### D.1 Các ví dụ về điểm yếu

Bảng dưới đây đưa ra những ví dụ về các điểm yếu trong những lĩnh vực an toàn khác nhau, bao gồm các ví dụ về những mối đe dọa mà có thể khai thác các điểm yếu này. Những danh sách này cung cấp những trợ giúp trong suốt quá trình đánh giá các mối đe dọa và điểm yếu, nhằm xác định các kịch bản sự cố liên quan. Cần phải nhấn mạnh, trong một số trường hợp thì có những mối đe dọa khác cũng có thể khai thác các điểm yếu này.

| Kiểu | Những ví dụ về các điểm yếu | Những ví dụ về các mối đe dọa |
|---|---|---|
| Phần cứng | Bảo trì thiết bị không đầy đủ/cài đặt lỗi các phương tiện lưu trữ | Vi phạm về bảo trì hệ thống thông tin |
| | Thiếu phương án thay thế định kỳ | Phá hủy thiết bị hoặc phương tiện thông tin |
| | Dễ ảnh hưởng bởi độ ẩm, bụi, bẩn | Bụi, ăn mòn, đóng băng |
| | Nhạy cảm với bức xạ điện từ | Bức xạ điện từ |
| | Thiếu biện pháp quản lý thay đổi cấu hình hiệu quả | Lỗi trong sử dụng |
| | Dễ ảnh hưởng bởi biến đổi điện áp | Mất nguồn cung cấp điện năng |
| | Dễ ảnh hưởng bởi thay đổi nhiệt độ | Hiện tượng khí tượng học |
| | Phần lưu trữ không được bảo vệ | Trộm cắp các phương tiện thông tin hoặc tài liệu |
| | Thiếu cẩn thận khi loại bỏ | Trộm cắp các phương tiện thông tin hoặc tài liệu |
| | Sao chép không được kiểm soát | Trộm cắp các phương tiện thông tin hoặc tài liệu |
| | Thiếu hoặc không kiểm thử thích đáng phần mềm | Lạm dụng quyền |
| | Lỗ hổng phổ biến trong phần mềm | Lạm dụng quyền |
| | Không "đăng xuất" khi rời khỏi máy trạm | Lạm dụng quyền |

| | | |
|---|---|---|
| Phần mềm | Loại bỏ hoặc tái sử dụng các phương tiện lưu trữ mà không xóa hết dữ liệu đúng cách | Lạm dụng quyền |
| | Thiếu các bản ghi phục vụ kiểm toán | Lạm dụng quyền |
| | Cấp sai quyền truy cập | Lạm dụng quyền |
| | Phần mềm phân phối quá rộng rãi | Sai lệch dữ liệu |
| | Áp dụng các chương trình ứng dụng cho các dữ liệu sai về mặt thời gian | Sai lệch dữ liệu |
| | Giao diện người dùng quá phức tạp | Lỗi trong sử dụng |
| | Thiếu tài liệu | Lỗi trong sử dụng |
| | Phạm vi thiết lập không chính xác | Lỗi trong sử dụng |
| | Ngày tháng không chính xác | Lỗi trong sử dụng |
| | Thiếu cơ chế nhận dạng và xác thực như xác thực người dùng | Giả mạo quyền |
| | Bảng mật khẩu không được bảo vệ | Giả mạo quyền |
| | Việc quản lý mật khẩu kém | Giả mạo quyền |
| | Kích hoạt những dịch vụ không cần thiết | Xử lý dữ liệu bất hợp pháp |
| | Phần mềm mới hoặc chưa chạy ổn định | Sai chức năng phần mềm |
| | Chỉ dẫn kỹ thuật cho những người phát triển phần mềm không rõ ràng hoặc không đầy đủ | Sai chức năng phần mềm |
| | Thiếu biện pháp quản lý thay đổi hiệu quả | Sai chức năng phần mềm |
| | Không kiểm soát được việc tải xuống và sử dụng phần mềm | Giả mạo phần mềm |
| | Thiếu bản sao lưu dự phòng | Giả mạo phần mềm |
| | Thiếu bảo vệ vật lí đối với tòa nhà, các cửa ra vào và cửa sổ | Trộm cắp các phương tiện hoặc tài liệu thông tin |
| | Lỗi khi đưa ra báo cáo quản lý | Sử dụng thiết bị trái phép |

| | | |
|---|---|---|
| Mạng | Thiếu bằng chứng về việc gửi hoặc nhận được một thông điệp | Từ chối hành động |
| | Đường truyền thông giao tiếp không được bảo vệ | Nghe trộm |
| | Luồng thông tin nhạy cảm không được bảo vệ | Nghe trộm |
| | Khớp nối cáp yếu | Lỗi các trang thiết bị viễn thông |
| | Điểm chịu lỗi duy nhất | Lỗi các trang thiết bị viễn thông |
| | Thiếu nhận diện và xác thực người gửi và người nhận | Giả mạo quyền |
| | Kiến trúc mạng không an toàn | Gián điệp từ xa |
| | Truyền đi những mật khẩu ở dạng rõ ràng (mật khẩu không được mã hóa) | Gián điệp từ xa |
| | Quản lý mạng không thích đáng | Tình trạng bão hòa của hệ thống thông tin |
| | Các kết nối mạng công cộng không được bảo vệ | Sử dụng trang thiết bị trái phép |
| Nhân sự | Sự vắng mặt của nhân viên | Vi phạm tính sẵn sàng của nhân viên |
| | Thủ tục tuyển dụng không đầy đủ | Phá hủy trang thiết bị hay phương tiện thông tin |
| | Đào tạo về an toàn không đầy đủ | Lỗi trong sử dụng |
| | Việc sử dụng phần mềm và phần cứng không đúng | Lỗi trong sử dụng |
| | Thiếu nhận thức về bảo mật | Lỗi trong sử dụng |
| | Thiếu cơ chế giám sát | Xử lý dữ liệu bất hợp pháp |
| | Thiếu giám sát công việc của nhân viên | Trộm cắp các phương tiện thông tin hoặc tài liệu |
| | Thiếu chính sách cho việc sử dụng đúng phương tiện thông tin viễn thông và thông điệp | Sử dụng trang thiết bị trái phép |
| | Không cẩn thận khi kiểm soát hay kiểm soát không đầy đủ sự vào ra tại | Phá hủy trang thiết bị hoặc phương tiện thông tin |

| | | |
|---|---|---|
| Địa điểm | các toàn nhà hay văn phòng | |
| | Vị trí ở một khu vực dễ bị lũ lụt | Lũ lụt |
| | Lưới điện không ổn định | Mất điện |
| | Thiếu sự bảo vệ đối với tòa nhà, các cửa ra vào và cửa sổ | Trộm cắp các trang thiết bị |
| Tổ chức | Thiếu thủ tục chính thức cho việc đăng ký và hủy đăng ký người dùng | Lạm dụng quyền |
| | Thiếu quy trình chính thức để xem xét (giám sát) quyền truy cập | Lạm dụng quyền |
| | Thiếu hoặc không có đầy đủ các quy định (liên quan đến an toàn) trong các hợp đồng với khách hàng và/hoặc các bên thứ ba | Lạm dụng quyền |
| | Thiếu thủ tục giám sát các phương tiện xử lý thông tin | Lạm dụng quyền |
| | Việc kiểm toán thiếu thường xuyên | Lạm dụng quyền |
| | Thiếu thủ tục nhận biết và đánh giá rủi ro | Lạm dụng quyền |
| | Thiếu ghi chép báo cáo khuyết điểm trong quản trị và vận hành | Lạm dụng quyền |
| | Việc đáp ứng bảo trì dịch vụ chưa thỏa đáng | Vi phạm về bảo trì hệ thống thông tin |
| | Thiếu hoặc không có đầy đủ các thỏa thuận mức dịch vụ | Vi phạm về bảo trì hệ thống thông tin |
| | Thiếu thủ tục kiểm soát sự thay đổi | Vi phạm về bảo trì hệ thống thông tin |
| | Thiếu thủ tục chính thức về kiểm soát ghi chép tài liệu ISMS | Sai lệch dữ liệu |
| | Thiếu thủ tục chính thức để giám sát bản ghi ISMS | Sai lệch dữ liệu |
| | Thiếu thủ tục chính thức cho việc xác thực các thông tin công khai sẵn có | Dữ liệu từ các nguồn không đáng tin |

