TCVN **T I Ê U C H U Ẩ N Q U Ố C G I A**

TCVN 10541:2014
ISO/IEC 27003:2010

Xuất bản lần 1

CÔNG NGHỆ THÔNG TIN – CÁC KỸ THUẬT AN TOÀN – HƯỚNG DẪN TRIỂN KHAI HỆ THỐNG QUẢN LÝ AN TOÀN THÔNG TIN

Information technology – Security techniques – Information security management system implementation guidance

HÀ NỘI – 2014

Mục lục

1 Phạm vi áp dụng 7
2 Tài liệu viện dẫn 7
3 Thuật ngữ và định nghĩa 8
4 Cấu trúc tiêu chuẩn 8
4.1 Cấu trúc chung của các điều 8
4.2 Cấu trúc chung của từng điều 9
4.3 Biểu đồ 10
5 Phê chuẩn cho khởi động dự án ISMS 12
5.1 Tổng quan về cách thức để được phê chuẩn cho khởi động dự án ISMS 12
5.2 Làm rõ các ưu tiên của tổ chức cho phát triển ISMS 14
5.3 Xác định phạm vi ISMS sơ bộ 17
5.3.1 Phát triển phạm vi ISMS sơ bộ 17
5.3.2 Xác định vai trò và trách nhiệm đối với phạm vi ISMS sơ bộ 18
5.4 Xây dựng tình huống nghiệp vụ và kế hoạch dự án trình ban quản lý phê chuẩn 19
6 Xác định phạm vi, các giới hạn và chính sách ISMS 21
6.1 Tổng quan về xác định phạm vi, các giới hạn và chính sách ISMS 21
6.2 Xác định phạm vi và các giới hạn về tổ chức 24
6.3 Xác định phạm vi và các giới hạn về công nghệ thông tin và truyền thông (ICT) 25
6.4 Xác định phạm vi và các giới hạn vật lý 27
6.5 Phối hợp phạm vi và các giới hạn để nhận được phạm vi và các giới hạn ISMS 28
6.6 Phát triển chính sách ISMS và được ban quản lý phê chuẩn 28
7 Tiến hành phân tích các yêu cầu an toàn thông tin 30
7.1 Tổng quan về tiến hành phân tích các yêu cầu an toàn thông tin 30
7.2 Xác định các yêu cầu an toàn thông tin cho quy trình ISMS 32
7.3 Xác định các tài sản thuộc phạm vi ISMS 33
7.4 Tiến hành đánh giá an toàn thông tin 34
8 Tiến hành đánh giá rủi ro và lập kế hoạch xử lý rủi ro 36
8.1 Tổng quan về tiến hành đánh giá rủi ro và lập kế hoạch xử lý rủi ro 36
8.2 Tiến hành đánh giá rủi ro 38
8.3 Chọn lựa mục tiêu và biện pháp quản lý 39
8.4 Phê chuẩn cho triển khai và vận hành ISMS 40
9 Thiết kế ISMS 41
9.1 Tổng quan về thiết kế ISMS 41
9.2 Thiết kế an toàn thông tin về tổ chức 45
9.2.1 Thiết kế cơ cấu tổ chức chính thức cho an toàn thông tin 45
9.2.2 Thiết kế cấu trúc khung hệ thống tài liệu về ISMS 46

9.2.3 Thiết kế chính sách an toàn thông tin 48
9.2.4 Phát triển các tiêu chuẩn và thủ tục an toàn thông tin 49
9.3 Thiết kế an toàn thông tin vật lý và ICT 51
9.4 Thiết kế an toàn thông tin ISMS cụ thể 53
9.4.1 Lập kế hoạch soát xét của ban quản lý 53
9.4.2 Thiết kế chương trình giáo dục, đào tạo và nâng cao nhận thức về an toàn thông tin ... 55
9.5 Đưa ra kế hoạch dự án ISMS chính thức 57
Phụ lục A (tham khảo): Danh sách các hoạt động 59
Phụ lục B (tham khảo): Các vai trò và trách nhiệm về an toàn thông tin 67
Phụ lục C (tham khảo): Thông tin về đánh giá nội bộ 72
Phụ lục D (tham khảo): Cấu trúc của các chính sách 74
Phụ lục E (tham khảo): Giám sát và đo lường 79
Thư mục tài liệu tham khảo 86

Lời nói đầu

TCVN 10541:2014 hoàn toàn tương đương với ISO/IEC 27003:2010

TCVN 10541:2014 do Viện Khoa học Kỹ thuật Bưu điện biên soạn, Bộ Thông tin và truyền thông tổ chức xây dựng và 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 – Hướng dẫn triển khai hệ thống quản lý an toàn thông tin

Information technology - Security techniques - Information security management system implementation guidance

1 Phạm vi áp dụng

Tiêu chuẩn này tập trung vào các khía cạnh then chốt để thiết kế và triển khai thành công một hệ thống quản lý an toàn thông tin (ISMS) theo TCVN ISO/IEC 27001:2009 (ISO/IEC 27001:2005). Tiêu chuẩn này mô tả quy trình đặc tả và thiết kế ISMS từ lúc khởi đầu đến khi đưa ra các kế hoạch triển khai. Tiêu chuẩn này cũng mô tả quy trình để được ban quản lý phê chuẩn cho triển khai ISMS, xác định một dự án triển khai ISMS (trong tiêu chuẩn này được gọi là dự án ISMS), và đưa ra hướng dẫn lập kế hoạch dự án ISMS để có được kế hoạch triển khai dự án ISMS chính thức.

Tiêu chuẩn này dành cho các tổ chức triển khai ISMS. Tiêu chuẩn này có thể áp dụng cho tất cả các tổ chức ở mọi loại hình (ví dụ, các doanh nghiệp thương mại, các cơ quan chính phủ, các tổ chức phi lợi nhuận) với đủ loại quy mô. Mỗi tổ chức có tính phức tạp và các rủi ro riêng, và các yêu cầu cụ thể của tổ chức sẽ chi phối việc triển khai ISMS. Các tổ chức có quy mô nhỏ sẽ nhận thấy các hoạt động được đưa ra trong tiêu chuẩn này đều có thể áp dụng cho họ và có thể được đơn giản hóa hơn nữa. Các tổ chức phức hợp hoặc quy mô lớn có thể nhận thấy cần phải có một hệ thống quản lý hoặc tổ chức theo phân cấp để quản lý các hoạt động trong tiêu chuẩn này một cách hiệu quả. Tuy nhiên, cả hai loại tổ chức đều có thể áp dụng tiêu chuẩn này để lập kế hoạch cho các hoạt động phù hợp.

Tiêu chuẩn này đưa ra các khuyến nghị và giải thích, không chỉ rõ các yêu cầu cụ thể. Tiêu chuẩn này được sử dụng phối hợp với TCVN ISO/IEC 27001:2009 (ISO/IEC 27001:2005) và TCVN ISO/IEC 27002:2011 (ISO/IEC 27002:2005), nhưng không chủ ý thay đổi và/hoặc giảm bớt các yêu cầu trong TCVN ISO/IEC 27001:2009 (ISO/IEC 27001:2005) hoặc các khuyến nghị trong TCVN ISO/IEC 27002:2011 (ISO/IEC 27002:2005). Không cần thiết hợp chuẩn theo tiêu chuẩn này.

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 phiên 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).

ISO/IEC 27000:2009, 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 (ISO/IEC 27001:2005), Công nghệ thông tin - Hệ thống quản lý an toàn thông tin – Các yêu cầu.

3 Thuật ngữ và định nghĩa

Tiêu chuẩn này sử dụng các thuật ngữ và định nghĩa nêu trong ISO/IEC 27000:2009, TCVN ISO/IEC 27001:2009 (ISO/IEC 27001:2005) và thuật ngữ, định nghĩa sau:

3.1

Dự án ISMS (ISMS project)

Các hoạt động có cấu trúc được một tổ chức thực hiện để triển khai ISMS.

4 Cấu trúc tiêu chuẩn

4.1 Cấu trúc chung của các điều

Triển khai ISMS là một hoạt động quan trọng và nhìn chung được thực hiện như một dự án trong mỗi tổ chức. Tiêu chuẩn này giải thích quá trình triển khai ISMS tập trung vào việc khởi động, lập kế hoạch và xác định dự án. Quy trình lập kế hoạch triển khai ISMS chính thức gồm năm giai đoạn và mỗi giai đoạn được thể hiện trong một điều. Tất cả các điều đều có cấu trúc giống nhau như mô tả dưới đây. Năm giai đoạn bao gồm:

a) Phê chuẩn cho khởi động dự án ISMS (Điều 5);

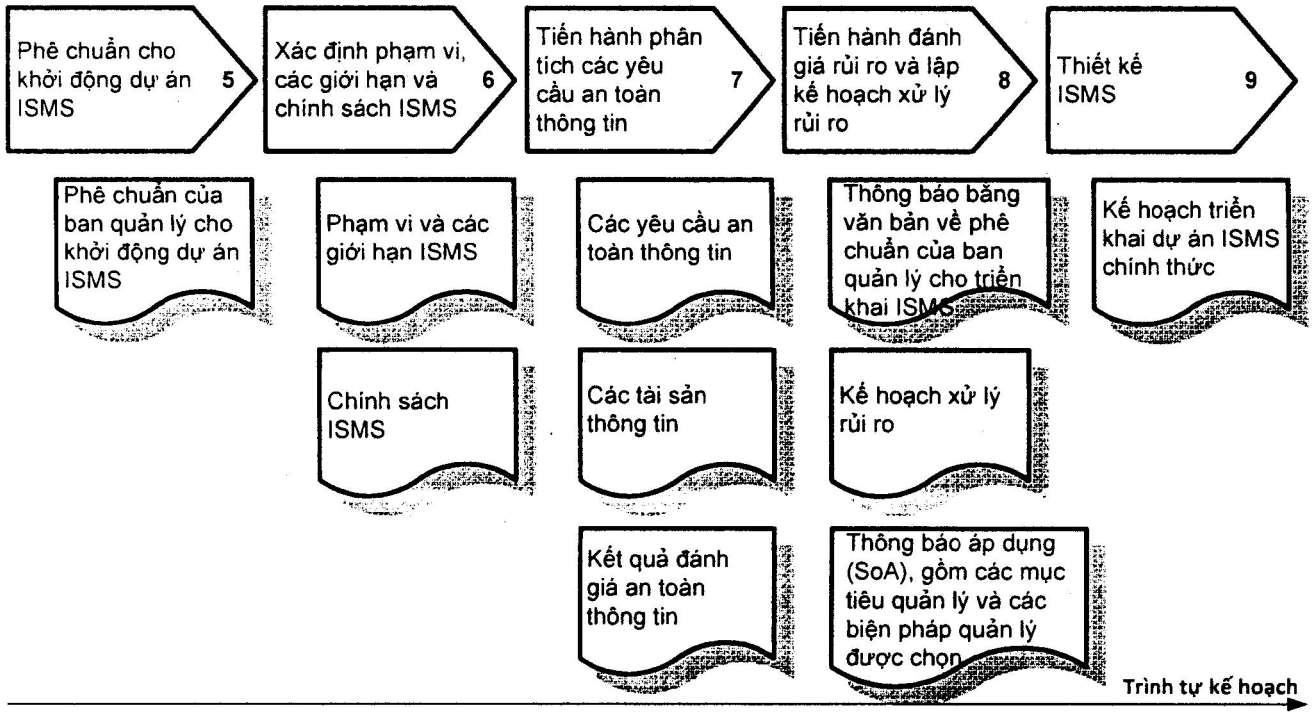
b) Xác định phạm vi ISMS và chính sách ISMS (Điều 6);

c) Tiến hành phân tích các yêu cầu an toàn thông tin (Điều 7);

d) Tiến hành đánh giá rủi ro và lập kế hoạch xử lý rủi ro (Điều 8);

e) Thiết kế ISMS (Điều 9).

Hình 1 mô tả năm giai đoạn trong quy trình lập kế hoạch dự án ISMS theo các tiêu chuẩn ISO/IEC và các tài liệu đầu ra chính.



Hình 1 - Các giai đoạn của dự án ISMS

Thông tin chi tiết được đề cập trong các phụ lục sau:

Phụ lục A – Tóm tắt các hoạt động có tham chiếu TCVN ISO/IEC 27001:2009 (ISO/IEC 27001:2005)

Phụ lục B – Các vai trò và trách nhiệm về an toàn thông tin

Phụ lục C – Thông tin về lập kế hoạch đánh giá nội bộ

Phụ lục D – Cấu trúc các chính sách

Phụ lục E – Thông tin về lập kế hoạch giám sát và đo lường

4.2 Cấu trúc chung của từng điều

Mỗi điều bao gồm:

a) một hoặc nhiều mục tiêu thể hiện nội dung cần đạt, được ghi chú trong hộp văn bản ở phần đầu mỗi điều; và

b) một hoặc nhiều hoạt động cần thiết để đạt được (các) mục tiêu của giai đoạn đó.

Mỗi hoạt động được mô tả trong một điều nhỏ.

Các mô tả hoạt động trong từng điều nhỏ được cấu trúc như sau:

Hoạt động

Phần *Hoạt động* xác định điều cần thỏa mãn để đạt được toàn bộ hoặc một phần các mục tiêu của giai đoạn.

Đầu vào

Phần *Đầu vào* mô tả xuất phát điểm, ví dụ các quyết định đã có trong các văn bản hoặc các đầu ra từ các hoạt động khác được mô tả trong tiêu chuẩn. Các đầu vào có thể được tham chiếu tới toàn bộ đầu ra từ một hoạt động liên quan hoặc thông tin cụ thể từ một hoạt động có thể được bổ sung sau điều tham chiếu.

Hướng dẫn

Phần *Hướng dẫn* cung cấp thông tin chi tiết cho phép thực hiện hoạt động này. Một số hướng dẫn có thể không phù hợp cho mọi trường hợp và có thể có các cách khác phù hợp hơn để đạt được các kết quả dự kiến.

Đầu ra

Phần *Đầu ra* mô tả (các) kết quả hoặc (các) sản phẩm thu được khi hoạt động này hoàn thành; ví dụ, một văn bản. Các đầu ra đều giống nhau và không phụ thuộc vào quy mô của tổ chức hoặc phạm vi ISMS.

Thông tin khác

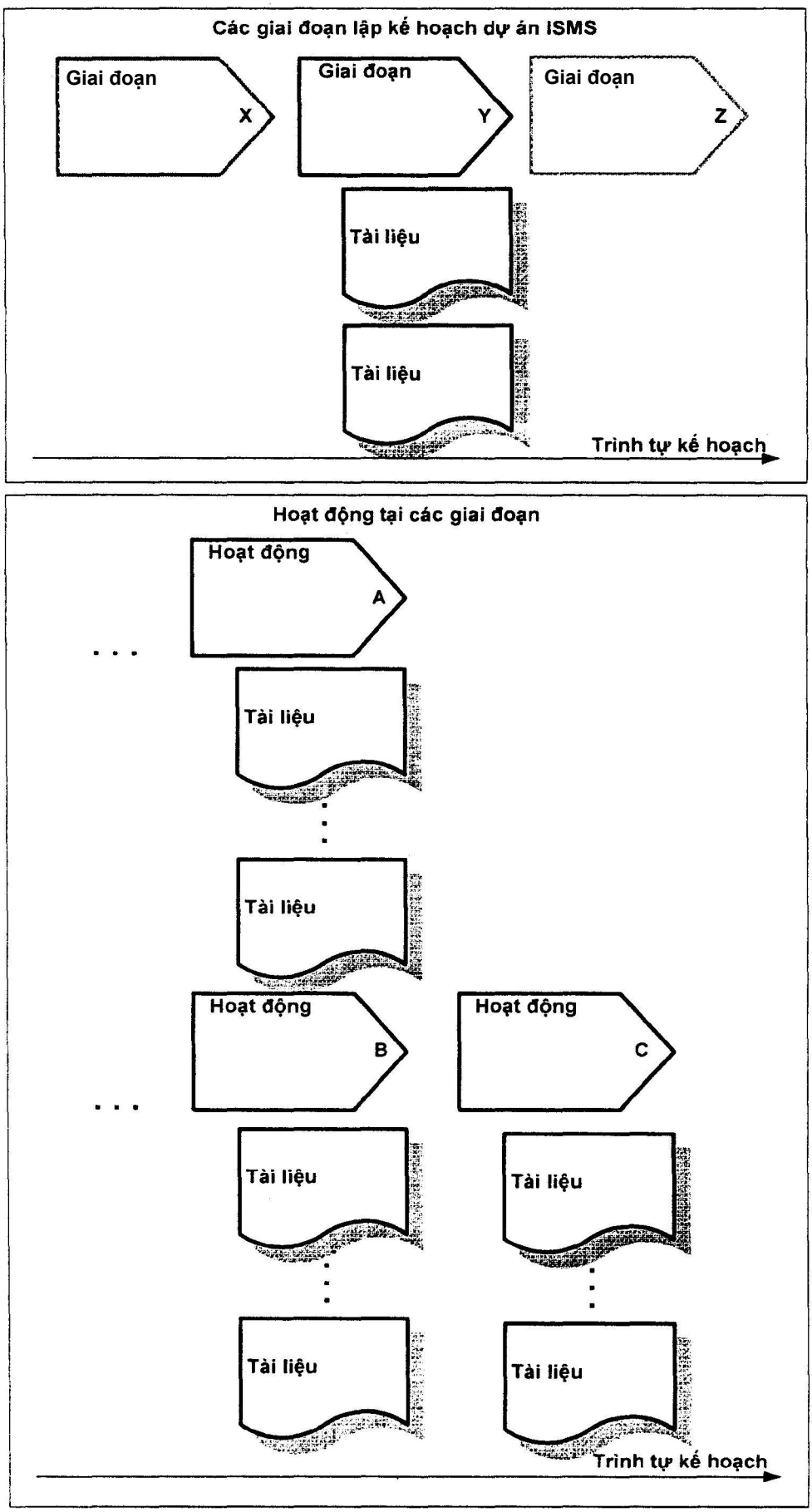
Phần *Thông tin khác* cung cấp thông tin bổ sung hỗ trợ việc triển khai hoạt động, ví dụ các thông tin tham chiếu đến các tiêu chuẩn khác.

CHÚ THÍCH: Các giai đoạn và các hoạt động được mô tả trong tiêu chuẩn này bao gồm một chuỗi các hoạt động thực hiện được đề xuất dựa trên sự phụ thuộc đã xác định qua từng mô tả "đầu vào" và "đầu ra". Tuy nhiên, tùy thuộc vào nhiều yếu tố khác nhau (ví dụ, hiệu lực của hệ thống quản lý hiện hành, hiểu biết về tầm quan trọng của an toàn thông tin, các lý do triển khai ISMS), mỗi tổ chức có thể lựa chọn hoạt động bất kỳ theo thứ tự cần thiết nào đó để chuẩn bị cho việc thiết lập và triển khai ISMS.