| | | |
|---|---|---|
| | Thiếu phân bổ trách nhiệm an toàn thông tin phù hợp | Từ chối hành động |
| | Thiếu kế hoạch liên tục trong nghiệp vụ | Lỗi trang thiết bị |
| | Thiếu chính sách sử dụng thư điện tử | Lỗi trong sử dụng |
| | Thiếu thủ tục giới thiệu phần mềm trong hệ thống vận hành | Lỗi trong sử dụng |
| | Thiếu ghi chép bản ghi quản trị và vận hành | Lỗi trong sử dụng |
| | Thiếu thủ tục xử lý thông tin đã được phân loại | Lỗi trong sử dụng |
| | Thiếu trách nhiệm an toàn thông tin trong mô tả công việc | Lỗi trong sử dụng |
| | Thiếu hoặc không có đầy đủ những điều khoản (liên quan đến an toàn thông tin) trong các hợp đồng với người lao động | Xử lý dữ liệu bất hợp pháp |
| | Thiếu hoạt động xử lý kỷ luật trong trường hợp xảy ra sự cố an toàn thông tin | Trộm cắp các trang thiết bị |
| | Thiếu chính sách chính thức đối với việc sử dụng thiết bị máy tính di động | Trộm cắp các trang thiết bị |
| | Thiếu quyền kiểm soát các tài sản bên ngoài tổ chức | Trộm cắp các trang thiết bị |
| | Thiếu hoặc không có đầy đủ các chính sách đối với bàn làm việc và máy tính của nhân viên | Trộm cắp các phương tiện thông tin hoặc tài liệu |
| | Thiếu giấy phép của các tổ chức xử lý thông tin | Trộm cắp các phương tiện thông tin hoặc tài liệu |
| | Thiếu cơ chế giám sát đối với các vi phạm an toàn thông tin | Trộm cắp các phương tiện thông tin hoặc tài liệu |

| | | |
|---|---|---|
| | Việc xem xét quản lý thiếu thường xuyên | Sử dụng trang thiết bị trái phép |
| | Thiếu thủ tục cho việc báo cáo các điểm yếu về an toàn | Sử dụng trang thiết bị trái phép |
| | Thiếu các thủ tục và điều khoản liên quan đến quyền sở hữu trí tuệ (bản quyền) | Sử dụng phần mềm giả mạo hoặc đã bị sao chép |

## D.2 Phương pháp đánh giá các điểm yếu về kỹ thuật

Các phương pháp chủ động thực hiện trước tiên như kiểm thử hệ thống thông tin có thể được sử dụng nhằm nhận biết các điểm yếu thông tin dựa trên tính nguy cấp của hệ thống Công nghệ thông tin và Truyền thông (ICT) và các nguồn lực sẵn có (ví dụ: các nguồn vốn được phân bổ, công nghệ sẵn có, các cá nhân có kinh nghiệm tiến hành kiểm thử). Các phương pháp kiểm thử bao gồm:

- Công cụ quét điểm yếu tự động
- Kiểm thử và ước lượng an toàn
- Kiểm thử việc xâm nhập
- Soát xét mã

Công cụ quét điểm yếu tự động được sử dụng để quét một nhóm các máy hoặc một mạng nhằm tìm ra các điểm yếu của những dịch vụ này (ví dụ: hệ thống cho phép Giao thức truyền tập tin FTP nặc danh, chuyển tiếp gửi thư). Tuy nhiên, cần phải lưu ý rằng một vài điểm yếu tiềm ẩn được nhận biết bằng công cụ quét tự động không hẳn là các điểm yếu thật sự trong bối cảnh của môi trường hệ thống. Ví dụ: một vài công cụ quét đánh giá các điểm yếu tiềm ẩn mà không xem xét đến môi trường và các yêu cầu của địa điểm. Một số điểm yếu được cảnh báo bởi phần mềm quét tự động có thể không thực sự là điểm yếu đối với một địa điểm cụ thể nhưng có thể được cấu hình như vậy theo yêu cầu của môi trường. Do đó, phương pháp kiểm thử này có thể đưa ra kết quả sai.

Kiểm thử và ước lượng an toàn (STE) là một kỹ thuật khác mà có thể được sử dụng trong việc nhận biết các điểm yếu của hệ thống ICT trong suốt quy trình đánh giá rủi ro. Phương pháp này bao gồm việc phát triển và thực thi một kế hoạch kiểm thử (như kịch bản thử nghiệm, các quy trình kiểm thử và kết quả mong đợi). Mục đích của việc kiểm thử an toàn hệ thống là để kiểm thử tính hiệu quả của các biện pháp an toàn trong một hệ thống ICT khi chúng được áp dụng trong môi trường hoạt động. Mục tiêu là để đảm bảo các biện pháp được áp dụng đáp ứng được các tiêu chí kỹ thuật về an toàn đã được phê duyệt đối với phần cứng và phần mềm và triển khai chính sách an toàn thông tin cho tổ chức hoặc đáp ứng được các tiêu chuẩn công nghiệp.

Kiểm thử thâm nhập có thể được dùng để bổ sung cho việc soát xét các biện pháp an toàn và đảm bảo các khía cạnh khác nhau của hệ thống ICT được an toàn. Kiểm thử thâm nhập, khi được sử dụng trong quy trình đánh giá rủi ro, để đánh giá khả năng của một hệ thống ICT nhằm chống lại những hoạt

động cố gắng phá vỡ an toàn hệ thống. Mục tiêu của việc kiểm thử thâm nhập là để kiểm thử hệ thống ICT từ các nguồn hiểm họa và xác định được các lỗi tiềm ẩn trong các phương án bảo vệ hệ thống ICT.

Soát xét mã là phương pháp toàn diện nhất (nhưng cũng tốn kém nhất) để đánh giá điểm yếu.

Kết quả của những phương pháp kiểm thử trên sẽ giúp ích cho việc nhận biết các điểm yếu của một hệ thống.

Điều quan trọng cần lưu ý là các công cụ và kỹ thuật thâm nhập có thể cho kết quả sai, trừ khi điểm yếu được khai thác một cách thành công. Để khai thác các điểm yếu cụ thể thì một điều cần thiết là phải biết chính xác hệ thống/ứng dụng/bản vá lỗi được cài đặt trên hệ thống được kiểm thử. Nếu những dữ liệu đó không được biết đến tại thời điểm kiểm thử thì không có khả năng khai thác thành công điểm yếu cụ thể đó; tuy nhiên, vẫn có thể phá hỏng hoặc khởi động lại hệ thống hoặc quy trình đã được kiểm thử. Trong trường hợp này, đối tượng được kiểm thử cần phải được xem xét là có dễ bị gây hại hay không.

Các phương pháp có thể bao gồm các hoạt động sau:

- Phỏng vấn người dân và người sử dụng
- Bảng câu hỏi thăm dò ý kiến
- Điều tra thực tế
- Phân tích tài liệu

# Phụ lục E

(Tham khảo)

## Các phương pháp tiếp cận đánh giá rủi ro an toàn thông tin

### E.1 Đánh giá rủi ro an toàn thông tin ở mức cao

Đánh giá ở mức cao sẽ cho phép định nghĩa được trình tự và thứ tự ưu tiên cho các hành động. Vì nhiều lý do khác nhau, như ngân sách, nên không thể có khả năng triển khai tất cả các biện pháp đánh giá rủi ro cùng một lúc mà chỉ giải quyết những rủi ro nghiêm trọng nhất thông qua quy trình xử lý rủi ro. Có thể là vội vàng để bắt đầu việc quản lý rủi ro chi tiết nếu việc triển khai mới chỉ được vạch ra sau một hoặc hai năm. Để đạt được mục tiêu này, việc đánh giá ở mức cao có thể bắt đầu với việc đánh giá ở mức cao các hậu quả thay vì bắt đầu với việc phân tích có hệ thống các mối đe dọa, các điểm yếu, các tài sản và các hậu quả.

Một lý do khác để bắt đầu với việc đánh giá ở mức cao là đồng bộ các kế hoạch khác có liên quan đến việc thay đổi quản lý (hoặc liên tục trong nghiệp vụ). Ví dụ: sẽ không thể đảm bảo hoàn toàn an toàn cho một hệ thống hay ứng dụng nếu hệ thống hay ứng dụng đã được lên kế hoạch thuê ngoài trong tương lai gần, mặc dù có thể vẫn có giá trị khi thực hiện đánh giá rủi ro để xác định hợp đồng thuê ngoài.

Những đặc tính của chu trình lặp của việc đánh giá rủi ro ở mức cao có thể bao gồm:

- Đánh giá rủi ro ở mức cao có thể đưa ra một tầm nhìn toàn diện hơn về tổ chức và hệ thống thông tin của tổ chức, xem xét các khía cạnh công nghệ một cách độc lập với các vấn đề nghiệp vụ. Theo cách này thì việc phân tích bối cảnh sẽ tập trung nhiều vào nghiệp vụ và môi trường vận hành hơn so với các yếu tố công nghệ.
- Đánh giá rủi ro ở mức cao có thể giải quyết một danh sách hạn chế hơn các đe dọa và điểm yếu đã được nhóm lại trong những phạm vi xác định hoặc, để đẩy nhanh quy trình đánh giá, có thể tập trung vào các rủi ro hoặc các kịch bản tấn công thay vì tập trung vào các thành phần của chúng.
- Những rủi ro mà được thể hiện trong đánh giá rủi ro ở mức cao thường tổng quát hơn những rủi ro đã được nhận biết cụ thể. Bởi vì các kịch bản hay những mối đe dọa được nhóm trong những phạm vi nên việc xử lý rủi ro đưa ra danh sách những biện pháp quản lý trong phạm vi này. Các hoạt động xử lý rủi ro trước tiên đưa ra và chọn lựa các biện pháp phổ biến mà hợp lí cho toàn bộ hệ thống.
- Tuy nhiên, đánh giá rủi ro ở mức cao do ít khi giải quyết chi tiết về công nghệ nên phù hợp hơn trong việc đưa ra các biện pháp quản lý về mặt tổ chức và phi kỹ thuật và các khía cạnh quản lý của các biện pháp quản lý kỹ thuật, hoặc các biện pháp bảo vệ kỹ thuật chính và phổ biến như sao lưu và chống virus.

Ưu điểm của việc đánh giá rủi ro ở mức cao là:

- Kết hợp với một phương pháp tiếp cận đơn giản khởi đầu có thể sẽ đạt được sự chấp nhận của chương trình đánh giá rủi ro.

- Có thể xây dựng một hình ảnh chiến lược của một chương trình an toàn thông tin thuộc tổ chức, hoạt động như là một công cụ lập kế hoạch tốt.
- Các nguồn tài nguyên và tiền bạc có thể được sử dụng ở nơi có nhiều lợi ích nhất và những hệ thống có nhu cầu bảo vệ nhiều nhất sẽ được giải quyết trước tiên.

Do các phân tích rủi ro ban đầu ở mức cao và có khả năng kém chính xác hơn nên nhược điểm tiềm ẩn duy nhất chính là một số quy trình nghiệp vụ hoặc hệ thống có thể không được xác định là cần một đánh giá rủi ro chi tiết lần thứ hai. Điều này có thể tránh được nếu có đầy đủ thông tin về mọi khía cạnh của tổ chức, các thông tin và hệ thống của tổ chức, bao gồm cả những thông tin thu được từ việc đánh giá các sự cố an toàn thông tin.

Việc đánh giá rủi ro ở mức cao xem xét đến các giá trị nghiệp vụ của các tài sản thông tin và những rủi ro từ quan điểm nghiệp vụ của tổ chức. Tại điểm quyết định đầu tiên (xem Hình 2), một số yếu tố hỗ trợ cho việc quyết định liệu việc đánh giá ở mức cao có đủ để xử lý rủi ro hay không; các yếu tố này có thể bao gồm như sau:

- Các mục tiêu nghiệp vụ đạt được bằng việc sử dụng nhiều tài sản thông tin khác nhau;
- Mức nghiệp vụ của tổ chức phụ thuộc vào mỗi tài sản thông tin, tức là liệu các chức năng mà tổ chức xem là tối quan trọng đối với sự tồn tại của tổ chức hoặc hiệu quả quản lý nghiệp vụ có phụ thuộc vào từng tài sản hay không, hoặc có phụ thuộc vào tính bí mật, tính toàn vẹn, tính sẵn sàng, tính chống chối bỏ, trách nhiệm giải trình, tính xác thực và độ tin cậy của thông tin đã được lưu trữ và xử lý trên tài sản này hay không;
- Mức đầu tư đối với mỗi tài sản thông tin, về mặt phát triển, duy trì hoặc thay thế tài sản
- Các tài sản thông tin mà tổ chức trực tiếp định giá cho chúng.

Khi các yếu tố này được đánh giá, quyết định trở nên dễ dàng hơn. Nếu các mục tiêu của một tài sản là cực kỳ quan trọng đối với hoạt động nghiệp vụ của tổ chức, hoặc nếu các tài sản có độ rủi ro cao thì khi đó một chu trình lặp lại lần thứ hai, đánh giá rủi ro chi tiết, cần phải được tiến hành đối với tài sản thông tin cụ thể (hoặc một phần tài sản đó).

Một quy tắc chung để áp dụng là: nếu việc thiếu an toàn thông tin có thể dẫn đến những hậu quả gây thiệt hại lớn cho tổ chức, cho các hoạt động nghiệp vụ hoặc các tài sản của tổ chức đó thì quy trình lặp lại lần thứ hai của việc đánh giá rủi ro, ở mức chi tiết hơn, là cần thiết cho việc nhận biết các rủi ro tiềm ẩn.

### E.2 Đánh giá chi tiết rủi ro an toàn thông tin

Quy trình đánh giá chi tiết rủi ro an toàn thông tin liên quan đến việc nhận biết và định giá chuyên sâu về các tài sản, đánh giá các mối đe dọa đối với các tài sản đó và đánh giá các điểm yếu. Kết quả từ các hoạt động này được sử dụng để đánh giá những rủi ro và sau đó là nhận biết phương pháp xử lý rủi ro.

Bước chi tiết này thường đòi hỏi nhiều thời gian, công sức và chuyên môn và có thể là thích hợp nhất cho hệ thống thông tin có rủi ro ở mức cao.

Giai đoạn cuối cùng của việc đánh giá chi tiết rủi ro an toàn thông tin là đánh giá những rủi ro tổng thể, đó cũng là trọng tâm của Phụ lục này.

Các hậu quả có thể được đánh giá theo nhiều cách, kể cả bằng cách sử dụng phương pháp định lượng (ví dụ: tiền tệ) và phương pháp định tính (dựa trên việc sử dụng các tính từ chỉ mức như: "vừa phải" hay "rất nghiêm trọng"), hoặc kết hợp cả hai. Cần phải thiết lập khung thời gian đối với tài sản có giá trị hoặc cần được bảo vệ để đánh giá khả năng xảy ra mối đe dọa. Khả năng xảy ra một mối đe dọa cụ thể bị ảnh hưởng bởi những điều sau đây:

- Sự hấp dẫn của tài sản, hoặc tác động có thể xảy ra có thể áp dụng được khi một mối đe dọa có chủ ý của con người đang được xem xét
- Sự dễ dàng chuyển đổi việc khai thác một điểm yếu của tài sản thành lợi nhuận, có thể áp dụng được nếu một mối đe dọa có chủ ý của con người đang được xem xét
- Khả năng kỹ thuật của tác nhân mối đe dọa, có thể áp dụng đối với các mối đe dọa có chủ ý của con người và
- Tính nhạy cảm của các điểm yếu đối với việc khai thác, có thể áp dụng đối với cả điểm yếu kỹ thuật và phi kỹ thuật

Nhiều phương pháp sử dụng các bảng biểu và kết hợp các biện pháp chủ quan và đo lường thực nghiệm. Điều quan trọng là tổ chức sử dụng một phương pháp mà tổ chức cảm thấy dễ dàng khi triển khai mà vẫn đảm bảo tính bí mật cho tổ chức và sẽ đem lại những kết quả có thể lặp lại. Một vài ví dụ về các kỹ thuật dựa trên bảng biểu được đưa ra ở phần tiếp theo.

Xem thêm IEC 31010 để có những hướng dẫn bổ sung về các kỹ thuật được sử dụng cho việc đánh giá chi tiết rủi ro an toàn thông tin.

Những ví dụ sau sử dụng con số để mô tả các phương pháp đánh giá định tính. Người sử dụng những phương pháp này cần phải nhận thức được rằng việc thực hiện thêm các thao tác toán học sử dụng các con số là kết quả định tính được tạo ra bởi những phương pháp đánh giá rủi ro định tính có thể không hợp lệ.

### E.2.1 Ví dụ 1 - Ma trận với các giá trị đã được xác định trước

Trong phương pháp đánh giá rủi ro có sử dụng ma trận với các giá trị đã được xác định trước, những tài sản vật chất hiện có hoặc đã được đề xuất phải được định giá về mặt chi phí thay thế hoặc tái xây dựng (tức là sử dụng phương pháp đo định lượng). Các chi phí này sau đó được chuyển đổi vào cùng một thang đo định tính mà đã được sử dụng cho thông tin (xem bên dưới). Các tài sản phần mềm hiện có hoặc đã được đề xuất được định giá theo cùng một cách giống như tài sản vật chất, với chi phí mua hoặc tái xây dựng đã được nhận biết và sau đó được chuyển đổi vào cùng một thang đo định tính mà đã được sử dụng cho thông tin. Ngoài ra, nếu bất cứ phần mềm ứng dụng nào được nhận thấy là phải có thêm yêu cầu đảm bảo tính bí mật hay tính toàn vẹn (ví dụ với những mà nguồn thương mại là tài sản rất nhạy cảm) thì phải được định giá theo cùng một cách giống như đối với thông tin.

Các giá trị đối với thông tin thu được bằng cách phỏng vấn người quản lý nghiệp vụ được lựa chọn ("chủ sở hữu dữ liệu"), là những người phát ngôn có thẩm quyền về dữ liệu, để xác định giá trị và mức nhạy cảm của dữ liệu được sử dụng trong thực tế, hoặc được lưu trữ, xử lý hoặc truy cập. Các cuộc phỏng vấn tạo điều kiện cho việc đánh giá về giá trị và độ nhạy cảm của thông tin trong trường hợp kịch bản dự kiến xấu nhất xảy ra từ các hậu quả nghiệp vụ bất lợi do tiết lộ trái phép, thay đổi trái phép, tính không sẵn sàng cho những chu kì thời gian khác nhau và tiêu hủy.