4.3 Biểu đồ

Các dự án thường được mô tả dưới dạng biểu đồ hoặc đồ họa tổng quan về các hoạt động và đầu ra.

Hình 2 thể hiện chú thích cho các biểu đồ nằm trong điều nhỏ tổng quan của từng giai đoạn. Các biểu đồ này đưa ra thông tin tổng quan về các hoạt động của từng giai đoạn.



Hình 2 - Chú thích luồng công việc

Trong hình trên, ô vuông phía trên thể hiện các giai đoạn lập kế hoạch của một dự án ISMS. Giai đoạn được đề cập trong mỗi điều sau đó được nhấn mạnh với các tài liệu đầu ra chính của giai đoạn đó.

Ô vuông phía dưới (các hoạt động của giai đoạn) bao gồm các hoạt động chính thuộc giai đoạn được nhấn mạnh trong ô vuông phía trên, và các tài liệu đầu ra chính của từng hoạt động.

Trục thời gian trong ô vuông phía dưới tương ứng với trục thời gian ở ô vuông phía trên.

Hoạt động A và Hoạt động B có thể được thực hiện đồng thời. Hoạt động C nên được bắt đầu sau khi Hoạt động A và B kết thúc.

5 Phê chuẩn cho khởi động dự án ISMS

5.1 Tổng quan về cách thức để được phê chuẩn cho khởi động dự án ISMS

Khi quyết định triển khai ISMS, nên xem xét một số yếu tố. Để xác định được các yếu tố này, ban quản lý nên hiểu được tình huống nghiệp vụ của một dự án triển khai ISMS và phê chuẩn tình huống này. Do vậy, mục tiêu của giai đoạn này là:

Mục tiêu: Được ban quản lý phê chuẩn cho khởi động dự án ISMS thông qua việc xác định tình huống nghiệp vụ và kế hoạch dự án.

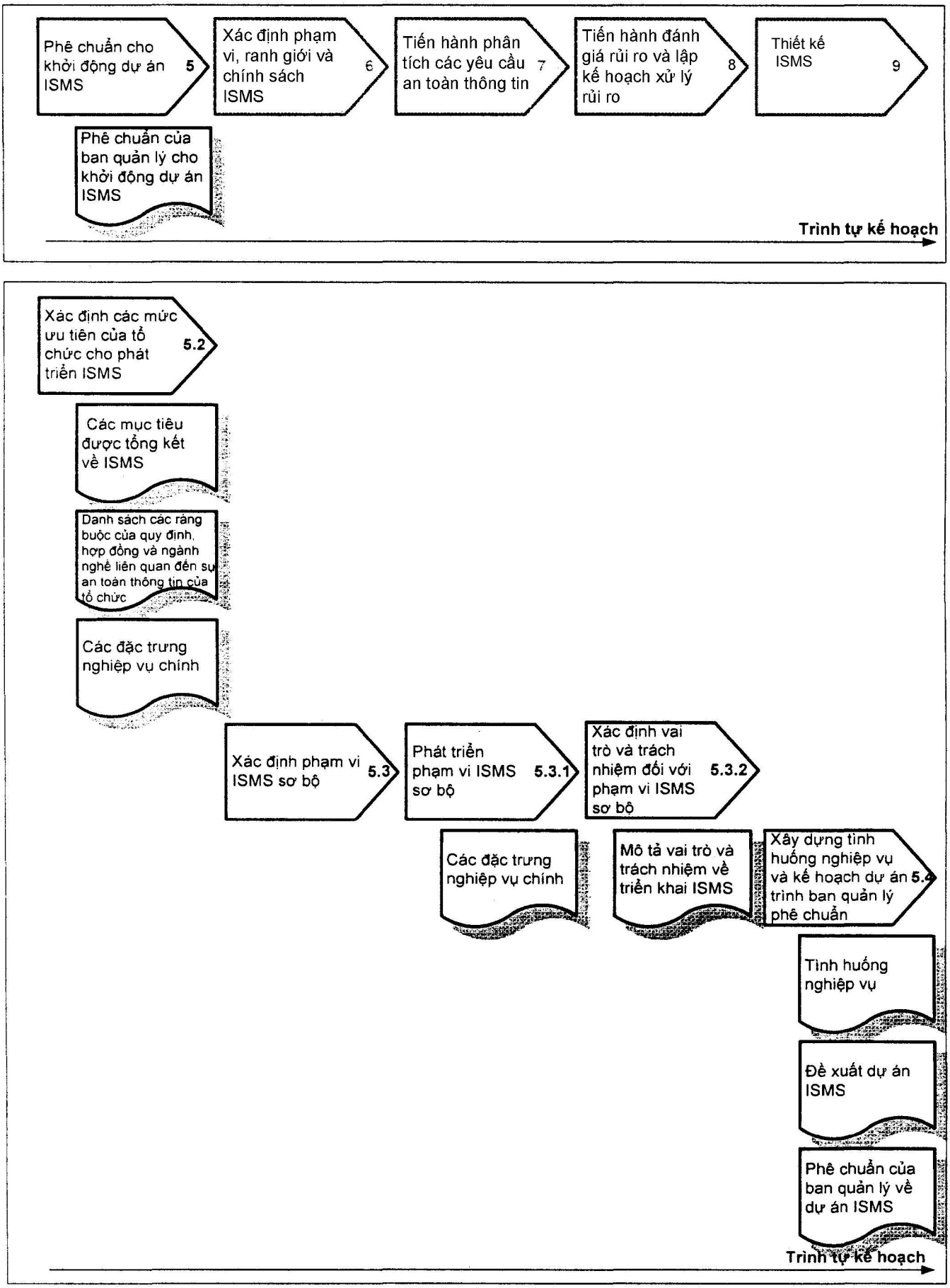
Để được ban quản lý phê chuẩn, tổ chức nên xây dựng một tình huống nghiệp vụ bao gồm cả các ưu tiên và mục tiêu triển khai ISMS và cơ cấu tổ chức cho ISMS. Cũng nên xây dựng kế hoạch ban đầu cho dự án ISMS.

Công việc thực hiện trong giai đoạn này sẽ giúp tổ chức hiểu được tính xác đáng của ISMS, và làm rõ các vai trò và trách nhiệm về an toàn thông tin trong tổ chức cần thiết cho một dự án ISMS.

Đầu ra mục tiêu của giai đoạn này sẽ là phê chuẩn sơ bộ, cam kết triển khai ISMS và thực hiện các hoạt động được mô tả trong tiêu chuẩn này của ban quản lý. Các sản phẩm của điều này gồm tình huống nghiệp vụ và dự thảo kế hoạch của dự án ISMS với các mốc thời gian chính.

Hình 3 mô tả quy trình để được ban quản lý phê chuẩn cho khởi động dự án ISMS.

CHÚ THÍCH: Đầu ra từ điều 5 (Cam kết bằng văn bản của ban quản lý về kế hoạch và triển khai ISMS) và một trong các đầu ra của điều 7 (Văn bản tóm tắt hiện trạng an toàn thông tin) không phải là các yêu cầu của TCVN ISO/IEC 27001:2009 (ISO/IEC 27001:2005). Tuy nhiên, các đầu ra từ các hoạt động này là đầu vào khuyến nghị đối với các hoạt động khác được mô tả trong tiêu chuẩn này.



Hình 3 – Tổng quan về cách thức để được ban quản lý phê chuẩn cho khởi động dự án ISMS

5.2 Làm rõ các ưu tiên của tổ chức cho phát triển ISMS

Hoạt động

Xác định các ưu tiên và yêu cầu an toàn thông tin của tổ chức, trong đó có quan tâm đến các mục tiêu triển khai ISMS.

Đầu vào

a) các mục tiêu chiến lược của tổ chức;

b) tổng quan về các hệ thống quản lý hiện có;

c) danh sách các yêu cầu an toàn thông tin theo luật pháp, qui định, và hợp đồng áp dụng cho tổ chức.

Hướng dẫn

Nhìn chung, để khởi động dự án ISMS, cần có sự phê chuẩn của ban quản lý. Do vậy, hoạt động nên được thực hiện đầu tiên là thu thập các thông tin liên quan thể hiện giá trị của ISMS đối với tổ chức. Tổ chức nên làm rõ tại sao lại cần có ISMS và quyết định các mục tiêu triển khai ISMS và khởi động dự án ISMS.

Có thể xác định được các mục tiêu triển khai ISMS khi trả lời các câu hỏi sau:

a) quản lý rủi ro – ISMS sẽ giúp quản lý tốt hơn các rủi ro an toàn thông tin như thế nào?

b) hiệu quả - ISMS có thể cải thiện được việc quản lý an toàn thông tin như thế nào?

c) lợi thế về nghiệp vụ – ISMS có thể tạo nên lợi thế cạnh tranh của tổ chức như thế nào?

Để trả lời các câu hỏi trên, các yêu cầu và ưu tiên về an toàn thông tin của mỗi tổ chức sẽ được làm rõ bởi các yếu tố sau:

a) các phạm vi tổ chức và các nghiệp vụ trọng yếu:

   1) Các phạm vi về tổ chức và các hoạt động nghiệp vụ nào là trọng yếu?

   2) Các phạm vi về tổ chức nào liên quan đến hoạt động nghiệp vụ và tập trung vào hoạt động nghiệp vụ nào?

   3) Tổ chức đang có mối quan hệ và các thỏa thuận nào với bên thứ ba?

   4) Các dịch vụ nào đang được thực hiện theo hình thức thuê khoán?

b) thông tin nhạy cảm và có giá trị:

   1) Thông tin nào quan trọng đối với tổ chức?

   2) Hậu quả có thể xảy ra nếu thông tin nào đó bị tiết lộ cho các bên không có thẩm quyền (ví dụ, mất lợi thế cạnh tranh, thiệt hại đến thương hiệu hoặc danh tiếng, hành động pháp lý...).

c) các điều luật đề cập đến các biện pháp an toàn thông tin:

1) Các điều luật nào liên quan đến việc xử lý rủi ro hoặc an toàn thông tin áp dụng cho tổ chức?

2) Tổ chức có phải là bộ phận của một tổ chức công toàn cầu được yêu cầu có báo cáo tài chính ngoài tổ chức không?

d) các thỏa thuận theo hợp đồng hoặc về tổ chức có liên quan đến an toàn thông tin:

1) Các yêu cầu lưu trữ nào (bao gồm cả các thời gian sử dụng) đối với kho dữ liệu?

2) Có yêu cầu theo hợp đồng nào liên quan đến tính riêng tư hoặc chất lượng (ví dụ, thỏa thuận mức dịch vụ - SLA) không?

e) các yêu cầu theo ngành nghề có chỉ rõ các chỉ tiêu hoặc biện pháp quản lý an toàn thông tin cụ thể:

1) Các yêu cầu theo chuyên ngành nào áp dụng cho tổ chức?

f) môi trường nguy hiểm:

1) Hình thức bảo vệ nào cần thiết và giúp chống lại những mối đe dọa nào?

2) Các kiểu thông tin nào yêu cầu bảo vệ?

3) Các loại hoạt động thông tin nào cần được bảo vệ?

g) các động lực cạnh tranh:

1) Các yêu cầu nào là những yêu cầu tối thiểu của thị trường đối với an toàn thông tin?

2) Các biện pháp quản lý an toàn thông tin bổ trợ nào phải cung cấp lợi thế cạnh tranh cho tổ chức?

h) các yêu cầu liên quan đến sự liên tục về nghiệp vụ:

1) Các quy trình nghiệp vụ nào là những quy trình nghiệp vụ trọng yếu?

2) Tổ chức có thể chịu những gián đoạn đối với mỗi quy trình nghiệp vụ trọng yếu trong bao lâu?

Phạm vi ISMS sơ bộ có thể được xác định khi có những thông tin ở trên. Phạm vi này cũng phải được sử dụng khi xây dựng tình huống nghiệp vụ và kế hoạch tổng thể của dự án ISMS để trình ban quản lý phê chuẩn. Phạm vi ISMS chi tiết sẽ được xác định trong suốt dự án ISMS.

Các yêu cầu trong 4.2.1 a) của TCVN ISO/IEC 27001:2009 (ISO/IEC 27001:2005) đã phác thảo phạm vi theo đặc thù nghiệp vụ, tổ chức, địa điểm, tài sản và công nghệ của tổ chức. Thông tin thu được từ các câu hỏi trên sẽ hỗ trợ việc xác định các yêu cầu này.

Khi đưa ra các quyết định ban đầu về phạm vi ISMS, nên quan tâm đến một số vấn đề sau:

a) Các chỉ thị về quản lý an toàn thông tin của người quản lý về mặt tổ chức và các nghĩa vụ được áp đặt từ bên ngoài lên tổ chức?

b) Trách nhiệm đối với các hệ thống thuộc phạm vi đề xuất có được nắm giữ bởi nhiều nhóm quản lý không (ví dụ, những người thuộc các bộ phận khác nhau hoặc phòng ban khác nhau)?

c) Các tài liệu liên quan đến ISMS sẽ được chuyển giao trong tổ chức như thế nào (ví dụ, bằng văn bản giấy hoặc thông qua mạng nội bộ)?

d) Các hệ thống quản lý hiện hành có thể hỗ trợ các nhu cầu của tổ chức không? Chúng có hoạt động hết công suất, được duy trì tốt và hoạt động như dự kiến không?

Dưới đây là các ví dụ về các mục tiêu quản lý có thể được sử dụng như đầu vào để xác định phạm vi ISMS sơ bộ:

a) hỗ trợ sự liên tục của hoạt động nghiệp vụ và khôi phục sau thảm họa;

b) cải thiện khả năng phục hồi sau các sự cố;

c) giải quyết vấn đề tuân thủ/các nghĩa vụ pháp lý theo luật pháp/hợp đồng;

d) cho phép chứng nhận theo các tiêu chuẩn ISO/IEC khác;

e) cho phép phát triển và bố trí về mặt tổ chức;

f) giảm các chi phí dành cho các biện pháp quản lý an toàn;

g) bảo vệ các tài sản có giá trị chiến lược;

h) thiết lập một môi trường quản lý nội bộ lành mạnh và hiệu quả;

i) cung cấp sự đảm bảo đối với các bên liên quan rằng các tài sản thông tin đã được bảo vệ một cách thích đáng;

Đầu ra

Sản phẩm của hoạt động này là:

a) tài liệu tóm tắt các mục tiêu, các ưu tiên về an toàn thông tin, các yêu cầu về mặt tổ chức đối với ISMS;

b) danh sách các yêu cầu theo quy định, hợp đồng và ngành nghề liên quan đến sự an toàn thông tin của tổ chức;

c) các đặc thù nghiệp vụ cơ bản, cơ cấu tổ chức, vị trí, tài sản và công nghệ của tổ chức.

Thông tin khác

TCVN ISO 9001:2008, TCVN ISO 14001:2005, ISO/IEC 20000-1:2005.

5.3 Xác định phạm vi ISMS sơ bộ

5.3.1 Phát triển phạm vi ISMS sơ bộ

Hoạt động

Các mục tiêu triển khai ISMS phải gồm cả xác định phạm vi ISMS sơ bộ.

Đầu vào

Đầu ra từ Hoạt động 5.2 Làm rõ các ưu tiên của tổ chức cho phát triển ISMS

Hướng dẫn

Để thực hiện dự án triển khai ISMS, nên xác định cấu trúc tổ chức cho ISMS. Phạm vi ISMS sơ bộ cũng nên được xác định để cung cấp cho ban quản lý hướng dẫn về các quyết định triển khai, và để hỗ trợ các hoạt động tiếp theo.

Phạm vi ISMS sơ bộ phải được sử dụng khi xây dựng tình huống nghiệp vụ và kế hoạch dự án đề xuất trình ban quản lý phê chuẩn.

Đầu ra từ giai đoạn này là tài liệu định nghĩa phạm vi ISMS sơ bộ, bao gồm:

a) tóm tắt các chỉ thị về quản lý an toàn thông tin của người quản lý về mặt tổ chức, và các nghĩa vụ áp đặt từ bên ngoài lên tổ chức;

b) mô tả tương tác của (các) khu vực thuộc phạm vi với các hệ thống quản lý khác;

c) danh sách các mục tiêu nghiệp vụ của quản lý an toàn thông tin (sản phẩm của 5.2);

d) danh sách các quy trình nghiệp vụ trọng yếu, các hệ thống, các tài sản thông tin, các cơ cấu tổ chức và các vị trí địa lý mà ISMS sẽ được áp dụng;

e) mối quan hệ của các hệ thống quản lý hiện hành, quy định, sự tuân thủ và các mục tiêu của tổ chức;

f) các đặc trưng nghiệp vụ, tổ chức, địa điểm, tài sản và công nghệ của tổ chức.

Cũng nên xác định các thành phần giống nhau và những điểm khác nhau về vận hành giữa các quy trình của (các) hệ thống quản lý hiện hành và ISMS được đề xuất.

Đầu ra

Sản phẩm là tài liệu mô tả phạm vi ISMS sơ bộ.

Thông tin khác

Không có thông tin đặc biệt nào khác.

CHÚ THÍCH: Cần đặc biệt lưu ý rằng, để được chứng nhận thì các yêu cầu cụ thể về hệ thống tài liệu của TCVN ISO/IEC 27001:2009 (ISO/IEC 27001:2005) về phạm vi ISMS phải được tuân thủ cho dù trong tổ chức hiện có cả các hệ thống quản lý khác .

5.3.2 Xác định vai trò và trách nhiệm đối với phạm vi ISMS sơ bộ

Hoạt động

Xác định các vai trò và trách nhiệm chung đối với phạm vi ISMS sơ bộ.

Đầu vào

a) đầu ra từ Hoạt động 5.3.1 Phát triển phạm vi ISMS sơ bộ ;

b) danh sách các bên liên quan được hưởng lợi từ các kết quả của dự án ISMS.

Hướng dẫn

Để thực hiện dự án ISMS, nên xác định rõ vai trò của tổ chức đối với dự án. Nhìn chung, vai trò của mỗi tổ chức là khác nhau tùy thuộc vào số người có liên quan đến an toàn thông tin. Cơ cấu tổ chức và các nguồn lực dành cho an toàn thông tin cũng thay đổi theo quy mô, loại hình và cơ cấu của tổ chức. Ví dụ, trong một tổ chức nhỏ, một người có thể thực hiện nhiều vai trò. Tuy nhiên, ban quản lý nên xác định rõ vai trò (thường là trưởng phòng an toàn thông tin, giám đốc an toàn thông tin hoặc tương tự) chịu trách nhiệm chung về quản lý an toàn thông tin, và đội ngũ nhân viên cũng nên được giao cho các vai trò và trách nhiệm dựa trên kỹ năng được yêu cầu để thực hiện công việc. Đây là vấn đề quan trọng để đảm bảo rằng các nhiệm vụ đều được thực hiện một cách hiệu quả và có hiệu lực.