Việc định giá được thực hiện bằng cách sử dụng các hướng dẫn về định giá thông tin, bao gồm các vấn đề như:

- An toàn cá nhận
- Thông tin riêng tư cá nhân
- Các nghĩa vụ về luật pháp và quy định
- Thi hành luật
- Lợi ích về thương mại và kinh tế
- Thiệt hại/gián đoạn về tài chính của các hoạt động
- Trật tự công cộng
- Chính sách nghiệp vụ và vận hành
- Đánh mất thiện chí
- Hợp đồng hoặc thoả thuận với khách hàng

Các hướng dẫn tạo điều kiện cho việc nhận biết giá trị trên một thang đo giá trị số, như thang đo từ 0 đến 4 được hiển thị trong ví dụ về ma trận dưới đây, do đó giúp xác định những giá trị định lượng khi có thể và hợp lôgic và các giá trị định tính nếu như không thể xác định giá trị định lượng, ví dụ như những mối đe dọa cho cuộc sống con người.

Hoạt động quan trọng tiếp theo là việc hoàn thành các cặp câu hỏi đối với từng loại mối đe dọa, đối với từng nhóm tài sản có liên quan đến từng loại mối đe dọa đó, để giúp cho việc đánh giá mức đe dọa (khả năng xảy ra) và mức điểm yếu (dễ dàng bị khai thác bởi các mối đe dọa gây ra các hậu quả xấu). Mỗi câu trả lời cho một câu hỏi được một điểm. Các điểm này được tích lũy thông qua một cơ sở tri thức và được đối chiếu với thang điểm. Dựa trên sự đối chiếu giữa điểm tích lũy với thang điểm sẽ cho chúng ta biết mức đe dọa từ mức cao xuống thấp và mức điểm yếu như trong ví dụ về ma trận dưới đây. Thông tin để hoàn thành bảng câu hỏi được thu thập từ những cuộc phỏng vấn với những người phụ trách về kỹ thuật, nhân sự và người dân và từ các cuộc kiểm tra vị trí vật lí và soát xét lại tài liệu.

Các giá trị tài sản, mức mối đe dọa và mức điểm yếu, tương ứng với từng loại hậu quả, có quan hệ phù hợp như trong ma trận dưới đây, sẽ xác định mỗi tổ hợp tương ứng với đo lường của rủi ro trong thang đo từ 0 đến 8. Các giá trị được đặt trong ma trận một cách có cấu trúc. Xem ví dụ ở bảng dưới đây:

**Bảng E.1 a)**

| | Khả năng xảy ra – mối đe dọa | Thấp (T) | | | Trung bình (TB) | | | Cao (C) | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Khả năng dễ bị khai thác (mức điểm yếu) | T | TB | C | T | TB | C | T | TB | C |
| Giá trị tài sản | 0 | 0 | 1 | 2 | 1 | 2 | 3 | 2 | 3 | 4 |
| | 1 | 1 | 2 | 3 | 2 | 3 | 4 | 3 | 4 | 5 |
| | 2 | 2 | 3 | 4 | 3 | 4 | 5 | 4 | 5 | 6 |
| | 3 | 3 | 4 | 5 | 4 | 5 | 6 | 5 | 6 | 7 |
| | 4 | 4 | 5 | 6 | 5 | 6 | 7 | 6 | 7 | 8 |

Đối với từng tài sản, cần phải xem xét các điểm yếu liên quan và các mối đe dọa tương ứng của từng tài sản này. Nếu có một điểm yếu mà không có mối đe dọa tương ứng, hoặc có một mối đe dọa mà không có điểm yếu tương ứng, thì không có rủi ro (nhưng cũng cần phải xem xét đến trường hợp khi tình huống này thay đổi). Trong bảng trên thì hàng tương ứng trong ma trận được nhận biết bởi giá trị tài sản và cột tương ứng được nhận biết bởi khả năng xảy ra mối đe dọa và khả năng dễ bị khai thác. Ví dụ, nếu tài sản có giá trị 3, mối đe dọa này là "cao" và điểm yếu là "thấp" thì đo lường cho rủi ro này là 5. Giả sử một tài sản có giá trị là 2, ví dụ như đối với việc thay đổi rủi ro, mức đe dọa là "thấp" và khả năng dễ bị khai thác là "cao", thì đo lường cho rủi ro là 4. Tùy theo nhu cầu của mỗi tổ chức mà có thể điều chỉnh kích thước của ma trận, về mặt số lượng các loại khả năng xảy ra mối đe dọa, các loại khả năng dễ bị khai thác và số lượng các loại định giá tài sản. Việc thêm các cột và các hàng sẽ đòi hỏi phải bổ sung thêm các phép đo rủi ro. Phương pháp tiếp cận này có giá trị trong việc xếp loại các rủi ro cần phải được giải quyết, xử lý.

Bảng E.1 b) dưới đây là một ma trận tương tự, có được từ việc xem xét khả năng xảy ra của một kịch bản sự cố, được sắp xếp theo tác động nghiệp vụ đã được ước đoán. Khả năng xảy ra của một kịch bản sự cố được đưa ra bởi một mối đe dọa khai thác một điểm yếu với một khả năng xảy ra nhất định. Bảng này thể hiện khả năng xảy ra của kịch bản sự cố và mức của tác động nghiệp vụ liên quan đến kịch bản sự cố đó. Kết quả rủi ro được đo thể hiện trên một thang đo từ 0 đến 8 mà có thể được ước lượng theo các tiêu chí chấp nhận rủi ro. Phạm vi rủi ro này cũng có thể được sắp xếp theo một tỉ lệ rủi ro tổng thể đơn giản, ví dụ như:

- Rủi ro mức thấp: 0-2
- Rủi ro mức trung bình: 3-5
- Rủi ro mức cao: 6-8

**Bảng E.1 b)**

| | Khả năng xảy ra của kịch bản sự cố | Rất thấp (Rất khó xảy ra) | Thấp (Khó xảy ra) | Trung bình (Có khả năng xảy ra) | Cao (Có thể xảy ra) | Rất cao (Thường xuyên xảy ra) |
|---|---|---|---|---|---|---|
| Tác động nghiệp vụ | Rất thấp | 0 | 1 | 2 | 3 | 4 |
| | Thấp | 1 | 2 | 3 | 4 | 5 |
| | Trung bình | 2 | 3 | 4 | 5 | 6 |
| | Cao | 3 | 4 | 5 | 6 | 7 |
| | Rất cao | 4 | 5 | 6 | 7 | 8 |

**E.2.2 Ví dụ 2 - Xếp hạng các mối đe dọa bằng đo lường rủi ro**

Một ma trận hoặc bảng như được thể hiện trong Bảng E.2 có thể được sử dụng để đưa ra các yếu tố của hậu quả (giá trị tài sản) và khả năng xảy ra mối đe dọa (ở đây chúng ta đang quan tâm đến khía cạnh là các điểm yếu). Bước đầu tiên là ước lượng hậu quả (giá trị tài sản) trên một thang đo đã được xác định trước, ví dụ: giá trị từ 1 đến 5 là ước lượng hậu quả của mỗi tài sản bị đe dọa (cột "b" trong bảng). Bước thứ hai là ước lượng khả năng xảy ra mối đe dọa trên một thang đo đã được nhận biết trước, ví dụ: giá trị từ 1 đến 5 là ước lượng khả năng xảy ra mối đe dọa của mỗi mối đe dọa (cột "c" trong bảng). Bước thứ ba là tính toán đo lường rủi ro bằng cách tính tích của 2 cột b và c (b x c). Cuối cùng, các mối đe dọa có thể được sắp xếp theo thứ tự gắn liền với mức rủi ro. Lưu ý, trong ví dụ này, số 1 trong cột b và c được coi như là hậu quả thấp nhất và khả năng thấp nhất xảy ra mối đe dọa.

**Bảng E.2**

| Mô tả mối đe dọa (a) | Hậu quả (giá trị tài sản) (b) | Khả năng xảy ra mối đe dọa (c) | Mức rủi ro (d) | Xếp loại đe dọa (e) |
|---|---|---|---|---|
| Đe dọa A | 5 | 2 | 10 | 2 |
| Đe dọa B | 2 | 4 | 8 | 3 |
| Đe dọa C | 3 | 5 | 15 | 1 |
| Đe dọa D | 1 | 3 | 3 | 5 |
| Đe dọa E | 4 | 1 | 4 | 4 |
| Đe dọa F | 2 | 4 | 8 | 3 |

Như bảng trên đã thể hiện, đây là phương pháp mà cho phép đối chiếu và sắp xếp theo thứ tự ưu tiên các mối đe dọa khác nhau mà có những hậu quả và khả năng xảy ra khác nhau. Trong một số trường hợp thì cần thiết kết hợp các giá trị tiền tệ với các thang đo thực nghiệm đã được sử dụng ở đây.

**E.2.3 Ví dụ 3 - Đánh giá giá trị đối với khả năng xảy ra và hậu quả có thể xảy ra của những rủi ro**

Ví dụ này nhấn mạnh vào những hậu quả của các sự cố an toàn thông tin (tức là các kịch bản sự cố) và xác định những hệ thống cần được ưu tiên. Điều này được thực hiện bằng cách đánh giá hai giá trị cho từng tài sản và rủi ro, kết hợp hai giá trị này sẽ xác định được số điểm cho từng tài sản. Khi tất cả các điểm của tài sản đối với hệ thống được tổng kết thì thước đo rủi ro của hệ thống đó được xác định.

Đầu tiên, gán giá trị cho mỗi tài sản. Mỗi giá trị này liên quan đến những hậu quả xấu tiềm ẩn mà có thể phát sinh nếu tài sản bị đe dọa. Đối với từng mối đe dọa có thể xảy ra đối với tài sản thì giá trị của tài sản phải được gán cho tài sản đó.

Tiếp theo là đánh giá giá trị khả năng xảy ra. Dựa vào khả năng xảy ra mối đe dọa và mức dễ dàng khai thác điểm yếu để đánh giá giá trị khả năng xảy ra, xem Bảng E.3 thể hiện khả năng xảy ra của một kịch bản sự cố.

**Bảng E.3**

| Khả năng xảy ra mối đe dọa | Thấp (T) | | | Trung bình (TB) | | | Cao (C) | | |
|---|---|---|---|---|---|---|---|---|---|
| Mức của điểm yếu | T | TB | C | T | TB | C | T | TB | C |
| Giá trị khả năng xảy ra của một kịch bản sự cố | 0 | 1 | 2 | 1 | 2 | 3 | 2 | 3 | 4 |

Tiếp theo, điểm của tài sản/mối đe dọa được tính bằng tổng của giá trị tài sản với giá trị khả năng xảy ra được thể hiện trong Bảng E.4. Điểm của tài sản/mối đe dọa được tính tổng để tạo ra điểm tổng của tài sản. Số liệu này có thể được sử dụng để phân biệt giữa các tài sản mà tạo ra bộ phận của một hệ thống.

**Bảng E.4**

| Giá trị tài sản | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| Giá trị khả năng xảy ra | | | | | |
| 0 | 0 | 1 | 2 | 3 | 4 |
| 1 | 1 | 2 | 3 | 4 | 5 |
| 2 | 2 | 3 | 4 | 5 | 6 |
| 3 | 3 | 4 | 5 | 6 | 7 |
| 4 | 4 | 5 | 6 | 7 | 8 |

Bước cuối cùng là tính tổng số điểm cho tất cả các tài sản của hệ thống, tạo ra điểm của hệ thống. Bước này được sử dụng để phân biệt giữa các hệ thống và để xác định thứ tự ưu tiên cho hệ thống bảo vệ.

Trong ví dụ sau, tất cả các giá trị đều được chọn một cách ngẫu nhiên.

Giả sử hệ thống S có ba tài sản là A1, A2 và A3; có hai mối đe dọa là T1 và T2 có thể xảy ra đối với hệ thống S. Đặt giá trị tài sản của A1 là 3, tương tự thế, đặt giá trị tài sản của A2 là 2 và giá trị tài sản của A3 là 4.

Nếu cho A1 và T1 có khả năng xảy ra mối đe dọa là thấp và khả năng dễ bị khai thác điểm yếu là ở mức trung bình thì khả năng này có giá trị là 1 (xem Bảng E.3).

Cặp điểm của tài sản/mối đe dọa (hay A1/T1) có thể được suy ra từ Bảng E.4: là giao điểm của giá trị tài sản là 3 và giá trị khả năng xảy ra là 1 thì giá trị từ Bảng E4 là 4. Tương tự thế, nếu cho A1/T2 có khả năng xảy ra mối đe dọa là trung bình và khả năng dễ bị khai thác điểm yếu là cao, thì điểm của A1/T2 là 6.

Và cuối cùng tổng điểm của tài sản A1/T được tính toán là 10. Tổng điểm của tài sản được tính toán cho từng tài sản và mối đe dọa có thể xảy ra. Tổng điểm của hệ thống được tính toán bằng cách cộng A1/T + A2/T + A3/T để đưa ra tổng S/T.

Các hệ thống khác nhau cũng như các tài sản khác nhau trong cùng một hệ thống có thể được đối chiếu để thiết lập thứ tự ưu tiên. Các ví dụ được thể hiện ở trên được áp dụng về mặt hệ thống thông tin, tuy nhiên phương pháp tiếp cận tương tự cũng có thể được áp dụng cho các hoạt động nghiệp vụ.

## Phụ lục F

(Tham khảo)

## Các ràng buộc thay đổi rủi ro

Trong khi xem xét những ràng buộc nhằm thay đổi rủi ro cần phải lưu ý xem xét đến các ràng buộc sau:

*Ràng buộc về thời gian:*

Có nhiều loại ràng buộc về thời gian. Ví dụ, các biện pháp cần phải được triển khai trong một khoảng thời gian chấp nhận được đối với những người quản lý của tổ chức. Một loại ràng buộc khác về thời gian là liệu một biện pháp có thể được triển khai trong khoảng thời gian tồn tại của thông tin hay hệ thống hay không. Loại ràng buộc thứ ba về thời gian là khoảng thời gian mà những người quản lý của tổ chức quyết định là một khoảng thời gian chấp nhận được khi tiếp xúc với một rủi ro cụ thể.

*Ràng buộc về tài chính:*

Các biện pháp được thiết kế để bảo vệ khi triển khai hoặc duy trì không được đắt hơn giá trị của những rủi ro, trừ trường hợp bắt buộc phải thực hiện (ví dụ như trong trường hợp tuân thủ theo pháp luật). Mọi cố gắng về tài chính được thực hiện đều không được vượt quá ngân sách được giao và đạt được lợi ích tài chính thông qua việc sử dụng các biện pháp. Tuy nhiên, trong một số trường hợp có thể không đạt được độ an toàn và mức chấp nhận rủi ro như mong muốn do bị ràng buộc về ngân sách. Bởi vậy, để giải quyết tình trạng này thì phụ thuộc vào quyết định của những người quản lý của tổ chức.

Cần phải hết sức cẩn thận trong trường hợp nếu như ngân sách của tổ chức làm giảm số lượng hay chất lượng của các biện pháp được triển khai, bởi vì điều này có thể dẫn đến việc duy trì rủi ro tiềm ẩn lớn hơn so với kế hoạch đã lập. Ngân sách được thiết lập cho các biện pháp nên được sử dụng như là một nhân tố giới hạn có sự xem xét tương đối.

*Ràng buộc về kỹ thuật:*

Các vấn đề về kỹ thuật, như là khả năng tương thích của các chương trình hay phần cứng, có thể dễ dàng tránh được nếu tất cả được xem xét trong suốt quá trình lựa chọn biện pháp. Ngoài ra, việc triển khai các biện pháp có hiệu lực trở về trước cho một quy trình hay hệ thống đang tồn tại thường bị cản trở bởi các ràng buộc kỹ thuật. Những khó khăn này có thể làm thay đổi sự cân bằng của các biện pháp về mặt an toàn thuộc về thủ tục và vật chất. Và cũng thật cần thiết để xem xét đến chương trình an toàn thông tin để đạt được các mục tiêu an toàn. Điều này có thể xảy ra khi các biện pháp không đáp ứng được những kết quả như mong muốn trong việc giảm thiểu rủi ro.

*Ràng buộc về vận hành:*

Những ràng buộc về vận hành như sự cần thiết để vận hành 24x7 nhưng vẫn cần thực hiện sao lưu kết quả có thể phức tạp và tốn kém hơn trừ khi chúng được xây dựng theo đúng thiết kế từ khi bắt đầu.

*Ràng buộc về văn hóa:*

Những ràng buộc về văn hóa để lựa chọn các biện pháp phù hợp có thể là đặc trưng của mỗi quốc gia, mỗi ngành, mỗi tổ chức hoặc thậm chí là của một bộ phận trong một tổ chức. Không phải tất cả các biện pháp đều có thể áp dụng được cho tất cả các nước. Ví dụ, có thể thực hiện các gói nghiên cứu ở các bộ phận của Châu Âu nhưng lại không thể áp dụng cho các bộ phận ở Trung Đông. Các khía cạnh về văn hóa không thể bỏ qua bởi vì rất nhiều biện pháp cần phải dựa vào sự hỗ trợ tích cực của các nhân viên. Nếu nhân viên không hiểu được sự cần thiết của các biện pháp hoặc không nhận ra biện pháp đó có được chấp nhận về mặt văn hóa hay không thì các biện pháp sẽ trở nên không hiệu quả theo thời gian.

*Ràng buộc về đạo đức:*

Những ràng buộc về đạo đức có thể gây tác động lớn đến các biện pháp như đạo đức thay đổi dựa vào các chuẩn mực xã hội. Điều này có thể cản trở việc triển khai các biện pháp như quét thư điện tử ở một số nước. Sự riêng tư của những thông tin có thể cũng thay đổi dựa vào quy tắc đạo đức của khu vực hay chính phủ. Điều này có thể được quan tâm nhiều hơn trong một số ngành công nghiệp so với những ngành khác, ví dụ như chính phủ và y tế.