Khi xác định các vai trò trong việc quản lý an toàn thông tin, nên lưu ý các vấn đề quan trọng nhất sau:

a) trách nhiệm chung về các nhiệm vụ phải thuộc ban quản lý;

b) một người (thường là trưởng phòng an toàn thông tin) được cử ra để thúc đẩy và phối hợp quy trình an toàn thông tin;

c) mỗi nhân viên đều có trách nhiệm như nhau đối với nhiệm vụ chính của mình và đối với việc duy trì an toàn thông tin tại nơi làm việc và trong tổ chức.

Các vai trò quản lý an toàn thông tin nên phối hợp với nhau; và có thể được hỗ trợ bởi một Diễn đàn an toàn thông tin, hoặc một tổ chức tương tự.

Sự cộng tác với các chuyên gia có nghiệp vụ phù hợp nên được cam kết (và được ghi vào văn bản) tại tất cả các giai đoạn phát triển, triển khai, vận hành và duy trì ISMS.

Các đại diện từ các phòng ban thuộc phạm vi đã được xác định (ví dụ quản lý rủi ro) chính là các thành viên tiềm năng của nhóm triển khai ISMS. Để sử dụng các nguồn lực một cách hiệu quả và nhanh chóng thì nên duy trì nhóm có kích cỡ thực tế nhỏ nhất. Các khu vực này không chỉ gồm các khu vực trực tiếp thuộc phạm vi ISMS mà còn cả các phân khu gián tiếp, ví dụ các phòng quản trị và quản lý rủi ro. pháp lý.

Đầu ra

Sản phẩm là tài liệu hoặc bảng biểu mô tả các vai trò và trách nhiệm kèm theo tên và tổ chức cần để triển khai ISMS thành công.

Thông tin khác

Phụ lục B cung cấp thông tin chi tiết về các vai trò và trách nhiệm cần có trong tổ chức để có thể triển khai ISMS thành công.

5.4 Xây dựng tình huống nghiệp vụ và kế hoạch dự án trình ban quản lý phê chuẩn

Hoạt động

Xây dựng tình huống nghiệp vụ và đề xuất dự án ISMS để được ban quản lý phê chuẩn và giao phó các nguồn lực cho dự án triển khai ISMS.

Đầu vào

a) đầu ra từ Hoạt động 5.2 Làm rõ các ưu tiên của tổ chức cho phát triển ISMS

b) đầu ra từ Hoạt động 5.3 Xác định phạm vi ISMS sơ bộ – Tài liệu sơ bộ về

    1) phạm vi ISMS, và

    2) các vai trò và trách nhiệm liên quan.

Hướng dẫn

Thông tin về tình huống nghiệp vụ và kế hoạch dự án ISMS ban đầu nên gồm cả trình tự kế hoạch, các nguồn lực, và các mốc thời gian đã được ước lượng cần cho các hoạt động chính được đề cập trong các điều từ 6 đến 9 của tiêu chuẩn này.

Tình huống nghiệp vụ và kế hoạch dự án ISMS ban đầu có vai trò như cơ sở của dự án, nhưng cũng đảm bảo được ban quản lý phê chuẩn và giao phó các nguồn lực cần cho triển khai ISMS. Phương thức mà ISMS sẽ hỗ trợ các mục tiêu nghiệp vụ cũng đóng góp vào hiệu lực của các quy trình tổ chức và làm tăng hiệu quả của nghiệp vụ.

Tình huống nghiệp vụ triển khai ISMS nên bao gồm các trình bày ngắn gọn hướng đến các mục tiêu của tổ chức và bao gồm các đối tượng sau:

a) các mục tiêu cụ thể và các mục đích;

b) lợi ích đối với tổ chức;

c) phạm vi ISMS sơ bộ, bao gồm cả các quy trình nghiệp vụ chịu tác động;

d) các quy trình và các yếu tố trọng yếu để tiếp cận các mục tiêu ISMS;

e) tổng quan dự án mức cao;

f) kế hoạch triển khai ban đầu;

g) các vai trò và trách nhiệm đã được xác định;

h) các nguồn lực được yêu cầu (cả về công nghệ và con người);

i) các vấn đề cần quan tâm khi triển khai bao gồm cả sự an toàn thông tin hiện tại;

j) trình tự kế hoạch cùng các mốc thời gian chính;

k) các chi phí dự kiến:

l) các yếu tố trọng yếu quyết định thành công;

m) định lượng các lợi ích đối với tổ chức.

Kế hoạch dự án nên bao gồm cả các hoạt động liên quan của các giai đoạn trong các điều từ 6 đến 9 của tiêu chuẩn này.

Các cá nhân tác động, hoặc bị ảnh hưởng bởi ISMS nên được xác định và được cho một khoảng thời gian phù hợp để xem xét và cho ý kiến về tình huống nghiệp vụ ISMS và đề xuất dự án ISMS. Tình huống nghiệp vụ và đề xuất dự án ISMS nên được cập nhật ngay khi có đầu vào. Ngay khi đã nhận đủ các ý kiến hỗ trợ thì tình huống nghiệp vụ và đề xuất dự án ISMS nên được trình bày để ban quản lý phê chuẩn.

Ban quản lý nên phê chuẩn tình huống nghiệp vụ và kế hoạch dự án ban đầu để nhận được sự cam kết của toàn bộ tổ chức và bắt đầu thực hiện dự án ISMS.

Các lợi ích dự kiến từ cam kết triển khai ISMS của ban quản lý gồm:

a) kiến thức và sự thi hành các điều luật, quy định, các nghĩa vụ thỏa thuận và các tiêu chuẩn liên quan đến an toàn thông tin sẽ giúp tránh được các trở ngại pháp lý và bị phạt do không tuân thủ;

b) sử dụng hiệu quả các quy trình an toàn thông tin;

c) sự ổn định và tin tưởng ngày càng tăng thông qua việc quản lý các rủi ro an toàn thông tin hiệu quả hơn;

d) định danh và bảo vệ thông tin nghiệp vụ trọng yếu.

Đầu ra

Sản phẩm của hoạt động này bao gồm:

a) văn bản phê chuẩn cho triển khai dự án ISMS của ban quản lý cùng các nguồn được phân bổ;

b) tài liệu tình huống nghiệp vụ;

c) bản đề xuất dự án ISMS ban đầu, có kèm theo các mốc thời gian, ví dụ thực hiện đánh giá rủi ro, triển khai, kiểm soát nội bộ, và soát xét của ban quản lý.

Thông tin khác

ISO/IEC 27000:2009 đưa ra các ví dụ về các yếu tố trọng yếu quyết định thành công để hỗ trợ tình huống nghiệp vụ ISMS.

6 Xác định phạm vi, các giới hạn và chính sách ISMS

6.1 Tổng quan về xác định phạm vi, các giới hạn và chính sách ISMS

Sự phê chuẩn cho triển khai ISMS của ban quản lý được dựa trên phạm vi ISMS sơ bộ, tình huống nghiệp vụ ISMS và kế hoạch dự án ban đầu. Định nghĩa chi tiết về phạm vi và các giới hạn ISMS, định nghĩa chính sách ISMS, sự chấp nhận và hỗ trợ từ ban quản lý là các yếu tố chính giúp triển khai ISMS thành công.

Do vậy, các mục tiêu của giai đoạn này gồm:

Mục tiêu:

Nhằm xác định phạm vi chi tiết và các giới hạn của ISMS, xây dựng chính sách ISMS, và được ban quản lý phê chuẩn.

Xem 4.2.1 a) và 4.2.1 b) của TCVN ISO/IEC 27001:2009 (ISO/IEC 27001:2005).

Để đạt được mục tiêu "Xác định phạm vi chi tiết và các giới hạn của ISMS", cần thực hiện các hoạt động sau:

a) xác định phạm vi và các giới hạn về tổ chức;

b) phạm vi và các giới hạn về công nghệ thông tin và truyền thông (ICT);

c) phạm vi và các giới hạn vật lý;

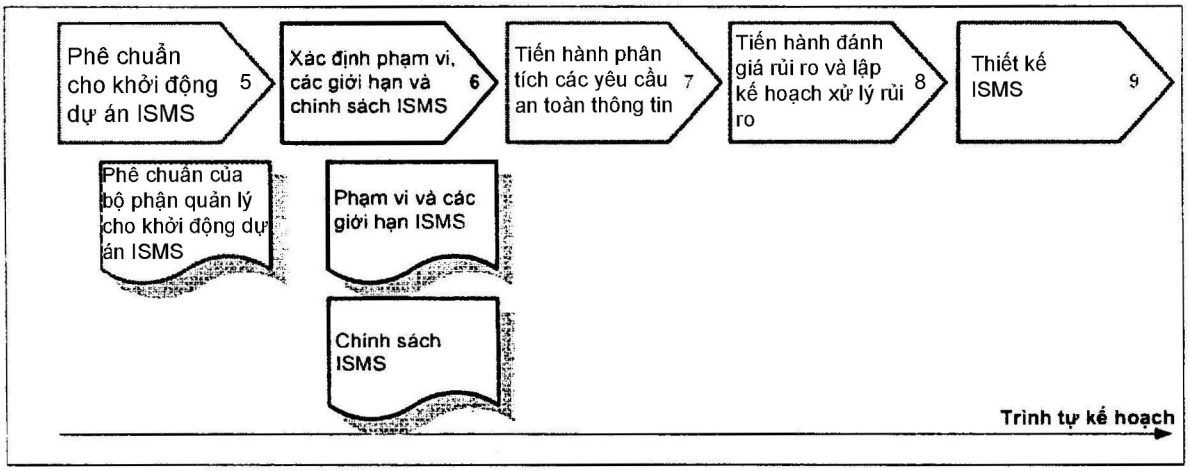
d) các đặc thù đã được chỉ rõ trong 4.2.1 a) và b) của TCVN ISO/IEC 27001:2009 (ISO/IEC 27001:2005), tức là các đặc thù về nghiệp vụ, tổ chức, địa điểm, tài sản và công nghệ của phạm vi và các giới hạn, và chính sách đã được xác định trong quy trình xác định phạm vi và các giới hạn này.

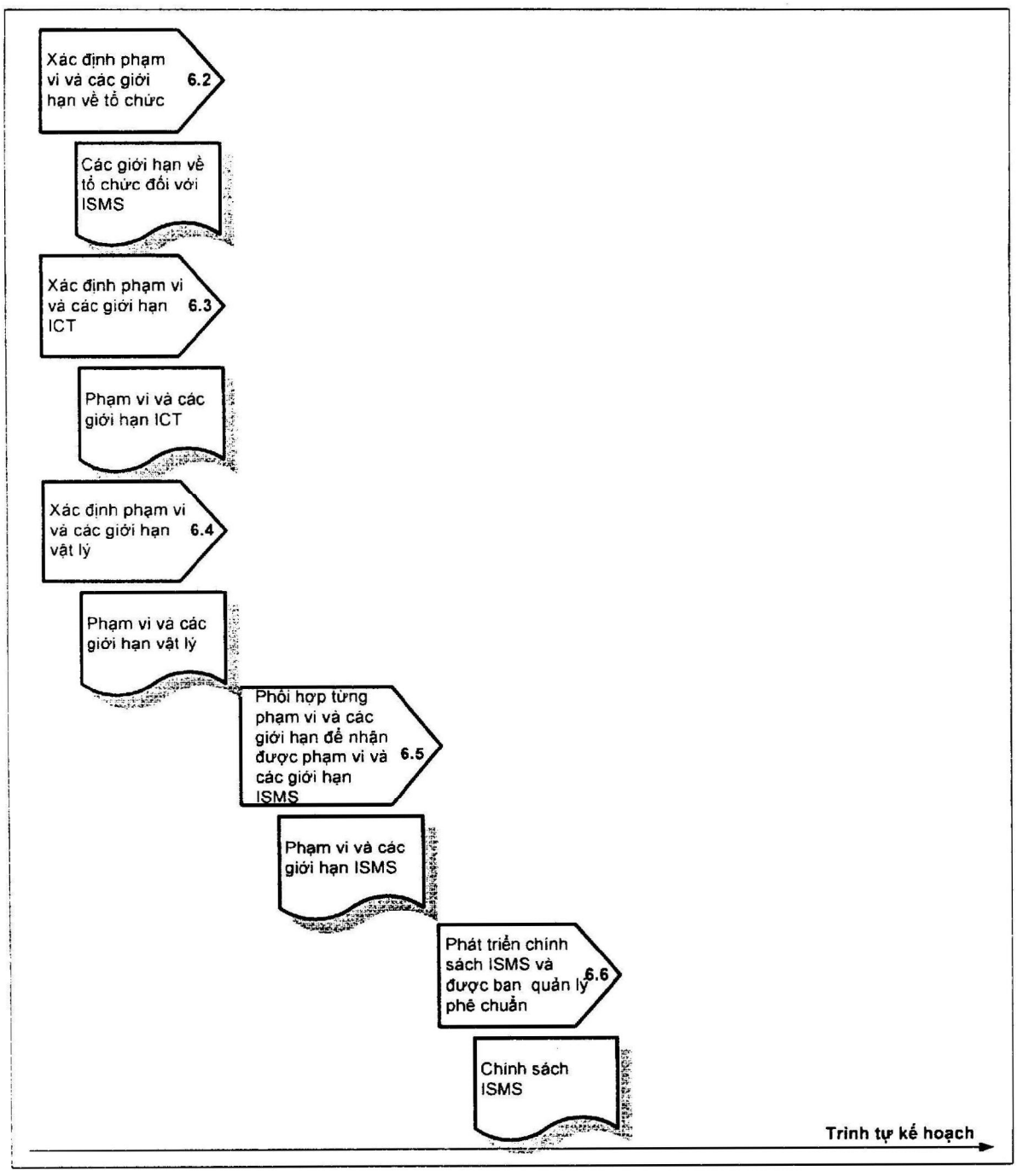
e) phối hợp phạm vi và các giới hạn cơ sở để nhận được phạm vi và các giới hạn ISMS.

Để xây dựng được một hệ thống quản lý hiệu quả cho tổ chức thì phạm vi ISMS chi tiết nên được xác định thông qua việc xem xét các tài sản thông tin trọng yếu của tổ chức. Để xác định các tài sản thông tin và đánh giá các cơ chế an toàn khả thi, điều quan trọng là phải có phương pháp tiếp cận có hệ thống và chuyên môn. Điều đó sẽ làm cho việc truyền thông trở nên dễ dàng và tăng cường sự thông hiểu nhất quán qua tất cả các giai đoạn của quá trình triển khai. Một điều quan trọng nữa là phải đảm bảo rằng các khu vực trọng yếu của tổ chức đều thuộc phạm vi ISMS.

Có thể xác định phạm vi ISMS là toàn bộ tổ chức, hoặc một bộ phận của tổ chức, ví dụ một phòng ban hoặc một bộ phận phụ trợ có liên quan. Ví dụ, với trường hợp "các dịch vụ" được cung cấp đến khách hàng thì phạm vi của ISMS có thể là một dịch vụ, hoặc một hệ thống quản lý chức năng chéo (toàn bộ một phòng ban hoặc một bộ phận của phòng ban). Để được chứng nhận thì các yêu cầu của TCVN ISO/IEC 27001:2009 (ISO/IEC 27001:2005) phải được thỏa mãn, không xét đến các hệ thống quản lý hiện hành đang áp dụng trong tổ chức.

Phạm vi và các giới hạn về tổ chức, phạm vi và các giới hạn về ICT (6.3) và phạm vi và các giới hạn vật lý (6.4) không nhất thiết phải được xác định lần lượt. Tuy nhiên, việc xác định phạm vi và các giới hạn sau sẽ thuận lợi nếu có tham khảo phạm vi và các giới hạn đã có được trước đó.





Hình 4 – Tổng quan về xác định phạm vi, các giới hạn và chính sách ISMS

6.2 Xác định phạm vi và các giới hạn về tổ chức

Hoạt động

Xác định phạm vi và các giới hạn về tổ chức.

Đầu vào

a) đầu ra từ Hoạt động 5.3 Xác định phạm vi ISMS sơ bộ – tài liệu phạm vi ISMS sơ bộ thể hiện:

   1) mối quan hệ của các hệ thống quản lý hiện hành, quy định, tuân thủ, và các mục tiêu của tổ chức;

   2) đặc thù về nghiệp vụ, tổ chức, địa điểm, tài sản và công nghệ.

b) đầu ra từ Hoạt động 5.2 Làm rõ các ưu tiên của tổ chức cho phát triển ISMS – phê chuẩn của ban quản lý cho triển khai ISMS và khởi động dự án cùng các nguồn lực cần thiết đã được phân bổ.

Hướng dẫn

Nỗ lực cần thiết để triển khai ISMS không phụ thuộc vào độ lớn của phạm vi mà ISMS sẽ được áp dụng. Điều này có thể cũng tác động tới tất cả các hoạt động liên quan đến việc duy trì an toàn thông tin của tất cả các danh mục thuộc phạm vi (ví dụ quy trình, các địa điểm, các hệ thống IT và con người), bao gồm cả việc triển khai và duy trì các biện pháp quản lý, quản lý vận hành, và thực thi các nhiệm vụ như xác định các tài sản thông tin và đánh giá rủi ro. Nếu ban quản lý quyết định loại trừ các bộ phận nhất định nào đó của tổ chức ra ngoài phạm vi của ISMS thì nên đưa ra lý do bằng văn bản.

Khi phạm vi của ISMS đã xác định thì quan trọng là các giới hạn phải đủ rõ ràng để giải thích cho những người không thuộc phạm vi này.

Tổ chức có thể đã có một số biện pháp quản lý liên quan tới an toàn thông tin dưới dạng kết quả triển khai các hệ thống quản lý khác. Các biện pháp này cũng nên được xem xét khi lập kế hoạch ISMS nhưng không nhất thiết phải chỉ ra các giới hạn của phạm vi đối với ISMS hiện hành.

Một phương pháp xác định các giới hạn về tổ chức là xác định các khu vực trách nhiệm không bị chồng lấn để dễ dàng cho việc phân công giải trình trách nhiệm trong tổ chức.