*Ràng buộc về môi trường:*

Các yếu tố về môi trường có thể ảnh hưởng đến việc lựa chọn các biện pháp, chẳng hạn như không gian sẵn có, các điều kiện khí hậu khắc nghiệt, vị trí địa lý tự nhiên và đô thị bao quanh. Ví dụ, thử nghiệm diễn tập chống động đất có thể cần thiết đối với một vài nước này nhưng lại không cần thiết đối với một số nước khác.

*Ràng buộc về pháp lý:*

Các yếu tố về pháp lý như bảo vệ dữ liệu cá nhân hoặc các quy định của luật hình sự về xử lý thông tin có thể ảnh hưởng đến việc lựa chọn các biện pháp. Việc tuân thủ theo luật pháp và quy định có thể chỉ thị cho một số biện pháp bao gồm bảo vệ dữ liệu và kiểm toán tài chính; các yếu tố về pháp lý này cũng có thể ngăn chặn việc sử dụng một số biện pháp, ví dụ như mã hóa. Các quy định và điều luật khác như luật về quan hệ lao động, phòng cháy chữa cháy, y tế và an toàn và các quy định trong các ngành kinh tế... có thể cũng ảnh hưởng nhiều đến việc lựa chọn biện pháp.

*Tính dễ dàng sử dụng:*

Giao diện công nghệ kém thân thiện với người dùng sẽ dẫn đến những lỗi do con người và làm cho các biện pháp trở nên vô ích. Nên lựa chọn các biện pháp kiểm soát mà cung cấp tối ưu tính dễ sử dụng trong khi đạt được một mức rủi ro tồn đọng chấp nhận được đối với các nghiệp vụ. Các biện pháp kiểm soát khó sử dụng sẽ gây tác động đến hiệu quả của các biện pháp, bởi vì người sử dụng có thể cố ý phá hỏng hoặc bỏ qua chúng càng nhiều càng tốt. Các biện pháp truy cập phức tạp trong một tổ chức có thể khuyến khích người sử dụng tìm đến các phương pháp truy cập trái phép để thay thế.

*Ràng buộc về nhân sự:*

Cần phải xem xét đến tính sẵn sàng và chi phí tiền lương của các nhóm kĩ năng chuyên môn trong việc triển khai các biện pháp và cũng cần xem xét đến khả năng thuyên chuyển nhân viên giữa các vị trí trong những điều kiện làm việc không thuận lợi. Các chuyên gia có thể không phải lúc nào cũng sẵn sàng để triển khai các biện pháp đã được lên kế hoạch hoặc chi phí cho các chuyên gia quá tốn kém đối với tổ chức. Các khía cạnh khác như xu hướng của một vài nhân viên phân biệt với các nhân viên khác, những người mà không được thẩm tra về an toàn thông tin, có thể ảnh hưởng lớn đến các chính sách an toàn và các hoạt động thực tiễn. Cũng như vậy, nhu cầu thuê đúng người đối với từng công việc và tìm được đúng người có thể dẫn đến việc tuyển dụng trước khi hoàn thành việc thẩm tra về an toàn thông tin. Yêu cầu về việc hoàn thành thẩm tra an toàn thông tin trước khi tuyển dụng là bình thường, đúng thực tiễn và an toàn nhất.

*Ràng buộc của việc hợp nhất các biện pháp mới và các biện pháp hiện có:*

Việc hợp nhất các biện pháp mới vào cơ sở hạ tầng hiện có và sự phụ thuộc lẫn nhau giữa các biện pháp thường bị bỏ qua. Những biện pháp mới có thể không dễ dàng được thực hiện nếu có điểm vô lí hoặc không tương thích với các biện pháp hiện có. Ví dụ, một kế hoạch sử dụng thẻ sinh trắc học cho biện pháp kiểm soát truy cập vật lí có thể gây xung đột với hệ thống nhập mã PIN hiện có. Chi phí cho việc thay đổi các biện pháp từ các biện pháp hiện có sang các biện pháp đã được lập kế hoạch cần phải tính đến các yếu tố được thêm vào tổng chi phí của xử lý rủi ro. Có thể không có khả năng triển khai một biện pháp đã được lựa chọn do sự can thiệp của các biện pháp hiện có.

# Phụ lục G

(Tham khảo)

## Sự khác biệt về định nghĩa giữa ISO/IEC 27005:2008 và ISO/IEC 27005:2011

CHÚ THÍCH: Phụ lục này dành cho người sử dụng ISO/IEC 27001:2005. Do có sự khác biệt của một số thuật ngữ và định nghĩa trong TCVN 9788:2013 và ISO/IEC 27001:2005 và tiếp theo là ISO/IEC 27005:2008, Phụ lục này tóm tắt tất cả những thay đổi liên quan.

| Thuật ngữ được định nghĩa trong ISO/IEC 27005:2008 | Thuật ngữ được định nghĩa trong ISO/IEC 27000:2009 được sử dụng trong ISO/IEC 27005:2008 | Thuật ngữ được định nghĩa trong TCVN 9788:2013 được sử dụng trong TCVN ISO/IEC 27005:2011 |
|---|---|---|
| n/a | n/a | **3.1**<br>**Hậu quả (consequence)**<br>Kết quả của một **sự kiện** (3.3) gây ảnh hưởng đến các mục tiêu của tổ chức<br>[TCVN 9788:2013]<br>CHÚ THÍCH 1: Một sự kiện có thể dẫn đến một loạt các hậu quả.<br>CHÚ THÍCH 2: Một hậu quả có thể chắc chắn hoặc không chắc chắn xảy ra và trong bối cảnh an toàn thông tin thì thường mang nghĩa tiêu cực.<br>CHÚ THÍCH 3: Hậu quả có thể được thể hiện dưới dạng định tính hoặc định lượng.<br>CHÚ THÍCH 4: Hậu quả ban đầu có thể gây ảnh hưởng leo thang đến các hậu quả tiếp theo. |
| n/a | **Biện pháp (control)**<br>Phương pháp quản lý rủi ro, bao gồm những chính sách, thủ tục, hướng dẫn, phương pháp hoặc cấu trúc tổ chức, mà có thể quản trị kỹ thuật, quản lý, hoặc pháp | **3.2**<br>**Biện pháp kiểm soát (control)**<br>Biện pháp sẽ làm thay đổi **rủi ro** (3.9) |

| | | |
|---|---|---|
| | luật trong tự nhiên.<br>CHÚ THÍCH: Biện pháp cũng được sử dụng với nghĩa như biện pháp bảo vệ, biện pháp đối phó.<br>[TCVN ISO/IEC 27002:2011] | [TCVN 9788:2013]<br>CHÚ THÍCH 1: Biện pháp an toàn thông tin bao gồm bất kỳ quy trình, chính sách, thủ tục, hướng dẫn, phương pháp hoặc cấu trúc tổ chức trong các lĩnh vực hành chính, kỹ thuật, quản lý, hoặc pháp luật để thay đổi rủi ro an toàn thông tin.<br>CHÚ THÍCH 2: Biện pháp thay đổi rủi ro không phải lúc nào cũng phát huy tác dụng như mong đợi hoặc như giả định.<br>CHÚ THÍCH 3: Biện pháp cũng được sử dụng với nghĩa là biện pháp bảo vệ hoặc biện pháp đối phó. |
| n/a | n/a | **3.3**<br>**Sự kiện (event)**<br>Sự xuất hiện hoặc sự thay đổi của một tập hợp các tình huống cụ thể<br>[TCVN 9788:2013]<br>CHÚ THÍCH 1: Một sự kiện có thể xảy ra một hay nhiều lần và có thể do nhiều lý do khác nhau.<br>CHÚ THÍCH 2: Một sự kiện có thể bao gồm cả những sự việc không xảy ra.<br>CHÚ THÍCH 3: Một sự kiện đôi khi có thể được dùng theo nghĩa "sự cố" hay "sự rủi ro". |

| | | |
|---|---|---|
| n/a | n/a | **3.4**<br>**Bối cảnh bên ngoài (external context)**<br>Môi trường bên ngoài nơi mà tổ chức theo đuổi để đạt được các mục tiêu của mình<br>[TCVN 9788:2013]<br>CHÚ THÍCH: Bối cảnh bên ngoài có thể bao gồm:<br>- môi trường văn hóa, xã hội, chính trị, pháp lý, quy định, tài chính, công nghệ, kinh tế, môi trường tự nhiên và môi trường cạnh tranh, trong phạm vi quốc tế, quốc gia, khu vực hoặc địa phương;<br>- những xu hướng và động lực chính tác động đến những mục tiêu của tổ chức<br>- những mối quan hệ, những nhận thức và giá trị đối với các bên liên quan bên ngoài tổ chức đó. |
| **3.1**<br>**Tác động (impact)**<br>Thay đổi bất lợi tới mức của các mục tiêu nghiệp vụ | | Thuật ngữ này đã bị lược bỏ |
| **3.2**<br>**Rủi ro an toàn thông tin (information security risk)**<br>Khả năng một mối đe dọa đã có sẽ khai | | Thuật ngữ này đã bị lược bỏ (xem CHÚ THÍCH 6 theo 3.9) |

| | | |
|---|---|---|
| thác các điểm yếu an toàn thông tin của một hoặc một nhóm tài sản và do đó gây hại cho tổ chức<br>CHÚ THÍCH: Thuật ngữ này được hiểu theo nghĩa là một sự kết hợp giữa khả năng xảy ra một sự kiện và hậu quả của nó | | |
| **n/a** | **n/a** | **3.5**<br>**Bối cảnh nội bộ (internal context)**<br>Môi trường nội bộ nơi mà tổ chức theo đuổi để đạt được các mục tiêu của mình<br>[TCVN 9788:2013]<br>CHÚ THÍCH: Bối cảnh nội bộ có thể bao gồm:<br>- quản trị, cấu trúc tổ chức, vai trò và trách nhiệm giải trình;<br>- những chính sách, mục tiêu và chiến lược của tổ chức được đưa ra để đạt được mục đích;<br>- năng lực, được hiểu như là các nguồn lực và tri thức (Ví dụ như nguồn vốn, thời gian, con người, các quy trình, các hệ thống và các công nghệ);<br>- các hệ thống thông tin, luồng thông tin và quy trình đưa ra quyết định (cả chính thức và không chính thức); |

| | | |
|---|---|---|
| | | - những mối quan hệ với các bên liên quan bên trong tổ chức và những nhận thức và giá trị của các bên liên quan bên trong tổ chức đó;<br>- văn hóa của tổ chức;<br>- những tiêu chuẩn, hướng dẫn và mô hình mà tổ chức tuân thủ<br>- hình thức và phạm vi của những mối quan hệ bằng hợp đồng. |
| **n/a** | **n/a** | **3.6**<br>**Mức rủi ro (level of risk)**<br>Tính chất nghiêm trọng của một **rủi ro** (3.9) được hiểu theo nghĩa là sự kết hợp giữa **hậu quả** (3.1) và **khả năng xảy ra** (3.7) của một sự kiện.<br>[TCVN 9788:2013] |
| **n/a** | **n/a** | **3.7**<br>**Khả năng xảy ra (likelihood)**<br>Cơ hội xảy ra một sự kiện<br>[TCVN 9788:2013]<br>CHÚ THÍCH 1: Trong thuật ngữ quản lý rủi ro, từ "khả năng |

| | | |
|---|---|---|
| | | xảy ra" thường được dùng để chỉ cơ hội xảy ra một sự kiện, có thể được định nghĩa, được đo lường hay được xác định một cách chủ quan hay khách quan, dưới dạng định tính hay định lượng và được mô tả bằng cách sử dụng thuật ngữ chung hoặc bằng toán học (như xác suất hoặc tần suất trong một khoảng thời gian nhất định).<br>CHÚ THÍCH 2: Thuật ngữ "khả năng xảy ra" có nghĩa tương đương với thuật ngữ "xác suất". Tuy nhiên thuật ngữ "xác suất" thường chỉ hiểu theo nghĩa hẹp như là thuật ngữ toán học. Do đó, trong thuật ngữ quản lý rủi ro, "khả năng xảy ra" thường được sử dụng với mục đích giải thích như thuật ngữ "xác suất". |
| n/a | **Rủi ro tồn đọng (residual risk)**<br>Rủi ro tồn đọng sau xử lý rủi ro<br>[TCVN ISO/IEC 27001:2009] | **3.8**<br>**Rủi ro tồn đọng (residual risk)**<br>**Rủi ro** (3.9) còn lại sau khi **xử lý rủi ro** (3.17)<br>[TCVN 9788:2013]<br>CHÚ THÍCH 1: Rủi ro tồn đọng có thể gồm rủi ro chưa được nhận biết.<br>CHÚ THÍCH 2: Rủi ro tồn đọng cũng có thể được gọi là "rủi ro được giữ lại". |
| | **Rủi ro (risk)**<br>Sự kết hợp giữa khả năng của một sự kiện và hậu quả của sự kiện đó | **3.9**<br>**Rủi ro (risk)** |

| | | |
|---|---|---|
| | [TCVN ISO/IEC 27002:2011] | Ảnh hưởng của sự không chắc chắn đến các mục tiêu<br><br>[TCVN 9788:2013]<br><br>CHÚ THÍCH 1: Một ảnh hưởng là một sự sai lệch so với kỳ vọng – kết quả ảnh hưởng có thể là tích cực hay tiêu cực.<br><br>CHÚ THÍCH 2: Những mục tiêu có thể có những khía cạnh khác nhau (như khía cạnh về tài chính, y tế và an toàn, an toàn thông tin và những mục tiêu về môi trường) và có thể áp dụng ở các mức khác nhau (như chiến lược, tổ chức mở rộng, dự án, sản phẩm và quy trình).<br><br>CHÚ THÍCH 3: Rủi ro thường được đặc trưng bởi các sự kiện (3.3) và hậu quả (3.1) tiềm ẩn hoặc là sự kết hợp giữa chúng.<br><br>CHÚ THÍCH 4: Rủi ro an toàn thông tin thường được thể hiện bằng sự kết hợp giữa hậu quả của một sự kiện an toàn thông tin và khả năng xảy ra kèm theo.<br><br>CHÚ THÍCH 5: Sự không chắc chắn là tình trạng thiếu thông tin liên quan tới việc hiểu biết hoặc nhận thức về một sự kiện, hậu quả hay khả năng xảy ra sự kiện.<br><br>CHÚ THÍCH 6: Rủi ro an toàn thông tin liên quan đến những tiềm ẩn mà những mối đe dọa có thể khai thác những điểm yếu của một hoặc một nhóm tài sản thông tin hoặc và do đó gây ra thiệt hại đối với tổ chức. |

| | | |
|---|---|---|
| n/a | **Phân tích rủi ro (risk analysis)**<br>Việc sử dụng có hệ thống các thông tin để nhận biết nguồn gốc và ước lượng rủi ro<br>CHÚ THÍCH: Phân tích rủi ro cung cấp một nền tảng cho ước lượng rủi ro, xử lý rủi ro và chấp nhận rủi ro<br>[TCVN ISO/IEC 27001:2009] | **3.10**<br>**Phân tích rủi ro (risk analysis)**<br>Quy trình để hiểu bản chất của rủi ro và xác định **mức rủi ro** (3.6)<br>[TCVN 9788:2013]<br>CHÚ THÍCH 1: Phân tích rủi ro cung cấp cơ sở cho việc ước lượng rủi ro và quyết định cách xử lý rủi ro.<br>CHÚ THÍCH 2: Phân tích rủi ro bao gồm cả ước đoán rủi ro. |
| | **Đánh giá rủi ro (risk assessment)**<br>Quy trình tổng thể bao gồm phân tích rủi ro và ước lượng rủi ro<br>[TCVN ISO/IEC 27001:2009] | **3.11**<br>**Đánh giá rủi ro (risk assessment)**<br>Quy trình tổng thể bao gồm **nhận biết rủi ro** (3.15), **phân tích rủi ro** (3.10) và **ước lượng rủi ro** (3.14)<br>[TCVN 9788:2013] |
| **3.3**<br>**Tránh rủi ro (risk avoidance)**<br>Quyết định để không xảy ra hoặc hành động để tránh được một tình huống rủi ro an toàn thông tin | | Thuật ngữ này hiện đã được bao hàm trong thuật ngữ Xử lý rủi ro |

| | | |
|---|---|---|
| [ISO/IEC Guide 73:2002] | | |
| **3.4**<br>**Truyền thông rủi ro (risk communication)**<br>Sự trao đổi hoặc chia sẻ thông tin về rủi ro giữa người ra quyết định và những thành phần tham gia khác<br>[ISO/IEC Guide 73:2002] | | **3.12**<br>**Truyền thông và tư vấn rủi ro (risk communication and consultation)**<br>Những quy trình liên tục và lặp đi lặp lại mà tổ chức tiến hành để cung cấp, chia sẻ hay thu nhận thông tin và tiến hành đối thoại với **những bên liên quan** (3.18) về quản lý **rủi ro** (3.9)<br>[TCVN 9788:2013]<br>CHÚ THÍCH 1: Thông tin có thể liên quan đến sự tồn tại, bản chất, hình thức, khả năng xảy ra, tầm quan trọng, việc ước lượng, khả năng chấp nhận và xử lý rủi ro.<br>CHÚ THÍCH 2: Tư vấn là một quy trình truyền thông hai chiều giữa tổ chức đó với những bên liên quan về một vấn đề trước khi đưa ra quyết định hoặc xác định định hướng về vấn đề đó. Tư vấn là:<br>- một quy trình tác động đến quyết định thông qua những ảnh hưởng hơn là thông qua quyền lực;<br>- là đầu vào để ra quyết định, nhưng không tham gia vào quá trình ra quyết định. |
| n/a | n/a | **3.13** |