Các trách nhiệm liên quan trực tiếp đến các tài sản thông tin hoặc các quy trình nghiệp vụ thuộc phạm vi ISMS nên được chọn là bộ phận của tổ chức chịu sự quản lý của ISMS. Trong quá trình xác định các giới hạn về tổ chức, nên quan tâm đến các vấn đề sau:

a) diễn đàn quản lý ISMS nên gồm những người quản lý tham gia trực tiếp vào phạm vi ISMS;

b) thành viên của ban quản lý chịu trách nhiệm về ISMS nên là người chịu trách nhiệm cuối cùng về tất cả các khu vực trách nhiệm bị tác động (tức là, vai trò của họ sẽ luôn bị chi phối bởi tầm quản lý và trách nhiệm của họ trong tổ chức).

c) trong trường hợp nếu vai trò chịu trách nhiệm quản lý ISMS không phải là một thành viên thuộc ban quản lý cao cấp thì người quản lý cao nhất cần phải thể hiện sự quan tâm đến an toàn thông tin và đóng vai trò như người ủng hộ triển khai ISMS ở mức cao nhất của tổ chức;

d) phạm vi và các giới hạn phải được xác định để đảm bảo rằng tất cả các tài sản liên quan đều được xem xét trong quá trình đánh giá rủi ro, và giải quyết được các rủi ro có thể xuất hiện qua các giới hạn này.

Tùy theo phương pháp tiếp cận, các giới hạn về tổ chức đã được phân tích nên xác định tất cả các cá nhân bị tác động bởi ISMS, và thông tin này nên được đưa vào phạm vi. Và cũng tùy theo phương pháp tiếp cận được lựa chọn mà việc xác định các cá nhân bị tác động có thể được đưa vào các quy trình và/hoặc các chức năng. Nếu một số quy trình thuộc phạm vi lại được bên thứ ba thực hiện thì các ràng buộc nên được ghi rõ ràng trong văn bản. Các ràng buộc đó sẽ phải được tập trung phân tích sâu hơn trong dự án triển khai ISMS.

Đầu ra

Sản phẩm của hoạt động này bao gồm:

a) mô tả các giới hạn về tổ chức đối với ISMS, bao gồm cả các lý do tại sao một số bộ phận của tổ chức lại bị loại ra ngoài phạm vi ISMS;

b) các chức năng và cấu trúc của các bộ phận thuộc phạm vi ISMS;

c) định danh thông tin được chuyển giao trong phạm vi và thông tin được chuyển giao ra ngoài các giới hạn;

d) các quy trình tổ chức và các trách nhiệm đối với các tài sản thông tin thuộc phạm vi và ngoài phạm vi ISMS;

e) quy trình phân cấp ban hành quyết định cũng như cấu trúc trong ISMS.

Thông tin khác

Không có thông tin đặc biệt nào khác.

6.3 Xác định phạm vi và các giới hạn về công nghệ thông tin và truyền thông (ICT)

Hoạt động

Xác định phạm vi và các giới hạn của các thành phần công nghệ thông tin và truyền thông (ICT) và các danh mục công nghệ khác thuộc phạm vi ISMS.

Đầu vào

a) đầu ra từ Hoạt động 5.3 Xác định phạm vi ISMS sơ bộ – Tài liệu về phạm vi ISMS sơ bộ;

b) đầu ra từ Hoạt động 6.2 Xác định phạm vi và các giới hạn về tổ chức.

Hướng dẫn

Có thể có được định nghĩa về phạm vi và các giới hạn ICT thông qua phương pháp tiếp cận hệ thống thông tin (chứ không phải là dựa trên IT). Một khi ban quản lý đã quyết định đưa các quy trình nghiệp vụ hệ thống thông tin vào phạm vi ISMS thì tất cả các thành phần ICT liên quan đều cần được xem xét. Tức là bao gồm tất cả các bộ phận của tổ chức thực hiện lưu giữ, xử lý hoặc chuyển giao thông tin trọng yếu, tài sản, hoặc những thứ có ý nghĩa quan trọng đối với các bộ phận thuộc phạm vi tổ chức. Các hệ thống thông tin có thể mở rộng ra ngoài biên giới về tổ chức hoặc quốc gia. Khi đó, nên quan tâm đến các yếu tố sau:

a) môi trường văn hóa xã hội;

b) các yêu cầu về pháp lý, quy định và hợp đồng áp dụng cho tổ chức;

c) giải trình trách nhiệm đối với các trách nhiệm chính;

d) các ràng buộc về kỹ thuật (ví dụ, băng thông có sẵn, độ sẵn sàng của dịch vụ...).

Liên quan đến các yếu tố cần quan tâm ở trên, để có thể áp dụng được thì các giới hạn ICT nên gồm thông tin mô tả các vấn đề sau:

a) cơ sở hạ tầng truyền thông, nơi trách nhiệm quản lý được tổ chức nắm giữ, bao gồm các công nghệ khác nhau (ví dụ, vô tuyến, hữu tuyến, hoặc các mạng dữ liệu/thoại);

b) phần mềm thuộc các giới hạn về tổ chức được tổ chức sử dụng và quản lý;

c) phần cứng ICT được yêu cầu bởi mạng hoặc các mạng, các ứng dụng hoặc các hệ thống sản xuất;

d) các vai trò và trách nhiệm liên quan đến phần cứng, mạng và phần mềm ICT.

Nếu một trong số các danh mục ở trên không chịu sự quản lý của tổ chức thì các ràng buộc với bên thứ ba nên được ghi vào văn bản. Xem 6.2, phần Hướng dẫn.

Đầu ra

Sản phẩm của hoạt động này bao gồm:

a) thông tin được chuyển giao trong phạm vi và thông tin được chuyển giao ra ngoài các giới hạn;

b) các giới hạn ICT đối với ISMS, bao gồm cả các lý do loại bỏ ICT có chịu sự quản lý của tổ chức ra ngoài phạm vi ISMS;

c) các hệ thống thông tin và mạng viễn thông, có mô tả các hệ thống thuộc phạm vi, và các vai trò và trách nhiệm đối với các hệ thống này. Các hệ thống nằm ngoài phạm vi cũng nên được tóm tắt một cách ngắn gọn.

Thông tin khác

Không có thông tin đặc biệt nào khác.

6.4 Xác định phạm vi và các giới hạn vật lý

Hoạt động

Xác định phạm vi và các giới hạn vật lý chịu sự chi phối của ISMS.

Đầu vào

a) đầu ra từ Hoạt động 5.3 Xác định phạm vi ISMS sơ bộ – Tài liệu phạm vi ISMS sơ bộ;

b) đầu ra từ Hoạt động 6.2 Xác định phạm vi và các giới hạn về tổ chức;

c) đầu ra từ Hoạt động 6.3 Xác định phạm vi và các giới hạn về công nghệ thông tin và truyền thông (ICT).

Hướng dẫn

Xác định phạm vi và các giới hạn vật lý chính là xác định các trụ sở, địa điểm hoặc các phương tiện của tổ chức chịu sự chi phối của ISMS. Việc xác định có thể sẽ phức tạp hơn nếu các hệ thống thông tin đi qua các biên giới vật lý cần có:

a) các phương tiện hoạt động ở xa;

b) các giao tiếp đến các hệ thống thông tin của khách hàng và các dịch vụ được cung cấp bởi dịch vụ bên thứ ba;

c) các giao tiếp phù hợp và các mức dịch vụ.

Khi xem xét các yếu tố ở trên, để có thể sử dụng được thì các giới hạn vật lý nên bao gồm tài liệu mô tả các vấn đề sau:

a) bản mô tả các chức năng và quy trình liên quan đến các địa điểm và mức độ mà tổ chức quản lý chúng;

b) các phương tiện đặc biệt được sử dụng để lưu trữ/chứa phần cứng ICT hoặc dữ liệu thuộc phạm vi (ví dụ các băng từ dự phòng) theo phạm vi chi phối của các giới hạn ICT.

Nếu một hoặc nhiều trong số các danh mục ở trên không thuộc sự quản lý của tổ chức thì các ràng buộc với bên thứ ba cũng nên được ghi vào văn bản. Xem 6.2, phần Hướng dẫn.

Đầu ra

Sản phẩm của hoạt động này bao gồm:

a) bản mô tả các giới hạn vật lý đối với ISMS, gồm cả các lý do loại bỏ các giới hạn vật lý chịu sự quản lý của tổ chức ra ngoài phạm vi ISMS;

b) bản mô tả về tổ chức và các đặc điểm địa lý của tổ chức có liên quan tới phạm vi.

Thông tin khác

Không có thông tin đặc biệt nào khác.

6.5 Phối hợp phạm vi và các giới hạn để nhận được phạm vi và các giới hạn ISMS

Hoạt động

Nhận được phạm vi và các giới hạn ISMS khi phối hợp từng phạm vi và các giới hạn.

Đầu vào

a) đầu ra từ Hoạt động 5.3 Xác định phạm vi ISMS sơ bộ – Tài liệu phạm vi ISMS sơ bộ;

b) đầu ra từ Hoạt động 6.2 Xác định phạm vi và các giới hạn về tổ chức;

c) đầu ra từ Hoạt động 6.3 Xác định phạm vi và các giới hạn về công nghệ thông tin và truyền thông (ICT);

d) đầu ra từ Hoạt động 6.4 Xác định phạm vi và các giới hạn vật lý.

Hướng dẫn

Phạm vi của ISMS có thể được mô tả và điều chỉnh theo nhiều cách. Ví dụ, có thể lựa chọn một địa điểm, chẳng hạn một trung tâm dữ liệu hoặc văn phòng, và liệt kê các quy trình trọng yếu; mỗi quy trình phải bao hàm các khu vực bên ngoài trung tâm dữ liệu đó. Ví dụ, một quy trình trọng yếu có thể là truy cập di động tới một hệ thống thông tin trung tâm.

Đầu ra

Sản phẩm của hoạt động này là tài liệu mô tả phạm vi và các giới hạn của ISMS, gồm các thông tin sau:

a) các đặc điểm chính của tổ chức (chức năng, cấu trúc, dịch vụ, tài sản, phạm vi và các giới hạn trách nhiệm đối với từng tài sản);

b) các quy trình tổ chức thuộc phạm vi;

c) cấu hình của thiết bị và các mạng thuộc phạm vi;

d) danh sách sơ bộ các tài sản thông tin thuộc phạm vi;

e) danh sách các tài sản ICT thuộc phạm vi (ví dụ, các máy chủ);

f) các bản đồ địa điểm thuộc phạm vi, trong đó chỉ ra các giới hạn vật lý của ISMS;

g) bản mô tả các vai trò và trách nhiệm đối với ISMS và mối quan hệ của họ với cơ cấu tổ chức;

h) chi tiết về các lý do loại bỏ các đối tượng ra ngoài phạm vi ISMS.

Thông tin khác

Không có thông tin đặc biệt nào khác.

6.6 Phát triển chính sách ISMS và được ban quản lý phê chuẩn

Hoạt động

Phát triển chính sách ISMS và được ban quản lý phê chuẩn.

Đầu vào

a) đầu ra từ Hoạt động 6.5 Phối hợp phạm vi và các giới hạn để nhận được phạm vi và các giới hạn ISMS – Tài liệu phạm vi và các giới hạn ISMS;

b) đầu ra từ Hoạt động 5.2 Làm rõ các ưu tiên của tổ chức cho phát triển ISMS – Tài liệu mục tiêu triển khai ISMS;

c) đầu ra từ Hoạt động 5.4 Xây dựng tình huống nghiệp vụ và kế hoạch dự án trình ban quản lý – Các nội dung đã lập thành tài liệu:

   1) các yêu cầu và các ưu tiên an toàn thông tin của tổ chức;

   2) kế hoạch dự án ban đầu về triển khai ISMS cùng với các mốc thời gian, ví dụ thực hiện đánh giá rủi ro, triển khai, soát xét nội bộ, và soát xét của ban quản lý.

Hướng dẫn

Trong quá trình xác định chính sách ISMS, nên quan tâm các vấn đề sau:

a) thiết lập các mục tiêu ISMS dựa trên các yêu cầu về tổ chức và các ưu tiên cho an toàn thông tin của tổ chức;

b) thiết lập trọng tâm chung và hướng dẫn hành động để đạt được các mục tiêu ISMS;

c) xem xét các yêu cầu của tổ chức, các nghĩa vụ pháp lý hoặc quy định và hợp đồng có liên quan đến an toàn thông tin;

d) bối cảnh quản lý rủi ro trong tổ chức;

e) thiết lập chỉ tiêu đánh giá các rủi ro (xem TCVN 10295:2014 (ISO/IEC 27005:2011)) và xác định cấu trúc đánh giá rủi ro;

f) làm rõ các trách nhiệm quản lý cấp cao đối với ISMS;

g) được ban quản lý phê chuẩn.

Đầu ra

Sản phẩm là một tài liệu mô tả chính sách ISMS đã được ban quản lý phê chuẩn. Văn bản này nên được phê chuẩn lại trong giai đoạn tiếp theo của dự án vì nó phụ thuộc vào thông tin đầu ra của quá trình đánh giá rủi ro.

Thông tin khác

TCVN 10295:2014 (ISO/IEC 27005:2011) cung cấp thông tin bổ sung về chỉ tiêu đánh giá rủi ro.

7 Tiến hành phân tích các yêu cầu an toàn thông tin

7.1 Tổng quan về tiến hành phân tích các yêu cầu an toàn thông tin

Phân tích tình huống hiện tại trong tổ chức là vấn đề quan trọng, vì có nhiều yêu cầu hiện tại và các tài sản thông tin cần được quan tâm khi triển khai ISMS. Để hiệu quả và thực tế thì các hoạt động được mô tả trong giai đoạn này có thể được thực hiện song song với các hoạt động được mô tả trong điều 6.

Mục tiêu: Nhằm xác định các yêu cầu phù hợp sẽ được hỗ trợ bởi ISMS, xác định các tài sản thông tin, và đạt được trạng thái an toàn thông tin hiện tại trong phạm vi. Xem TCVN ISO/IEC 27001:2009 (ISO/IEC 27001:2005): 4.2.1.c), 4.2.1.d), 4.2.1.e).

Thông tin thu thập được thông qua quá trình phân tích an toàn thông tin nên:

a) cung cấp cho ban quản lý điểm xuất phát (tức là cơ sở dữ liệu chuẩn);

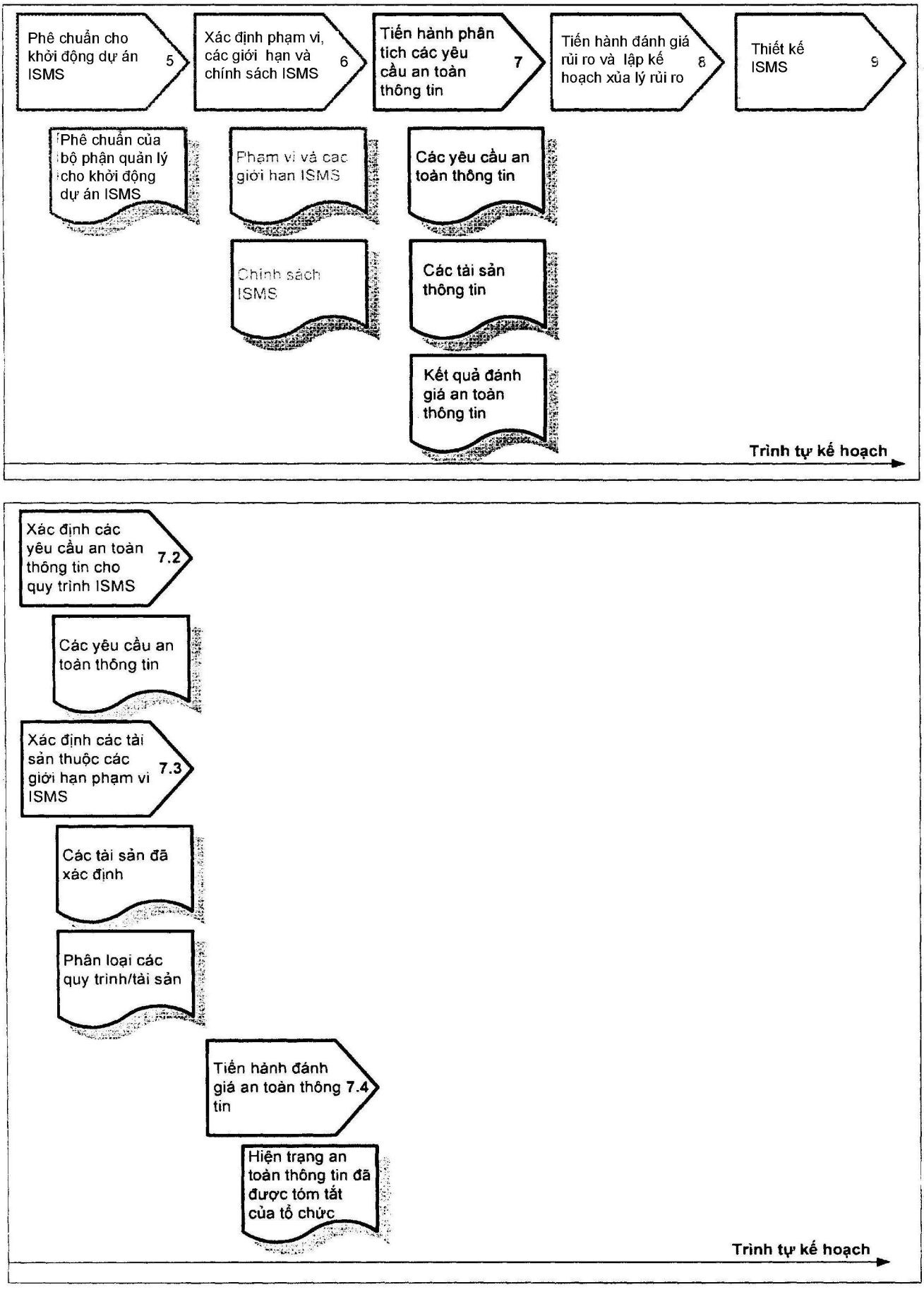
b) xác định và lập thành tài liệu các điều kiện triển khai;

c) cung cấp hiểu biết rõ ràng và vững chắc về các thiết bị của tổ chức;

d) quan tâm đến các tình huống và tình trạng cụ thể của tổ chức;

e) xác định mức bảo vệ thông tin mong muốn;

f) quyết định tài liệu thông tin cần thiết cho toàn bộ hoặc một phần của tổ chức thuộc phạm vi triển khai đã được đề xuất.



Hình 5 – Tổng quan về giai đoạn tiến hành phân tích các yêu cầu an toàn thông tin

7.2 Xác định các yêu cầu an toàn thông tin cho quy trình ISMS

Hoạt động

Phân tích và xác định các yêu cầu chi tiết về an toàn thông tin cho quy trình ISMS.

Đầu vào

a) đầu ra từ Hoạt động 5.2 Làm rõ các ưu tiên của tổ chức cho phát triển ISMS – Các tài liệu:

   1) tóm tắt các mục tiêu, các ưu tiên an toàn thông tin, và các yêu cầu của tổ chức đối với ISMS;

   2) danh sách các ràng buộc theo quy định, hợp đồng và ngành nghề có liên quan đến an toàn thông tin của tổ chức.

b) đầu ra từ Hoạt động 6.5 Phối hợp phạm vi và các giới hạn để nhận được phạm vi và các giới hạn ISMS – Phạm vi và các giới hạn của ISMS;

c) đầu ra từ Hoạt động 6.6 Phát triển chính sách ISMS và được ban quản lý phê chuẩn – Chính sách ISMS.

Hướng dẫn

Đầu tiên, phải thu thập được tất cả các thông tin hỗ trợ ISMS. Đối với mỗi quy trình về tổ chức và nhiệm vụ chuyên môn, cần đưa ra quyết định xem thông tin quan trọng ở mức nào, tức là mức bảo vệ được yêu cầu. Có rất nhiều điều kiện nội tại có thể ảnh hưởng đến an toàn thông tin, và các điều kiện này nên được xác định rõ. Trong giai đoạn đầu này, không cần mô tả công nghệ thông tin một cách chi tiết. Thay vào đó là một tóm tắt cơ bản về thông tin được phân tích cho một quy trình của tổ chức và các ứng dụng và hệ thống ICT liên quan.

Việc phân tích các quy trình của tổ chức sẽ cung cấp các nhận định về ảnh hưởng của các sự cố an toàn thông tin đến hoạt động của tổ chức. Nhìn chung, nên đưa ra một mô tả rất cơ bản về các quy trình của tổ chức. Nên xác định và lập thành tài liệu về các quy trình, các chức năng, các địa điểm, các hệ thống thông tin và các mạng thông tin nếu chúng chưa được đưa vào phạm vi ISMS.

Nên lưu ý các vấn đề sau khi xác định các yêu cầu an toàn thông tin chi tiết cho ISMS:

a) định danh sơ bộ các tài sản thông tin quan trọng và việc bảo vệ an toàn thông tin hiện tại đối với các tài sản này;

b) xác định mong muốn của tổ chức và ảnh hưởng của mong muốn đó lên các yêu cầu xử lý thông tin trong tương lai;

c) phân tích các thể thức hiện tại về xử lý thông tin, các ứng dụng hệ thống, các mạng thông tin, địa điểm của các hoạt động và các nguồn lực IT...;

d) xác định tất cả các yêu cầu quan trọng (ví dụ các yêu cầu của pháp luật và quy định, các nghĩa vụ thỏa thuận, các yêu cầu của tổ chức, các tiêu chuẩn theo ngành nghề, các thỏa thuận giữa khách hàng và nhà cung cấp, các điều kiện bảo hiểm...);

e) xác định mức độ nhận thức về an toàn thông tin, và từ đó đưa ra các yêu cầu về giáo dục và đào tạo tương ứng với mỗi đơn vị quản trị và vận hành.

Đầu ra

Sản phẩm của hoạt động này gồm:

a) định danh các quy trình chính, các chức năng, địa điểm, các hệ thống thông tin và các mạng truyền thông;

b) các tài sản thông tin của tổ chức;

c) phân loại các quy trình/tài sản trọng yếu;

d) các yêu cầu về an toàn thông tin thu được từ các yêu cầu của pháp luật, quy định và hợp đồng của tổ chức;

e) danh sách các điểm yếu phổ biến sẽ được xử lý như một kết quả của các yêu cầu an toàn;

f) các yêu cầu về giáo dục và đạo tạo an toàn thông tin của tổ chức.

Thông tin khác

Không có thông tin đặc biệt nào khác

7.3 Xác định các tài sản thuộc phạm vi ISMS

Hoạt động

Xác định rõ các tài sản sẽ được ISMS hỗ trợ.

Đầu vào

a) đầu ra từ Hoạt động 6.5 Phối hợp phạm vi và các giới hạn để nhận được phạm vi và các giới hạn ISMS – Phạm vi và các giới hạn ISMS;

b) đầu ra từ Hoạt động 6.6 Phát triển chính sách ISMS và được ban quản lý phê chuẩn – Chính sách ISMS;

c) đầu ra từ Hoạt động 7.2 Xác định các yêu cầu an toàn thông tin cho quy trình ISMS.

Hướng dẫn

Để xác định được các tài sản thuộc phạm vi ISMS, nên xác định và lập danh sách các thông tin sau:

a) tên của quy trình;

b) mô tả quy trình và các hoạt động liên quan (được thiết lập, được lưu trữ, được trao đổi, bị loại bỏ);

c) tầm quan trọng của quy trình đối với tổ chức (trọng yếu, quan trọng, không quan trọng);

d) đơn vị sở hữu quy trình (đơn vị thuộc tổ chức);

e) các quy trình cung cấp đầu vào và đầu ra từ quy trình này;

f) các ứng dụng IT hỗ trợ quy trình;

g) phân loại thông tin (bí mật, toàn vẹn, sẵn sàng, điều khiển truy cập, chống chối bỏ, và/hoặc các tài sản quan trọng khác đối với tổ chức, ví dụ, thời gian thông tin có thể được lưu trữ).

Đầu ra

Sản phẩm của hoạt động này bao gồm:

a) các tài sản thông tin đã được xác định của các quy trình chính của tổ chức thuộc phạm vi ISMS;

b) phân loại an toàn thông tin của các quy trình và các tài sản thông tin trọng yếu;

Thông tin khác

Không có thông tin đặc biệt nào khác.

7.4 Tiến hành đánh giá an toàn thông tin

Hoạt động

Thực hiện đánh giá an toàn thông tin bằng cách so sánh tình trạng an toàn thông tin hiện tại của tổ chức với các mục tiêu mong muốn.

Đầu vào

a) đầu ra từ Hoạt động 6.5 Phối hợp phạm vi và các giới hạn để nhận được phạm vi và các giới hạn ISMS – Phạm vi và các giới hạn của ISMS;

b) đầu ra từ Hoạt động 6.6 Phát triển chính sách ISMS và được ban quản lý phê chuẩn - Chính sách ISMS;

c) đầu ra từ Hoạt động 7.2 Xác định các yêu cầu an toàn thông tin cho quy trình ISMS;

d) đầu ra từ Hoạt động 7.3 Xác định các tài sản thuộc phạm vi ISMS.

Hướng dẫn

Đánh giá an toàn thông tin là hoạt động xác định mức an toàn thông tin hiện tại (tức là các thủ tục xử lý bảo vệ thông tin hiện tại của tổ chức). Mục đích cơ bản của đánh giá an toàn thông tin là cung cấp thông tin dưới dạng chính sách và các hướng dẫn để hỗ trợ việc mô tả được yêu cầu cho hệ thống quản lý. Điều đó rất cần thiết để đảm bảo rằng các thiếu sót đã được xác định được xử lý song song bằng một kế hoạch hành động tối ưu. Tất cả các bên tham gia đều nên biết rõ các kết quả phân tích của tổ chức, các tài liệu tiêu chuẩn, và có liên hệ với người quản lý phù hợp.

Những đánh giá về an toàn thông tin sẽ phân tích tình huống hiện tại của tổ chức dựa trên các thông tin sau, xác định hiện trạng an toàn thông tin và lập tài liệu về các điểm yếu:

a) các sự kiện cơ bản xảy ra với các quy trình then chốt;

b) phân loại các tài sản thông tin;

c) yêu cầu an toàn thông tin về tổ chức.

Các kết quả đánh giá an toàn thông tin cùng với các mục tiêu của tổ chức thường là yếu tố quan trọng thúc đẩy các hoạt động an toàn thông tin trong tương lai. Đánh giá an toàn thông tin nên được thực hiện bởi một nguồn lực nội bộ hoặc bên ngoài hoàn toàn độc lập với tổ chức.

Những người tham gia vào việc đánh giá an toàn thông tin nên là các cá nhân có hiểu biết vững về môi trường, các điều kiện hiện tại và những vấn đề liên quan đến an toàn thông tin. Các cá nhân này nên được chọn lựa từ các bộ phận khác nhau của tổ chức và bao gồm:

a) những người quản lý chuyên môn (ví dụ những người đứng đầu các bộ phận của tổ chức);

b) những người sở hữu quy trình (tức là đại diện cho những khu vực quan trọng của tổ chức);

c) các cá nhân khác có hiểu biết vững về môi trường, các điều kiện hiện tại, và những vấn đề liên quan đến an toàn thông tin. Ví dụ, những người dùng quy trình nghiệp vụ và những người thực hiện chức năng quản trị, vận hành và pháp lý.

Dưới đây là các hành động quan trọng để có thể đánh giá an toàn thông tin thành công:

a) xác định và lập danh sách các tiêu chuẩn liên quan của tổ chức (ví dụ TCVN ISO/IEC 27002:2011 (ISO/IEC 27002:2005));

b) xác định các yêu cầu quản lý xuất hiện từ các chính sách, các yêu cầu pháp lý và quy định, các nghĩa vụ thỏa thuận, các vấn đề nảy sinh từ quá trình soát xét trước đây, hoặc những vấn đề nảy sinh từ các đánh giá rủi ro trước đây.

c) sử dụng các thông tin trên như các tài liệu tham khảo dùng cho ước đoán sơ bộ sẽ được thực hiện theo các yêu cầu hiện tại của tổ chức về mức an toàn thông tin.

Sự phân cấp ưu tiên kết hợp với những phân tích của tổ chức sẽ là cơ sở để xem xét các biện pháp phòng ngừa và kiểm tra (biện pháp quản lý) an toàn thông tin.

Cách thức tiến hành đánh giá an toàn thông tin như sau:

a) lựa chọn các quy trình nghiệp vụ tổ chức quan trọng và các bước quy trình theo các yêu cầu an toàn thông tin;

b) xây dựng một biểu đồ đầy đủ bao hàm hết các quy trình chính của tổ chức, bao gồm cả cơ sở hạ tầng (logic và kỹ thuật) nếu tổ chức chưa có biểu đồ này hoặc biểu đồ chưa được thực hiện trong quá trình phân tích của tổ chức;

c) thảo luận với một cá nhân phù hợp có vai trò chính và phân tích tình huống hiện tại của tổ chức theo mối quan hệ với các yêu cầu an toàn thông tin. Ví dụ, các quy trình nào là trọng yếu, hiện

tại chúng vận hành thế nào? (Các kết quả về sau sẽ được sử dụng trong quá trình đánh giá rủi ro);

d) xác định các thiếu sót của các biện pháp quản lý bằng cách so sánh các biện pháp quản lý hiện tại với các yêu cầu của các biện pháp quản lý đã được xác định trước đó;

e) hoàn thiện và lập tài liệu về tình trạng hiện tại.

Đầu ra

Sản phẩm của hoạt động này là:

a) tài liệu tóm tắt tình trạng an toàn đã được đánh giá của tổ chức, và các điểm yếu đã được ước lượng.

Thông tin khác

Việc đánh giá an toàn thông tin được tiến hành tại giai đoạn này sẽ chỉ đưa ra các thông tin sơ bộ về tình trạng và các điểm yếu an toàn thông tin của tổ chức, vì bộ chính sách và tiêu chuẩn an toàn thông tin đầy đủ sẽ được phát triển ở giai đoạn sau (xem điều 9) và cho đến thời điểm này vẫn chưa tiến hành đánh giá rủi ro.

8 Tiến hành đánh giá rủi ro và lập kế hoạch xử lý rủi ro

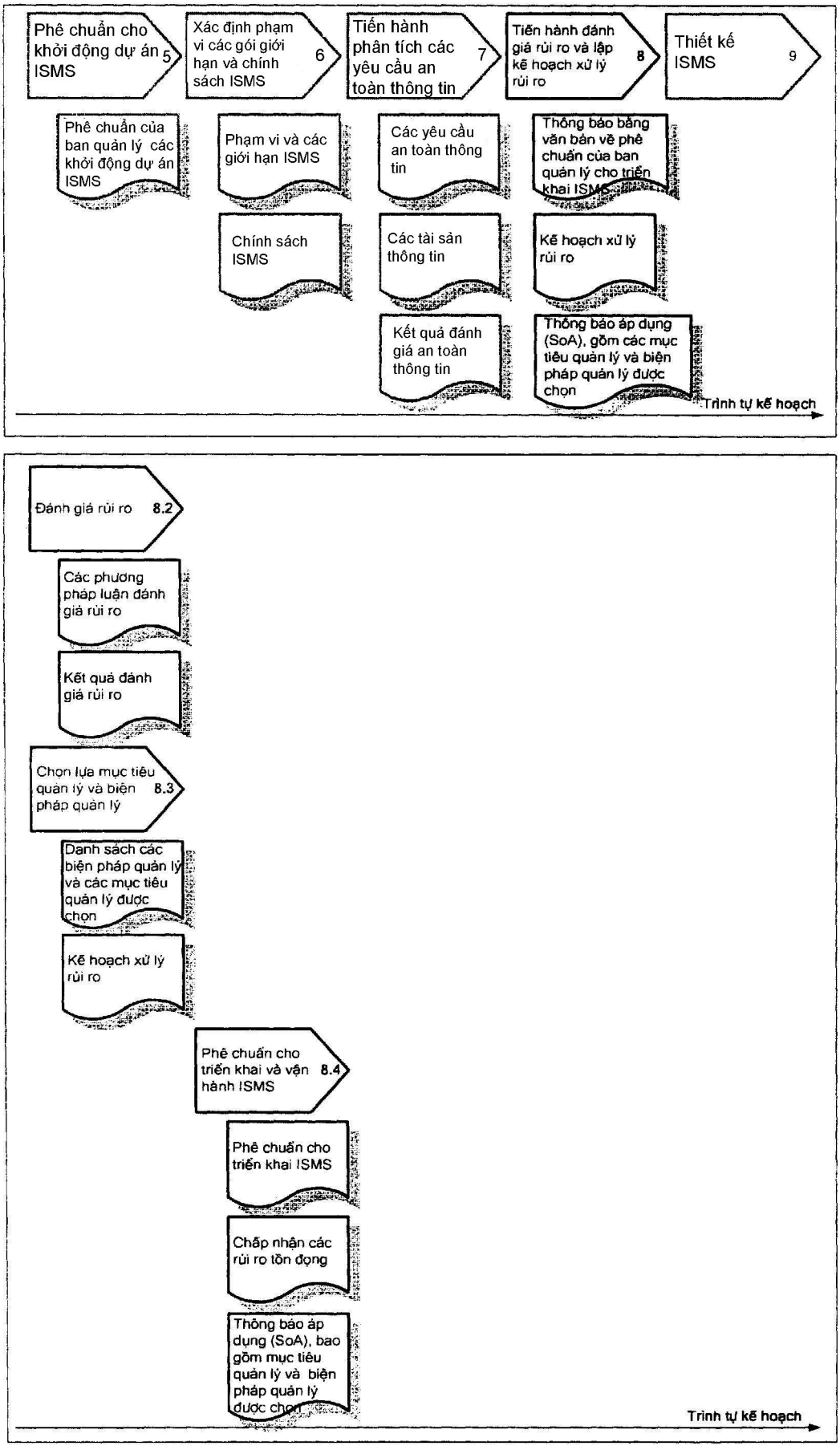
8.1 Tổng quan về tiến hành đánh giá rủi ro và lập kế hoạch xử lý rủi ro

Triển khai một ISMS nên giải quyết nhiều rủi ro an toàn thông tin liên quan. Việc định danh, ước lượng, xử lý rủi ro theo kế hoạch và lựa chọn mục tiêu quản lý và biện pháp quản lý là những bước quan trọng trong triển khai ISMS và nên được thực hiện trong giai đoạn này.

TCVN 10295:2014 (ISO/IEC 27005:2011) đưa ra hướng dẫn cụ thể về Quản lý rủi ro an toàn thông tin và sẽ được tham chiếu xuyên suốt điều 8.

Giả sử rằng ban quản lý đã cam kết triển khai ISMS, phạm vi và chính sách ISMS đã được xác định, và các tài sản thông tin cũng đã được xác định theo kết quả đánh giá an toàn thông tin.

Mục tiêu:
Nhằm xác định phương pháp đánh giá rủi ro, xác định, phân tích và ước lượng rủi ro an toàn thông tin để chọn lựa cách xử lý rủi ro, mục tiêu quản lý và biện pháp quản lý.
Tham khảo 4.2.1 c) đến 4.2.1 j) của TCVN ISO/IEC 27001:2009 (ISO/IEC 27001:2005).



Hình 6 - Tổng quan về giai đoạn đánh giá rủi ro

8.2 Tiến hành đánh giá rủi ro

Hoạt động

Thực hiện đánh giá rủi ro.

Đầu vào

a) đầu ra từ hoạt động trong điều 7 Tiến hành phân tích các yêu cầu an toàn thông tin – Thông tin về:

1) tình trạng an toàn thông tin đã được tóm tắt;

2) các tài sản thông tin đã được xác định.

b) đầu ra từ hoạt động trong điều 6 Xác định phạm vi, các giới hạn và chính sách ISMS – Các nội dung đã được lập thành tài liệu:

1) phạm vi ISMS;

2) chính sách ISMS.

c) TCVN 10295:2014 (ISO/IEC 27005:2011).

Hướng dẫn

Hiệu suất của mỗi đánh giá rủi ro trong bối cảnh nghiệp vụ thuộc phạm vi ISMS là yếu tố cần thiết để tuân thủ và triển khai ISMS thành công theo TCVN ISO/IEC 27001:2009 (ISO/IEC 27001:2005). Đánh giá rủi ro nên:

a) xác định các mối đe dọa và nguồn gốc của chúng;

b) xác định các biện pháp quản lý hiện hành và đã được hoạch định;

c) xác định các điểm yếu có thể bị các mối đe dọa khai thác để gây hại cho tài sản hoặc tổ chức;

d) xác định hậu quả gây mất tính bí mật, toàn vẹn, sẵn sàng, chống chối bỏ, và những yêu cầu an toàn khác đối với tài sản;

e) đánh giá tác động nghiệp vụ có thể nảy sinh từ các sự cố an toàn thông tin đã lường trước hoặc trên thực tế;

f) đánh giá các kịch bản sự cố có thể xảy ra;

g) ước đoán mức độ rủi ro;

h) so sánh mức độ rủi ro với chỉ tiêu đánh giá rủi ro và chỉ tiêu chấp nhận rủi ro.

Những người tham gia vào việc đánh giá rủi ro nên là những cá nhân có kiến thức vững chắc về các mục tiêu của tổ chức cũng như hiểu biết về vấn đề an toàn (ví dụ có kiến thức sâu sắc về những gì liên quan đến các mối đe dọa các mục tiêu của tổ chức). Những người này nên được chọn từ nhiều bộ phận của tổ chức. Tham khảo Phụ lục B, "Các vai trò và trách nhiệm về an toàn thông tin".

Mỗi tổ chức có thể sử dụng một phương pháp đánh giá rủi ro riêng phù hợp với đặc thù của dự án,đặc thù của tổ chức hoặc chuẩn đặc thù về ngành nghề.