| | | |
|---|---|---|
| | | **Tiêu chí rủi ro (risk criteria)**<br>Điều khoản tham chiếu mà dựa vào đó để ước lượng mức nghiêm trọng của **rủi ro** (3.9)<br>[TCVN 9788:2013]<br>CHÚ THÍCH 1: Tiêu chí rủi ro dựa vào những mục tiêu, bối cảnh nội bộ và bối cảnh bên ngoài của tổ chức.<br>CHÚ THÍCH 2: Tiêu chí rủi ro có thể được bắt nguồn từ những tiêu chuẩn, luật, chính sách và các yêu cầu khác. |
| **3.5**<br>**Ước đoán rủi ro (risk estimation)**<br>Quy trình ấn định các giá trị cho khả năng xuất hiện và hậu quả của rủi ro<br>[ISO/IEC Guide 73:2002]<br>CHÚ THÍCH 1: Trong bối cảnh của tiêu chuẩn này, thuật ngữ "activity" được sử dụng thay cho thuật ngữ "process" trong ước lượng rủi ro<br>CHÚ THÍCH 2: Trong bối cảnh của tiêu chuẩn này, thuật ngữ "likelihood" được sử dụng thay cho thuật ngữ "probability" trong ước lượng rủi ro | | Thuật ngữ này đã bị lược bỏ |

| | | |
|---|---|---|
| n/a | **Ước lượng rủi ro (risk evaluation)**<br>Quy trình đối chiếu rủi ro đã được ước đoán với tiêu chí rủi ro cho trước để xác định tầm ảnh hưởng của rủi ro<br>[TCVN ISO/IEC 27001:2009] | **3.14**<br>**Ước lượng rủi ro (risk evaluation)**<br>Quy trình đối chiếu kết quả của việc **phân tích rủi ro** (3.10) với các **tiêu chí rủi ro** (3.13) để xác định xem rủi ro đó và/hoặc mức nghiêm trọng của rủi ro đó có thể chấp nhận hoặc chịu đựng được hay không.<br>[TCVN 9788:2013]<br>CHÚ THÍCH: Ước lượng rủi ro hỗ trợ việc quyết định cách xử lý rủi ro. |
| **3.6**<br>**Nhận biết rủi ro (risk identification)**<br>Quy trình tìm kiếm, liệt kê và đưa ra các yếu tố đặc tính của rủi ro<br>[ISO/IEC Guide 73:2002]<br>CHÚ THÍCH: Trong bối cảnh của tiêu chuẩn này, thuật ngữ "activity" được sử dụng thay cho thuật ngữ "process" trong việc nhận biết rủi ro | | **3.15**<br>**Nhận biết rủi ro (risk identification)**<br>Quy trình tìm kiếm, nhận dạng và mô tả rủi ro<br>[TCVN 9788:2013]<br>CHÚ THÍCH 1: Nhận biết rủi ro bao gồm nhận biết về nguồn gốc của rủi ro, các sự kiện, những nguyên nhân và hậu quả tiềm ẩn của chúng.<br>CHÚ THÍCH 2: Nhận biết rủi ro có thể liên quan đến dữ liệu trong quá khứ, phân tích lý thuyết, thông tin và ý kiến chuyên môn và nhu cầu của các bên liên quan. |

| | | |
|---|---|---|
| n/a | **Quản lý rủi ro (risk management)**<br>Các hoạt động điều phối để chỉ đạo và kiểm soát tổ chức về vấn đề rủi ro | **3.16**<br>**Quản lý rủi ro (risk management)**<br>Hoạt động phối hợp về vấn đề rủi ro để điều hành và kiểm soát tổ chức<br>[TCVN 9788:2013]<br>CHÚ THÍCH: Tiêu chuẩn này sử dụng thuật ngữ "quy trình" để mô tả tổng quan việc quản lý rủi ro. Các yếu tố bên trong quy trình quản lý rủi ro được gọi là "các hoạt động". |
| **3.7**<br>**Giảm nhẹ rủi ro (risk reduction)**<br>Các hành động để giảm khả năng có thể xảy ra, các hậu quả tiêu cực, hoặc cả hai, có liên quan đến rủi ro<br>[ISO/IEC Guide 73:2002]<br>CHÚ THÍCH: Trong bối cảnh của tiêu chuẩn này, thuật ngữ "likelihood" được sử dụng thay cho thuật ngữ "probability" trong giảm nhẹ rủi ro | | Thuật ngữ này đã được thay thế bằng thuật ngữ "thay đổi rủi ro" và hiện tại được bao hàm trong thuật ngữ "xử lý rủi ro" |
| **3.8**<br>**Duy trì rủi ro (risk retention)**<br>Việc chấp nhận gánh nặng thiệt hại hoặc lợi ích thu được từ việc duy trì một rủi ro cụ thể | | Thuật ngữ này hiện tại được bao hàm trong thuật ngữ "xử lý rủi ro" |

| | | |
|---|---|---|
| [ISO/IEC Guide 73:2002]<br>CHÚ THÍCH: Trong bối cảnh rủi ro an toàn thông tin, chỉ các hậu quả tiêu cực (các thiệt hại) được xem xét khi duy trì rủi ro | | |
| **3.9**<br>**Truyền rủi ro (risk transfer)**<br>Việc chia sẻ với các bên khác về gánh nặng thiệt hại hoặc lợi ích thu được từ một rủi ro<br>CHÚ THÍCH: Trong bối cảnh rủi ro an toàn thông tin, chỉ các hậu quả tiêu cực (các thiệt hại) được xem xét khi truyền rủi ro | | Thuật ngữ này được thay thế bởi thuật ngữ "chia sẻ rủi ro" và hiện tại được bao hàm trong thuật ngữ "xử lý rủi ro" |
| **n/a** | **Xử lý rủi ro (risk treatment)**<br>Quy trình lựa chọn và triển khai các biện pháp thay đổi rủi ro<br>CHÚ THÍCH: Trong tiêu chuẩn này thuật ngữ "control" (biện pháp) được sử dụng tương đương với thuật ngữ "measure"<br>[TCVN ISO/IEC 27001:2009] | **3.17**<br>**Xử lý rủi ro (risk treatment)**<br>Quá trình điều chỉnh rủi ro<br>[TCVN 9788:2013]<br>CHÚ THÍCH 1: Xử lý rủi ro có thể liên quan đến việc:<br>- tránh rủi ro bằng cách quyết định không bắt đầu hoặc tiếp tục việc hoạt động làm tăng thêm rủi ro;<br>- chấp nhận hoặc làm tăng rủi ro để theo đuổi một cơ hội;<br>- loại bỏ nguồn gốc rủi ro; |

| | | |
|---|---|---|
| | | - thay đổi khả năng xảy ra;<br>- thay đổi hậu quả;<br>- chia sẻ rủi ro với một bên hay nhiều bên khác (bao gồm cả hợp đồng và gây quỹ bồi thường rủi ro.<br>- Duy trì rủi ro bằng lựa chọn có hiểu biết.<br>CHÚ THÍCH 2: Xử lý rủi ro để giải quyết các hậu quả tiêu cực đôi khi được gọi là "giảm nhẹ rủi ro", "loại bỏ rủi ro", "ngăn chặn rủi ro" và "giảm bớt rủi ro".<br>CHÚ THÍCH 3: Xử lý rủi ro có thể tạo ra những rủi ro mới hoặc làm thay đổi những rủi ro hiện có. |
| n/a | n/a | **3.18**<br>**Bên liên quan (stakeholder)**<br>Cá nhân hay tổ chức có thể gây ảnh hưởng, bị ảnh hưởng, hoặc nhận thấy bị ảnh hưởng bởi một quyết định hay một hành động<br>[TCVN 9788:2013]<br>CHÚ THÍCH: Người đưa ra quyết định có thể là một bên liên quan. |

| | | |
|---|---|---|
| | **Mối đe dọa (threat)**<br>Một nguyên nhân tiềm ẩn từ một sự cố không mong muốn, có thể gây hại cho hệ thống hoặc tổ chức | Áp dụng định nghĩa như trong ISO/IEC 27000:2009 |

## Thư mục tài liệu tham khảo


[1] ISO/IEC 27005:2011, Information technology – Security techniques – Information security risk management

[2] ISO/IEC 27000, Information technology – Security techniques – Information security management systems – Overview and vocabulary

[3] TCVN ISO/IEC 27001:2009, Công nghệ thông tin – Các kỹ thuật an toàn – Hệ thống quản lý an toàn thông tin – Các yêu cầu

[4] TCVN ISO/IEC 27002:2011, Công nghệ thông tin – Các kỹ thuật an toàn – Quy tắc thực hành quản lý an toàn thông tin

[5] TCVN 9788:2013, Quản lý rủi ro – Từ vựng

[6] ISO/IEC 16085:2006, Systems and software engineering – Life cycle processes – Risk management

[7] AS/NZS 4360:2004, Risk Management

[8] NIST Special Publication 800-12, An Introduction to Computer Security: The NIST Handbook

[9] NIST Special Publication 800-30, Risk Management Guide for Information Technology Systems, Recommendations of the National Institute of Standards and Technology.