Đầu ra

Sản phẩm của hoạt động này là:

a) bản mô tả các phương pháp đánh giá rủi ro;

b) các kết quả từ đánh giá rủi ro.

Thông tin khác

Phụ lục B – Thông tin về các vai trò và trách nhiệm.

CHÚ THÍCH: Kịch bản sự cố là mô tả về một mối đe dọa sẽ khai thác một hoặc nhiều điểm yếu trong một sự cố an toàn thông tin. TCVN ISO/IEC 27001:2009 (ISO/IEC 27001:2005) mô tả sự tồn tại của kịch bản sự cố như là "những thất bại về an toàn" (xem TCVN 10295:2014 (ISO/IEC 27005:2011)).

8.3 Chọn lựa mục tiêu và biện pháp quản lý

Hoạt động

Xác định các phương án xử lý rủi ro và lựa chọn các biện pháp quản lý thích hợp theo các phương án xử lý rủi ro đã được xác định.

Đầu vào

a) đầu ra của hoạt động 8.2 Tiến hành đánh giá rủi ro – Kết quả đánh giá rủi ro;

b) TCVN 10295:2014 (ISO/IEC 27005:2011);

c) TCVN ISO/IEC 27002:2011 (ISO/IEC 27002:2005).

Hướng dẫn

Điều quan trọng là phải đặc tả mối quan hệ giữa các rủi ro và các phương án đã được chọn để xử lý chúng (ví dụ, một kế hoạch xử lý rủi ro), vì việc này sẽ cung cấp một tóm tắt về xử lý rủi ro. Các phương án có thể để xử lý rủi ro đã được liệt kê trong 4.2.1 f) của TCVN ISO/IEC 27001:2009 (ISO/IEC 27001:2005).

Phụ lục A "Các mục tiêu quản lý và biện pháp quản lý" của TCVN ISO/IEC 27001:2009 (ISO/IEC 27001:2005) được sử dụng để lựa chọn mục tiêu quản lý và biện pháp quản lý cho xử lý rủi ro. Nếu không tìm được mục tiêu quản lý và biện pháp quản lý thích hợp ở Phụ lục A thì phải xác định và sử dụng các mục tiêu và biện pháp quản lý thay thế khác. Điều quan trọng là phải chứng minh được rằng phương thức giảm bớt rủi ro của các biện pháp quản lý được lựa chọn sẽ đúng như yêu cầu từ kế hoạch xử lý rủi ro.

Dữ liệu trong Phụ lục A của TCVN ISO/IEC 27001:2009 (ISO/IEC 27001:2005) là chưa thực sự đầy đủ. Cũng có thể xác định thêm các biện pháp quản lý đặc trưng theo ngành nghề để hỗ trợ các nhu cầu cụ thể của nghiệp vụ cũng như của ISMS.

Để giảm nhẹ rủi ro, việc kiểm soát mối quan hệ giữa mỗi rủi ro và các mục tiêu, biện pháp quản lý được chọn sẽ rất có lợi cho việc thiết kế triển khai ISMS. Thông tin này có thể được bổ sung vào danh sách mô tả mối quan hệ giữa các rủi ro và các phương án được chọn để xử lý rủi ro.

Để hỗ trợ việc đánh giá, tổ chức nên biên soạn một danh sách các biện pháp quản lý đã được chọn là phù hợp và khả thi đối với ISMS của tổ chức. Điều đó sẽ làm tăng sự thuận lợi trong việc cải thiện các mối quan hệ nghiệp vụ, ví dụ thuê khoán bằng hình thức điện tử, bằng cách đưa ra bản tóm tắt các biện pháp quản lý được áp dụng.

Cần đặc biệt lưu ý rằng, bản tóm tắt các biện pháp quản lý thường chứa những thông tin nhạy cảm. Vì vậy, cần phải rất thận trọng trong việc lập bản tóm tắt các biện pháp quản lý để cung cấp nội bộ và ra bên ngoài tổ chức. Trong khi xác định tài sản, có thể cũng nên cân nhắc cả các thông tin đã được tạo ra trong quá trình thiết lập ISMS.

Đầu ra

Sản phẩm của hoạt động này gồm:

a) danh sách các biện pháp và mục tiêu quản lý đã được chọn;

b) kế hoạch xử lý rủi ro, gồm:

1) mô tả quan hệ giữa các rủi ro và phương án xử lý rủi ro đã được chọn;

2) mô tả mối quan hệ giữa các rủi ro và các mục tiêu, biện pháp quản lý đã được chọn (đặc biệt trong trường hợp nhằm giảm rủi ro)

Thông tin khác

TCVN ISO/IEC 27002:2011 (ISO/IEC 27002:2005).

8.4 Phê chuẩn cho triển khai và vận hành ISMS

Hoạt động

Được ban quản lý phê chuẩn cho triển khai ISMS và lập văn bản chấp nhận các rủi ro tồn đọng.

Đầu vào

a) đầu ra từ Hoạt động 5.4 Xây dựng tình huống nghiệp vụ và kế hoạch dự án trình ban quản lý phê – phê chuẩn ban đầu của ban quản lý về dự án ISMS;

b) đầu ra từ Hoạt động trong điều 6 Xác định phạm vi, các giới hạn và chính sách ISMS – Các nội dung đã lập thành tài liệu:

1) các mục tiêu và chính sách ISMS;

2) phạm vi của ISMS.

c) đầu ra từ Hoạt động 8.2 Tiến hành đánh giá rủi ro – Các nội dung đã lập thành tài liệu:

1) mô tả các phương pháp đánh giá rủi ro;

2) kết quả đánh giá rủi ro.

d) đầu ra từ Hoạt động 8.3 Chọn lựa mục tiêu và biện pháp quản lý – Kế hoạch xử lý rủi ro.

Hướng dẫn

Để được ban quản lý phê chuẩn, nên chuẩn bị các tài liệu đã được mô tả trong phần đầu vào để ban quản lý đánh giá và đưa ra quyết định.

Việc chuẩn bị cho Thông báo áp dụng (SoA) cũng thuộc những nỗ lực quản lý an toàn thông tin. Mức độ chi tiết của thông tin mô tả các biện pháp quản lý phải đáp ứng được các yêu cầu cần thiết để có thể hỗ trợ ban quản lý phê chuẩn ISMS.

Phê chuẩn chấp nhận các rủi ro tồn đọng và cấp phép vận hành thực sự cho ISMS nên được thực hiện bởi ban quản lý cao nhất. Những quyết định đó nên dựa trên cơ sở đánh giá rủi ro và các cơ hội có thể có được khi triển khai ISMS nếu so sánh với các cơ hội khi không triển khai ISMS.

Đầu ra

Sản phẩm của hoạt động này gồm:

a) thông báo bằng văn bản về phê chuẩn cho triển khai ISMS của ban quản lý;

b) chấp nhận của ban quản lý về các rủi ro tồn đọng;

c) thông báo áp dụng, bao gồm mục tiêu quản lý và biện pháp quản lý được chọn.

Thông tin khác

Không có thông tin đặc biệt nào khác.

9 Thiết kế ISMS

9.1 Tổng quan về thiết kế ISMS

Nên xây dựng thiết kế chi tiết của dự án ISMS và phát triển các hoạt động đã được hoạch định để triển khai ISMS. Tùy thuộc vào kết quả từ các hoạt động trước đó cũng như kết quả của các hoạt động cụ thể trong giai đoạn thiết kế sẽ được nêu trong điều này, mỗi tổ chức sẽ xây dựng được một kế hoạch dự án ISMS chi tiết chính thức riêng.

Kế hoạch triển khai dự án ISMS chính thức cụ thể là đầu ra của điều này. Dựa trên kế hoạch đó, dự án ISMS có thể được khởi động trong tổ chức với vai trò là giai đoạn "DO" của mô hình PDCA đã được nêu trong TCVN ISO/IEC 27001:2009 (ISO/IEC 27001:2005).

Giả sử rằng ban quản lý đã cam kết triển khai ISMS như đã xác định trong phạm vi và chính sách ISMS. Các tài sản thông tin và các kết quả đánh giá an toàn thông tin giả sử đã sẵn sàng. Và, kế hoạch xử lý rủi ro có mô tả các rủi ro, các phương án xử lý rủi ro cùng với các mục tiêu quản lý và biện pháp quản lý được chọn cũng đã sẵn sàng.

Thiết kế ISMS được mô tả ở đây tập trung vào cấu trúc bên trong và yêu cầu của ISMS. Cũng cần lưu ý rằng, trong một số các trường hợp, thiết kế ISMS có thể có tác động trực tiếp hay gián tiếp đến thiết kế các quy trình nghiệp vụ. Ngoài ra, cần lưu ý rằng, việc tích hợp các thành phần của ISMS với các cơ sở hạ tầng và công việc quản lý có trước vẫn là yêu cầu luôn luôn tồn tại.

Mục tiêu: Nhằm hoàn thiện kế hoạch triển khai ISMS chính thức bằng cách: thiết kế an toàn về tổ chức dựa trên các phương án xử lý rủi ro được chọn và các yêu cầu liên quan đến việc lập hồ sơ và tài liệu, thiết kế các biện pháp quản lý phối hợp cung cấp sự an toàn cho ICT, các quy trình vật lý và tổ chức, và thiết kế yêu cầu cụ thể về ISMS.

Xem 4.2.2 a) - e), h) của TCVN ISO/IEC 27001:2009 (ISO/IEC 27001:2005).

Trong khi thiết kế ISMS, nên quan tâm đến các nội dung sau:

a) sự an toàn về tổ chức – bao hàm các khía cạnh quản trị của an toàn thông tin, gồm cả trách nhiệm thực hiện xử lý rủi ro của tổ chức. Nội dung này nên được thể hiện dưới dạng tập hợp các hoạt động để có được các chính sách, mục tiêu, quy trình và thủ tục để xử lý và cải thiện an toàn thông tin theo các nhu cầu và rủi ro của tổ chức;

b) an toàn ICT – bao hàm các khía cạnh an toàn thông tin liên quan cụ thể đến trách nhiệm vận hành ICT nhằm giảm rủi ro. Nội dung này nhằm đáp ứng các yêu cầu của tổ chức và triển khai kỹ thuật của các biện pháp quản lý nhằm giảm rủi ro;

c) an toàn vật lý – bao hàm các khía cạnh an toàn thông tin liên quan cụ thể đến trách nhiệm xử lý môi trường vật lý, ví dụ các trụ sở và cơ sở hạ tầng của chúng nhằm giảm rủi ro. Nội dung này nhằm đáp ứng các yêu cầu của tổ chức và triển khai kỹ thuật của các biện pháp quản lý nhằm giảm rủi ro;

d) ISMS cụ thể – bao hàm các khía cạnh của các yêu cầu cụ thể khác của ISMS theo TCVN ISO/IEC 27001:2009 (ISO/IEC 27001:2005), ngoại trừ các vấn đề đã bao hàm trong ba nội dung trên. Nội dung này tập trung vào những hoạt động cụ thể nên được tiến hành khi triển khai để có được một ISMS sẵn sàng vận hành, bao gồm:

    1) giám sát;

    2) đo lường;

    3) đánh giá ISMS nội bộ;

    4) đào tạo và nâng cao nhận thức;

    5) quản lý sự cố;

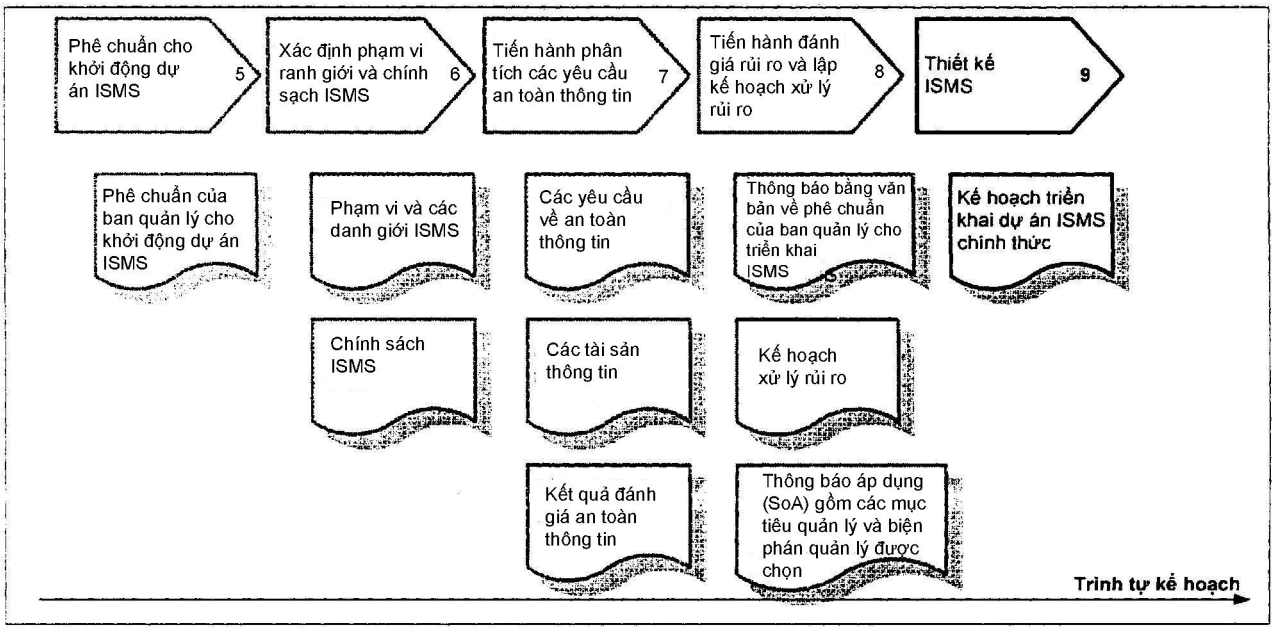
    6) soát xét của ban quản lý;

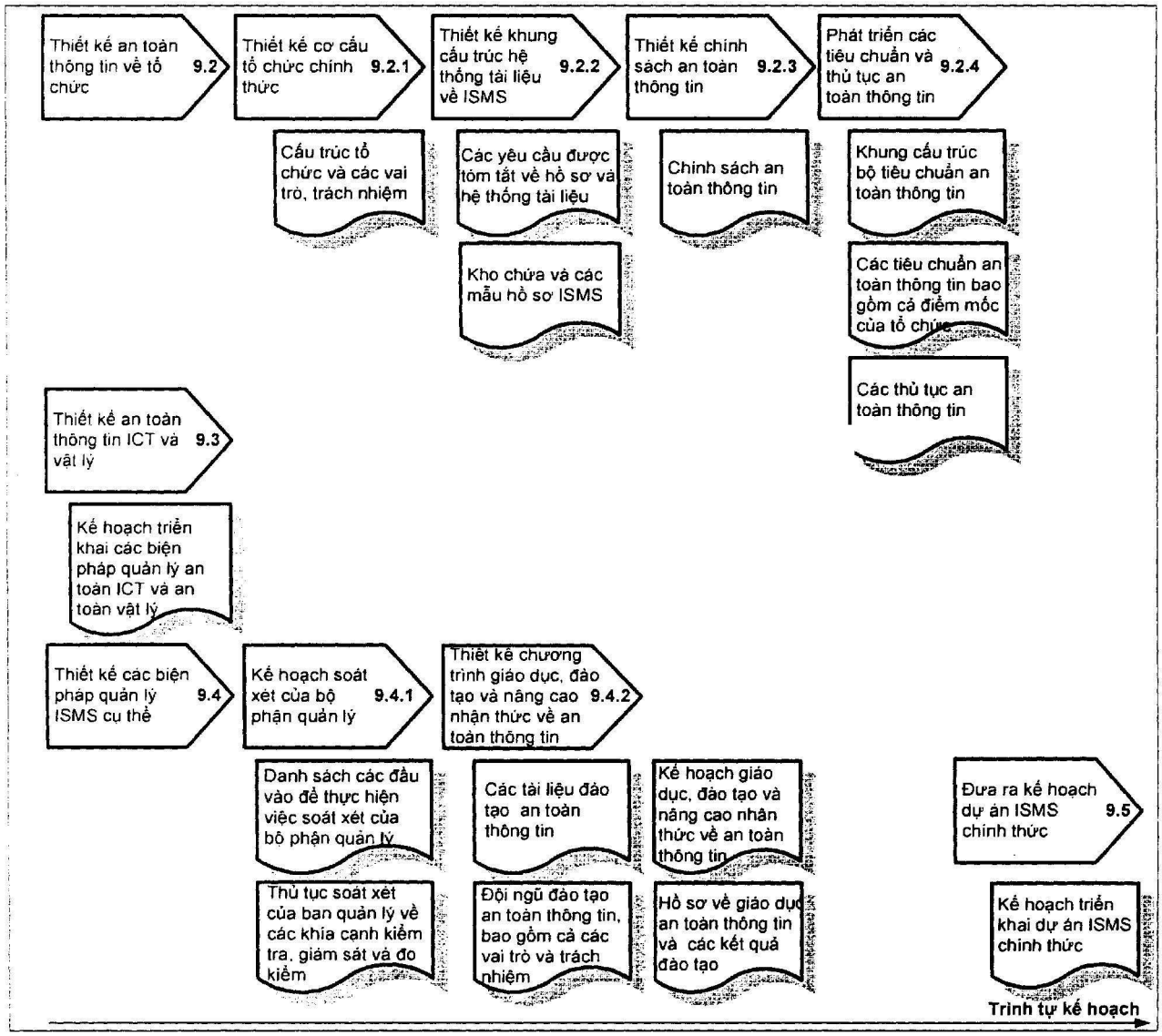
    7) cải tiến ISMS bao gồm các hành động ngăn ngừa và khắc phục.

Việc phát triển Dự án ISMS và thiết kế triển khai các biện pháp quản lý theo kế hoạch nên có sự tham gia và sử dụng các kỹ năng và kinh nghiệm của đội ngũ nhân viên từ các bộ phận của tổ chức thuộc phạm vi ISMS hoặc từ các bộ phận có trách nhiệm quản lý liên quan đến ISMS. Các khía cạnh cụ thể này của ISMS cũng cần được trao đổi với ban quản lý.

Để thiết kế các biện pháp quản lý đã được lựa chọn để xử lý rủi ro, điều cốt yếu là phải thiết kế môi trường an toàn vật lý và ICT và môi trường an toàn về tổ chức. An toàn ICT không chỉ tập trung vào các hệ thống thông tin và mạng mà còn cả các yêu cầu về vận hành. An toàn vật lý tập trung vào tất cả các khía cạnh về quản lý truy cập, chống chối bỏ, bảo vệ vật lý các tài sản thông tin và những gì được lưu trữ, hoặc giữ lại, và cả các phương tiện bảo vệ các biện pháp quản lý an toàn.

Các biện pháp quản lý được chọn trong các hoạt động được mô tả trong 8.3 nên được triển khai theo một kế hoạch triển khai chi tiết và được cấu trúc cụ thể thuộc kế hoạch dự án ISMS. Phần thông tin cụ thể này của kế hoạch dự án ISMS nên đưa ra cách thức xử lý từng rủi ro để đạt được các mục tiêu quản lý. Phần thông tin cụ thể này của kế hoạch dự án ISMS rất quan trọng để các biện pháp quản lý được chọn được triển khai đúng và có hiệu lực. Nhóm quản lý an toàn thông tin có trách nhiệm xây dựng phần thông tin cụ thể này trong kế hoạch triển khai dự án, và về sau phần thông tin này sẽ được đưa vào kế hoạch dự án ISMS chính thức.





Hình 7 – Tổng quan về giai đoạn thiết kế ISMS

9.2 Thiết kế an toàn thông tin về tổ chức

9.2.1 Thiết kế cơ cấu tổ chức chính thức cho an toàn thông tin

Hoạt động

Phân định các chức năng, vai trò và trách nhiệm tổ chức về an toàn thông tin đồng nhất theo xử lý rủi ro.

Đầu vào

a) đầu ra từ Hoạt động 5.3.2 Xác định vai trò và trách nhiệm đối với phạm vi ISMS sơ bộ - Bảng mô tả các vai trò và trách nhiệm;

b) đầu ra từ Hoạt động 6.5 Phối hợp phạm vi và các giới hạn để nhận được phạm vi và các giới hạn ISMS – Phạm vi và các giới hạn của ISMS;

c) đầu ra từ Hoạt động 6.6 Phát triển chính sách ISMS và được ban quản lý phê chuẩn – Chính sách ISMS;

d) đầu ra từ Hoạt động 7.2 Xác định các yêu cầu an toàn thông tin cho quy trình ISMS;

e) đầu ra từ Hoạt động 7.3 Xác định các tài sản thuộc phạm vi ISMS;

f) đầu ra từ Hoạt động 7.4 Tiến hành đánh giá an toàn thông tin;

g) đầu ra từ Hoạt động 8.2 Tiến hành đánh giá rủi ro – Các kết quả của đánh giá rủi ro;

h) đầu ra từ Hoạt động 8.3 Chọn lựa mục tiêu và biện pháp quản lý;

i) TCVN ISO/IEC 27002:2011 (ISO/IEC 27002:2005).

Hướng dẫn

Thiết kế các cơ cấu tổ chức và các quy trình vận hành ISMS nội bộ, nếu khả thi, nên dựa trên và tích hợp với các cấu trúc quản lý đã có. Tương tự như vậy, việc tích hợp ISMS vào các cấu trúc quản lý sẵn có có quy mô lớn hơn (ví dụ, đánh giá nội bộ) nên được xét đến trong quy trình thiết kế ISMS.

Cơ cấu tổ chức được thiết kế cho ISMS cũng nên phản ánh các hoạt động triển khai và vận hành ISMS, cũng như đưa ra các vấn đề liên quan đến các vận hành ISMS, ví dụ các phương pháp giám sát và lập hồ sơ.

Do đó, cấu trúc cho các vận hành ISMS nên được thiết kế dựa trên triển khai ISMS theo kế hoạch có cân nhắc các vấn đề sau đây:

a) liệu mỗi một vai trò về triển khai ISMS có cần thiết cho các vận hành ISMS không?

b) các vai trò đã được xác định có khác các vai trò về triển khai ISMS không?

c) cần bổ sung những vai trò nào về triển khai ISMS?

Ví du, có thể bổ sung những vai trò về vận hành ISMS dưới đây:

a) người có trách nhiệm về các thực thi an toàn thông tin trong mỗi bộ phận;

b) người có trách nhiệm về đo lường ISMS trong mỗi bộ phận.

Lưu ý đến các vấn đề được đề cập trong Phụ lục B " Các vai trò và trách nhiệm về an toàn thông tin" có thể giúp đưa ra quyết định về cấu trúc và vai trò về vận hành ISMS khi xét duyệt lại cấu trúc và các vai trò về vận hành ISMS.

Đầu ra

Sản phẩm của hoạt động này là tài liệu tóm tắt:

a) cơ cấu tổ chức, các vai trò và trách nhiệm của cơ cấu tổ chức đó.

Thông tin khác

Phụ lục B – Thông tin về các vai trò và trách nhiệm.

Phụ lục C – Thông tin về lập kế hoạch đánh giá.

9.2.2 Thiết kế cấu trúc khung hệ thống tài liệu về ISMS

Hoạt động

Xác định các yêu cầu và cấu trúc khung của hồ sơ và tài liệu về ISMS để đáp ứng các yêu cầu quản lý liên tục hồ sơ và tài liệu về ISMS.

Đầu vào

a) đầu ra từ Hoạt động 6.5 Phối hợp phạm vi và các giới hạn để nhận được phạm vi và các giới hạn ISMS – Phạm vi và các giới hạn của ISMS;

b) định nghĩa phạm vi và các giới hạn của ISMS;

c) đầu ra từ Hoạt động 6.6 Phát triển chính sách ISMS và được ban quản lý phê chuẩn – Chính sách ISMS;

d) đầu ra từ hoạt động 8.4 Phê chuẩn cho triển khai và vận hành ISMS ;

e) đầu ra từ hoạt động 9.2.1 Thiết kế cơ cấu tổ chức chính thức cho an toàn thông tin;

f) TCVN ISO/IEC 27002:2011 (ISO/IEC 27002:2005).

Hướng dẫn

Thiết kế lập hồ sơ ISMS bao gồm những hoạt động sau:

a) cấu trúc khung mô tả các nguyên tắc lập tài liệu ISMS, cấu trúc các quy trình lập tài liệu về ISMS, các vai trò liên quan, các định dạng dữ liệu và báo cáo ban quản lý các đường dẫn;

b) thiết kế các yêu cầu về tài liệu;

c) thiết kế các yêu cầu về hồ sơ.

Hệ thống tài liệu ISMS nên gồm các hồ sơ về các quyết định của ban quản lý; đảm bảo rằng các hành động đều có thể được truy vết tới các quyết định và chính sách của ban quản lý; và đảm bảo rằng các kết quả trong hồ sơ đều có thể được tái tạo lại.

Các tài liệu ISMS nên đưa ra được các chứng cứ cho thấy các biện pháp quản lý đều được lựa chọn dựa trên kết quả của đánh giá rủi ro và xử lý rủi ro, và các quy trình đó đã được triển khai theo các mục tiêu và chính sách ISMS.

Hệ thống tài liệu có ý nghĩa rất quan trọng giúp tái tạo các kết quả và quy trình. Đối với các biện pháp quản lý đã được chọn, việc xây dựng và hệ thống tài liệu của các quy trình nên được giao cho một người chịu trách nhiệm.

Hệ thống tài liệu ISMS nên gồm các tài liệu như được nêu trong 4.3.1 của TCVN ISO/IEC 27001:2009 (ISO/IEC 27001:2005).

Các tài liệu ISMS phải được quản lý và sẵn sàng cung cấp đến người dùng khi cần. Về vấn đề này, cần thực hiện các thủ tục sau:

a) thiết lập thủ tục hành chính về quản lý tài liệu ISMS;

b) phê chuẩn chính thức các tài liệu trước khi ban hành;

c) đảm bảo rằng những thay đổi và tình trạng sửa đổi hiện hành của tài liệu đã được xác định;

d) bảo vệ và quản lý các tài liệu như một tài sản thông tin của tổ chức.

Điều quan trọng là các phiên bản liên quan của các tài liệu áp dụng phải luôn sẵn sàng cho những người cần sử dụng, đảm bảo rằng các tài liệu phải dễ đọc, dễ tìm, được chuyển giao, lưu trữ và cuối cùng được hủy bỏ theo các quy trình phù hợp với phân loại của chúng.

Hơn nữa, phải đảm bảo các tài liệu có nguồn gốc từ bên ngoài đều được xác định rõ, việc quảng bá chúng phải được quản lý nhằm ngăn ngừa tình trạng vô tình sử dụng các tài liệu đã hết hiệu lực, và áp dụng các biện pháp truy vết thích hợp đối với chúng nếu chúng vẫn được giữ lại cho mục đích nào đó.

Các hồ sơ nên được thiết lập, bảo quản và quản lý như một bằng chứng cho thấy ISMS của tổ chức đã tuân thủ TCVN ISO/IEC 27001:2009 (ISO/IEC 27001:2005), và cho thấy hiệu lực của các vận hành ISMS.

Cũng cần giữ lại các hồ sơ về tình trạng triển khai của toàn bộ chu trình PDCA, cũng như những hồ sơ về các sự kiện và các sự cố an toàn thông tin, các hồ sơ về giáo dục, đào tạo, các kỹ năng, kinh nghiệm và các văn bằng chứng chỉ, các soát xét ISMS nội bộ, các hành động phòng ngừa và khắc phục, và các hồ sơ về tổ chức.

Nên thực hiện các công việc sau khi quản lý các hồ sơ:

a) lập tài liệu về các biện pháp quản lý được yêu cầu để xác định, lưu trữ, bảo vệ, tìm kiếm, loại bỏ dữ liệu, và thời gian lưu trữ tài liệu này;

b) xác định những thứ nên được lập hồ sơ, và mức độ chi tiết trong các quy trình quản lý vận hành;

c) nếu thời gian lưu trữ tài liệu đã được chỉ định trong các điều luật liên quan thì thời gian lưu trữ nên được thiết lập tuân theo yêu cầu pháp luật.

Đầu ra

Sản phẩm của hoạt động này gồm:

a) tài liệu tóm tắt các yêu cầu về hồ sơ ISMS và biện pháp quản lý tài liệu;

b) kho chứa và các mẫu hồ sơ được yêu cầu của ISMS.

Thông tin khác

Không có thông tin đặc biệt nào khác.

9.2.3 Thiết kế chính sách an toàn thông tin

Hoạt động

Lập tài liệu về vị trí chiến lược của việc quản lý và quản trị các mục tiêu an toàn thông tin theo sự vận hành ISMS.

Đầu vào

a) đầu ra từ Hoạt động 5.2 Làm rõ các ưu tiên của tổ chức cho phát triển ISMS – Các mục tiêu đã được tóm tắt và danh sách các yêu cầu;

b) đầu ra từ Hoạt động 5.4 Xây dựng tình huống nghiệp vụ và kế hoạch dự án trình ban quản lý – Phê chuẩn ban đầu của ban quản lý về dự án ISMS;

c) đầu ra từ Hoạt động 6.5 Phối hợp phạm vi và các giới hạn để nhận được phạm vi và các giới hạn ISMS – Phạm vi và các giới hạn của ISMS;

d) đầu ra từ Hoạt động 6.6 Phát triển chính sách ISMS và được ban quản lý phê chuẩn – Chính sách ISMS;

e) đầu ra từ Hoạt động 7.2 Xác định các yêu cầu an toàn thông tin cho quy trình ISMS;

f) đầu ra từ Hoạt động 7.3 Xác định các tài sản thuộc phạm vi ISMS;

g) đầu ra từ Hoạt động 7.4 Tiến hành đánh giá an toàn thông tin;

h) đầu ra từ Hoạt động 8.2 Tiến hành đánh giá rủi ro – Các kết quả của đầu ra đánh giá rủi ro từ Hoạt động 8.3 Chọn lựa mục tiêu và biện pháp quản lý;

i) đầu ra từ Hoạt động 9.2.1 Thiết kế cơ cấu tổ chức chính thức cho an toàn thông tin;

j) đầu ra từ Hoạt động 9.2.2 Thiết kế cấu trúc khung hệ thống tài liệu về ISMS;

k) TCVN ISO/IEC 27002:2011 (ISO/IEC 27002:2005) điều 5.1.1.

Hướng dẫn

Tài liệu chính sách an toàn thông tin thể hiện vị trí chiến lược của tổ chức theo các mục tiêu an toàn thông tin trong toàn bộ tổ chức.

Chính sách an toàn thông tin được xây dựng dựa trên thông tin và các hiểu biết. Những vấn đề đã được ban quản lý xác định là quan trọng trong các phân tích trước đây nên được dẫn chứng. Những khả năng có thể xảy ra nếu không tuân thủ chính sách cũng cần được chỉ rõ . Nên nhấn mạnh các tác động đáng nghi ngại của luật lệ và quy định tới tổ chức.

Các ví dụ của chính sách an toàn thông tin có thể được xây dựng từ tài liệu tham khảo, internet, các tổ chức quan tâm và các hiệp hội ngành nghề. Các trình bày và diễn giải có thể được xây dựng từ các hồ sơ thường niên, các tài liệu chính sách khác hoặc các tài liệu do ban quản lý cung cấp.

Có thể có nhiều cách diễn giải và các yêu cầu khác nhau về quy mô thực sự của một chính sách. Nên tóm tắt rõ để đội ngũ nhân viên có thể hiểu được mục đích của chính sách. Hơn nữa, cũng nên phân biệt rõ những mục tiêu nào được yêu cầu phải thỏa mãn bộ các quy định và mục tiêu của tổ chức.

Quy mô và cấu trúc của chính sách an toàn thông tin nên hỗ trợ các tài liệu được sử dụng ở giai đoạn tiếp theo trong quy trình giới thiệu hệ thống quản lý an toàn thông tin (xem thêm Phụ lục D – Cấu trúc của các chính sách).

Các tổ chức lớn và phức tạp (ví dụ, các tổ chức có trụ sở ở nhiều nơi) có thể cần phải xây dựng một chính sách tổng thể và nhiều chính sách thích ứng theo từng khu vực.

Xem hướng dẫn về nội dung tài liệu chính sách an toàn thông tin trong 5.1.1 của TCVN ISO/IEC 27002:2011 (ISO/IEC 27002:2005).

Chính sách được đề xuất (có số phiên bản và ngày ban hành) nên được kiểm tra chéo và được thiết lập trong tổ chức bởi giám đốc điều hành. Sau khi được thiết lập trong ban quản lý hoặc tương đương, giám đốc điều hành sẽ phê chuẩn chính sách an toàn thông tin. Sau đó, chính sách an toàn thông tin sẽ được chuyển cho mọi thành viên của tổ chức theo một phương thức phù hợp, dễ truy cập và dễ hiểu.

Đầu ra

Đầu ra của hoạt động này là tài liệu về chính sách an toàn thông tin.

Thông tin khác

Phụ lục B – Thông tin về các vai trò và trách nhiệm.

Phụ lục D – Thông tin về cấu trúc chính sách.

9.2.4 Phát triển các tiêu chuẩn và thủ tục an toàn thông tin

Hoạt động

Phát triển các tiêu chuẩn và thủ tục an toàn thông tin áp dụng cho toàn tổ chức hoặc các bộ phận cụ thể của tổ chức

Đầu vào

a) đầu ra từ Hoạt động 6.5 Phối hợp phạm vi và các giới hạn để nhận được phạm vi và các giới hạn ISMS – Phạm vi và các giới hạn của ISMS;

b) đầu ra từ Hoạt động 6.6 Phát triển chính sách ISMS và được ban quản lý phê chuẩn – Chính sách ISMS;

c) đầu ra từ Hoạt đông 8.2 Tiến hành đánh giá rủi ro;

d) đầu ra từ Hoạt động 8.3 Chọn lựa mục tiêu và biện pháp quản lý;

e) đầu ra từ Hoạt động 8.4 Phê chuẩn cho triển khai và vận hành ISMS – Báo cáo về khả năng ứng dụng, bao gồm các mục tiêu quản lý và các biện pháp quản lý được lựa chọn;

f) Đầu ra từ Hoạt động 9.2.1 Thiết kế cơ cấu tổ chức chính thức cho an toàn thông tin;

g) Đầu ra từ Hoạt động 9.2.2 Thiết kế cấu trúc khung hệ thống tài liệu về ISMS;

h) Đầu ra từ Hoạt động 9.2.3 Thiết kế chính sách an toàn thông tin;

i) TCVN ISO/IEC 27002:2011 (ISO/IEC 27002:2005).

Hướng dẫn

Để có cơ sở cho hoạt động an toàn thông tin trong tổ chức thì các tiêu chuẩn an toàn thông tin cũng như bộ các yêu cầu pháp lý và quy định áp dụng nên được cung cấp đến những người cần chúng.

Đại diện từ các bộ phận thuộc phạm vi ISMS của tổ chức nên tham gia vào quy trình phát triển các tiêu chuẩn và thủ tục này. Những người tham gia nên được cấp quyền và là đại diện cho tổ chức. Ví dụ, các vai trò có thể gồm:

a) những người quản lý an toàn thông tin,

b) các đại diện về an toàn vật lý,

c) những người sở hữu các hệ thống thông tin, và

d) những người sở hữu quy trình của các khu vực vận hành và chiến lược.

Nhóm biên tập các tiêu chuẩn và thủ tục này nên có số lượng nhỏ nhất có thể và được sử dụng tạm thời khi có yêu cầu. Mỗi đại diện nên chủ động giữ liên lạc với khu vực của họ để có thể hỗ trợ vận hành liên tục. Sau này, họ sẽ tiếp tục thực hiện các cải tiến về thủ tục và thông lệ khi vận hành.

Các tiêu chuẩn và thủ tục an toàn sau đó nên được sử dụng như nền tảng cơ bản cho bước thiết kế các thủ tục kỹ thuật hoặc vận hành chi tiết.

Phương thức hữu ích để phát triển các tiêu chuẩn và thủ tục an toàn thông tin là quan tâm đến từng nội dung hướng dẫn triển khai của TCVN ISO/IEC 27001:2009 (ISO/IEC 27001:2005) và TCVN ISO/IEC 27002:2011 (ISO/IEC 27002:2005) được đánh giá là khả thi (dựa trên các kết quả của đánh giá rủi ro), và mô tả chính xác xem chúng nên được áp dụng như thế nào.

Cũng nên xem xét các thủ tục và tiêu chuẩn an toàn thông tin đã có. Ví dụ, chúng có thể được cải tiến và phát triển, hoặc chúng có cần được thay thế hoàn toàn hay không?

Các tài liệu liên quan và được cập nhật nên được cấp phát cho tất cả mọi thành viên thuộc phạm vi ISMS. Các tiêu chuẩn và thủ tục an toàn thông tin nên áp dụng cho toàn bộ tổ chức hoặc được làm rõ đối với mọi cá nhân có vai trò, các hệ thống và khu vực thuộc phạm vi. Phiên bản đầu tiên nên được ban hành kịp thời.

Quy trình soát xét và sửa đổi nên được xác định ngay ở giai đoạn ban đầu. Sau đó, nên xây dựng chiến lược về phương thức phổ biến các thông tin về chính sách thay đổi.

Đầu ra

a) sản phẩm của hoạt động này là kế hoạch triển khai chi tiết và có cấu trúc đối với các biện pháp quản lý liên quan đến sự an toàn về mặt tổ chức, kế hoạch này sẽ được đưa vào kế hoạch dự án ISMS chính thức, trong đó có cả cấu trúc khung của bộ các tiêu chuẩn an toàn thông tin;

b) các tiêu chuẩn an toàn thông tin bao gồm cả điểm mốc của tổ chức;

c) các thủ tục an toàn thông tin để đạt được các tiêu chuẩn an toàn thông tin.

Thông tin khác

Phụ lục D – Thông tin về cấu trúc chính sách.

9.3 Thiết kế an toàn thông tin vật lý và ICT

Hoạt động

Thiết kế các biện pháp quản lý các môi trường an toàn vật lý và ICT.

Đầu vào

a) đầu ra từ Hoạt động 6.5 Phối hợp phạm vi và các giới hạn để nhận được phạm vi và các giới hạn ISMS – Phạm vi và các giới hạn của ISMS;

b) đầu ra từ Hoạt động 6.6 Phát triển chính sách ISMS và được ban quản lý phê chuẩn – Chính sách ISMS;

c) đầu ra từ Hoạt động 7.2 Xác định các yêu cầu an toàn thông tin cho quy trình ISMS;

d) đầu ra từ Hoạt động 7.3 Xác định các tài sản thuộc phạm vi ISMS;

e) đầu ra từ Hoạt động 7.4 Tiến hành đánh giá an toàn thông tin;

f) đầu ra từ Hoạt động 8.3 Chọn lựa mục tiêu và biện pháp quản lý;

g) đầu ra từ Hoạt động 8.4 Phê chuẩn cho triển khai và vận hành ISMS ;

h) TCVN ISO/IEC 27002:2011 (ISO/IEC 27002:2005).

Hướng dẫn

Trong hoạt động này, đối với từng biện pháp quản lý, nên lập thành tài liệu các thông tin sau, các thông tin này sẽ được đưa vào kế hoạch dự án ISMS:

a) tên người chịu trách nhiệm triển khai từng biện pháp quản lý;

b) độ ưu tiên của biện pháp quản lý sẽ được triển khai;

c) các nhiệm vụ hoặc hoạt động để triển khai các biện pháp quản lý;

d) thời gian triển khai biện pháp quản lý;

e) người được báo cáo về việc triển khai biện pháp quản lý ngay khi hoàn tất;

f) các nguồn lực để triển khai (nguồn nhân lực, các yêu cầu về nguồn lực, các yêu cầu về không gian, các chi phí).

Ban đầu, an toàn ICT và vật lý nên được thiết kế về mặt khái niệm. Nên quan tâm đến các vấn đề sau:

Các trách nhiệm thuộc quy trình triển khai ban đầu nhìn chung bao gồm:

a) đặc tả các mục tiêu của các biện pháp quản lý, có mô tả về trạng thái mong muốn dự kiến;

b) phân bổ các nguồn lực (khối lượng công việc, các nguồn tài chính);

c) đích thời gian thực tế để triển khai biện pháp quản lý;

d) các phương án tích hợp với an toàn ICT, vật lý và tổ chức.

Sau khi thiết kế khái niệm, nên hoàn thành thiết kế thực tế, ví dụ phát triển hệ thống để đạt được và triển khai thực tế tốt nhất đối với tổ chức. Nên quan tâm đến các vấn đề sau:

Các trách nhiệm thuộc quy trình triển khai thực tế bao gồm:

a) thiết kế từng biện pháp quản lý đã được lựa chọn cho các lĩnh vực ICT, vật lý và tổ chức theo mức vận hành của nơi áp dụng;

b) thuyết minh từng biện pháp quản lý theo thiết kế đã thống nhất;

c) đưa ra các thủ tục và thông tin về các biện pháp quản lý và các khóa đào tạo nâng cao nhận thức về an toàn thông tin;

d) cung cấp các hỗ trợ và triển khai các biện pháp quản lý tại nơi áp dụng;

Tùy thuộc vào loại biện pháp quản lý (ICT, vật lý hoặc tổ chức): có thể không nhất thiết và luôn phù hợp nếu phân định rõ ràng giữa phần ban đầu và phần chính thức của quy trình triển khai.

Việc triển khai các biện pháp quản lý luôn đòi hỏi sự phối hợp giữa nhiều cá nhân có vai trò khác nhau trong tổ chức. Do đó, ví dụ, những người có trách nhiệm đối với hệ thống sẽ được yêu cầu tìm kiếm, lắp đặt và duy trì các tiện ích kỹ thuật. Những cá nhân có các vai trò khác có thể lại thích hợp với việc xây dựng và lập tài liệu về các thủ tục sử dụng hệ thống.

An toàn thông tin nên được tích hợp trong các thủ tục và quy trình sử dụng rộng rãi trong tổ chức. Nếu điều đó khó triển khai đối với một bộ phận của tổ chức, hoặc một bên thứ ba thì các bên liên quan nên

trao đổi điều này ngay để thống nhất đưa ra cách giải quyết. Các giải pháp cho vấn đề này phải bao gồm thay đổi các thủ tục và quy trình, phân bổ lại các vai trò và trách nhiệm và sửa đổi các thủ tục kỹ thuật cho phù hợp.

Các kết quả của quá trình triển khai các biện pháp quản lý ISMS bao gồm:

a) kế hoạch triển khai, trong đó đưa ra quy trình triển khai các biện pháp quản lý một cách chi tiết, như thời gian biểu, cơ cấu của nhóm triển khai...

b) các hồ sơ và tài liệu về kết quả triển khai.

Đầu ra

Sản phẩm của hoạt động này là kế hoạch triển khai chi tiết và có cấu trúc các biện pháp quản lý an toàn ICT và vật lý, kế hoạch này sẽ được đưa vào kế hoạch dự án ISMS. Trong đó, đối với từng biện pháp quản lý phải bao gồm:

a) mô tả chi tiết;

b) các trách nhiệm về thiết kế và triển khai;

c) kế hoạch làm việc dự kiến;

d) các nhiệm vụ liên quan;

e) các nguồn lực được yêu cầu;

f) quyền sở hữu (các kênh báo cáo).

Thông tin khác

Không có thông tin đặc biệt nào khác.

9.4 Thiết kế an toàn thông tin ISMS cụ thể

9.4.1 Lập kế hoạch soát xét của ban quản lý

Hoạt động

Xây dựng kế hoạch để đảm bảo có sự tham gia và cam kết của ban quản lý về việc soát xét quá trình vận hành và những cải tiến liên tục của ISMS.

Đầu vào

a) đầu ra từ Hoạt động 6.5 Phối hợp phạm vi và các giới hạn để nhận được phạm vi và các giới hạn ISMS – Phạm vi và các giới hạn của ISMS;

b) đầu ra từ Hoạt động 6.6 Phát triển chính sách ISMS và được ban quản lý phê chuẩn – Chính sách ISMS;

c) đầu ra từ Hoạt động 8.4 Phê chuẩn cho triển khai và vận hành ISMS – Báo cáo về khả năng ứng dụng, gồm các mục tiêu quản lý và các biện pháp quản lý đã được chọn;

d) đầu ra từ Hoạt động 9.2.3 Thiết kế chính sách an toàn thông tin;

e) TCVN 10542:2014 (ISO/IEC 27004:2009).

Hướng dẫn

Soát xét các hoạt động ISMS của ban quản lý nên bắt đầu tại các giai đoạn đầu tiên khi đặc tả ISMS và xây dựng tình huống nghiệp vụ và tiếp tục với việc soát xét thường xuyên sự vận hành của ISMS. Sự tham gia sát sao này giúp thích ứng ISMS theo các yêu cầu nghiệp vụ và duy trì sự tuân thủ của nghiệp vụ theo ISMS.

Lập kế hoạch cho các soát xét của ban quản lý là xác định thời gian và phương thức để ban quản lý tiến hành các soát xét. Tham khảo thông tin chi tiết về các điều kiện tiên quyết đối với các soát xét của ban quản lý trong 7.2 của TCVN ISO/IEC 27001:2009 (ISO/IEC 27001:2005).

Để lập kế hoạch soát xét, cần cân nhắc xem những vai trò nào sẽ tham gia vào việc này. Việc lựa chọn các vai trò tham gia cũng nên được ban quản lý thông qua, và sau đó những người này nên được thông báo sớm nhất có thể. Cũng nên cung cấp cho ban quản lý đủ dữ liệu liên quan đến sự cần thiết và mục đích của quy trình soát xét này (xem Phụ lục B để có thông tin chi tiết về các vai trò và trách nhiệm).

Các soát xét của ban quản lý nên dựa trên các kết quả từ đo lường ISMS và các thông tin được thu thập trong quá trình vận hành của ISMS. Thông tin này sẽ được sử dụng cho các hoạt động quản lý ISMS để kiểm chứng tính hoàn thiện và hiệu lực của ISMS. Đầu vào và đầu ra yêu cầu cho soát xét ISMS có trong TCVN ISO/IEC 27001:2009 (ISO/IEC 27001:2005), và các thông tin chi tiết về các bài đo ISMS có trong TCVN 10542:2014 (ISO/IEC 27004:2009).

Cũng cần lưu ý rằng, nên thực hiện soát xét về phương pháp luận và các kết quả đánh giá rủi ro. Công việc này nên thực hiện tại các thời điểm như đã hoạch định, và lưu ý đến những thay đổi về môi trường, như việc tổ chức và công nghệ.

Nên hoàn thành việc lập kế hoạch đánh giá ISMS nội bộ để có thể thường xuyên đánh giá ISMS ngay khi nó được triển khai. Các kết quả đánh giá ISMS nội bộ là các đầu vào quan trọng của các soát xét ISMS của ban quản lý. Do vậy, nên lập kế hoạch đánh giá ISMS nội bộ trước khi các cuộc soát xét của ban quản lý được thực hiện. Đánh giá ISMS nội bộ nên cho thấy liệu các mục tiêu của các biện pháp quản lý, các biện pháp quản lý, các quy trình và thủ tục ISMS có được triển khai một cách hiệu lực, được duy trì và tuân thủ các yếu tố sau không:

a) các yêu cầu của TCVN ISO/IEC 27001:2009 (ISO/IEC 27001:2005);

b) các quy định và điều luật liên quan, và

c) các yêu cầu an toàn thông tin đã được xác định.

(Xem Phụ lục C để có thông tin chi tiết về lập kế hoạch đánh giá).

Điều kiện tiên quyết để tiến hành các soát xét của ban quản lý là phải có thông tin thu thập trên cơ sở ISMS đã được triển khai và vận hành. Thông tin được cung cấp cho ban soát xét có thể bao gồm:

a) các hồ sơ sự cố trong giai đoạn vận hành trước đây;

b) bằng chứng về hiệu lực của các biện pháp quản lý và sự không tuân thủ đã được xác định;

c) các kết quả của các cuộc kiểm tra thường xuyên khác (chi tiết hơn nếu các cuộc kiểm tra phát hiện thấy sự không tuân thủ chính sách);

d) các khuyến nghị cải tiến ISMS.

Kế hoạch giám sát nên chỉ ra các kết quả giám sát sẽ được lập hồ sơ và được báo cáo đến ban quản lý (xem thêm thông tin về giám sát trong Phụ lục E).

Đầu ra

Sản phẩm của hoạt động này là tài liệu tóm tắt kế hoạch cần cho việc soát xét của ban quản lý, trong đó đưa ra:

a) các đầu vào được yêu cầu để thực hiện việc soát xét của ban quản lý;

b) các thủ tục cho soát xét của ban quan lý về các khía cạnh đánh giá, giám sát và đo lường.

Thông tin khác

Phụ lục B – Các vai trò và trách nhiệm về an toàn thông tin.

Phụ lục C – Thông tin về đánh giá nội bộ.

Phụ lục E – Thông tin về thiết lập giám sát và đo lường.

9.4.2 Thiết kế chương trình giáo dục, đào tạo và nâng cao nhận thức về an toàn thông tin

Hoạt động

Phát triển chương trình giáo dục, đào tạo và nâng cao nhận thức về an toàn thông tin.

Đầu vào

a) đầu ra từ Hoạt động 6.5 Phối hợp phạm vi và các giới hạn để nhận được phạm vi và các giới hạn ISMS – Phạm vi và các giới hạn của ISMS;

b) đầu ra từ Hoạt động 6.6 Phát triển chính sách ISMS và được ban quản lý phê chuẩn – Chính sách ISMS;

c) đầu ra từ Hoạt động 7.2 Xác định các yêu cầu an toàn thông tin cho quy trình ISMS – Cụ thể là các yêu cầu của tổ chức về đào tạo và giáo dục an toàn thông tin;

d) đầu ra từ Hoạt động 8.3 Chọn lựa mục tiêu và biện pháp quản lý – Kế hoạch xử lý rủi ro;

e) đầu ra từ Hoạt động 8.4 Phê chuẩn cho triển khai và vận hành ISMS – Báo cáo về khả năng áp dụng, bao gồm mục tiêu của các biện pháp quản lý và các biện pháp quản lý được lựa chọn;

f) đầu ra từ Hoạt động 9.2.3 Thiết kế chính sách an toàn thông tin;

g) đầu ra từ Hoạt động 9.2.4 Phát triển các tiêu chuẩn và thủ tục an toàn thông tin;

h) tổng quan về chương trình đào tạo và giáo dục chung của tổ chức.

Hướng dẫn

Ban quản lý phải chịu trách nhiệm về công tác giáo dục và đào tạo để chắc chắn tất cả các cá nhân đã được giao trách nhiệm đều có năng lực thực hiện các nhiệm vụ được yêu cầu. Về lý tưởng thì nội dung giáo dục và đào tạo được thực hiện nên giúp tất cả mọi người nhận thức và hiểu được ý nghĩa và tầm quan trọng của các hoạt động an toàn thông tin mà họ tham gia, và cách thức mà họ có thể đóng góp vào việc đạt được các mục đích của ISMS.

Điều quan trọng tại thời điểm này là phải đảm bảo rằng mọi nhân viên thuộc phạm vi ISMS đều được đào tạo và/hoặc giáo dục đủ về an toàn thông tin. Với những tổ chức lớn, sẽ là không đủ nếu chỉ dùng một bộ tài liệu đào tạo chung cho toàn bộ tổ chức, vì trong đó sẽ chứa quá nhiều dữ liệu chỉ liên quan đến các loại công việc nhất định, và do vậy tài liệu sẽ có khối lượng quá lớn, phức tạp và khó sử dụng. Trong những trường hợp này, thường thì phải có nhiều bộ tài liệu đào tạo khác nhau được thiết kế cho từng nhóm lao động cụ thể, ví dụ cho những người làm văn phòng, đội ngũ IT hoặc lái xe, chúng được thiết kế phù hợp với nhu cầu riêng của từng nhóm.

Chương trình giáo dục, đào tạo và nâng cao nhận thức về an toàn thông tin nên đảm bảo các hồ sơ về đào tạo và giáo dục an toàn thông tin sẽ được lập ra. Các hồ sơ này nên được soát xét thường xuyên để chắc chắn mọi người đều được đào tạo theo nhu cầu. Nên có một người chịu trách nhiệm về việc này.

Các tài liệu đào tạo an toàn thông tin nên được thiết kế nằm trong nội dung các tài liệu đào tạo được tổ chức sử dụng khác, đặc biệt là các khóa đào tạo cho những người sử dụng các hệ thống IT. Lý tưởng nhất là việc đào tạo các vấn đề liên quan đến an toàn thông tin nên được đưa vào mọi khóa đào tạo cho những người sử dụng IT.

Tài liệu đào tạo an toàn thông tin tối thiểu nên chứa các thông tin sau:

a) các rủi ro và các mối đe dọa an toàn thông tin;

b) các khái niệm cơ bản về an toàn thông tin;

c) định nghĩa rõ về sự cố an toàn thông tin: hướng dẫn cách để xác định, xử lý và báo cáo một sự cố an toàn thông tin;

d) chính sách, các tiêu chuẩn và thủ tục an toàn thông tin của tổ chức;

e) các trách nhiệm và các kênh báo cáo về an toàn thông tin trong tổ chức;

f) hướng dẫn cách hỗ trợ cải thiện an toàn thông tin;

g) hướng dẫn về các sự cố an toàn thông tin và lập hồ sơ;

h) địa chỉ để có thêm thông tin.

Nhóm đào tạo an toàn thông tin nên được xác định với các nhiệm vụ sau:

a) xây dựng và quản lý các hồ sơ đào tạo;

b) xây dựng và quản lý các tài liệu đào tạo;

c) thực hiện đào tạo.

Các nhiệm vụ này có thể được phân bổ cho đội ngũ đạo tạo hiện có trong tổ chức. Tuy nhiên, nhóm đạo tạo hiện có này có thể yêu cầu phải được đào tạo thêm về các khái niệm an toàn thông tin để đảm bảo rằng chúng sẽ được trình bày hiệu quả và chính xác.

Chương trình giáo dục, đào tạo và nâng cao nhận thức về an toàn thông tin nên đưa ra thủ tục để đảm bảo rằng các tài liệu đào tạo được soát xét và cập nhật thường xuyên. Nên giao cho một cá nhân trách nhiệm cụ thể về soát xét và cập nhật các tài liệu đào tạo.

Đầu ra

Sản phẩm của hoạt động này gồm:

a) các tài liệu giáo dục, đào tạo và nâng cao nhận thức về an toàn thông tin;

b) đội ngũ thực hiện giáo dục, đào tạo và nâng cao nhận thức về an toàn thông tin, bao gồm các vai trò và trách nhiệm;

c) các kế hoạch giáo dục, đào tạo và nâng cao nhận thức về an toàn thông tin;

d) các hồ sơ thực tế thể hiện các kết quả của công tác giáo dục, đào tạo và nâng cao nhận thức về an toàn thông tin cho các nhân viên.

Thông tin khác

Không có thông tin đặc biệt nào khác.

9.5 Đưa ra kế hoạch dự án ISMS chính thức

Hoạt động

Hoàn thành kế hoạch dự án ISMS, bao gồm các hoạt động cần để triển khai các biện pháp quản lý được lựa chọn.

Đầu vào

a) đầu ra từ Hoạt động 6.5 Phối hợp phạm vi và các giới hạn để nhận được phạm vi và các giới hạn ISMS – Phạm vi và các giới hạn của ISMS;

b) đầu ra từ Hoạt động 6.6 Phát triển chính sách ISMS và được ban quản lý phê chuẩn – Chính sách ISMS;

c) đầu ra từ Hoạt động 9.2 Thiết kế an toàn thông tin về tổ chức;

d) đầu ra từ Hoạt động 9.3 Thiết kế an toàn thông tin vật lý và ICT;

e) đầu ra từ Hoạt động 9.4 Thiết kế an toàn thông tin ISMS;

f) TCVN ISO/IEC 27002:2011 (ISO/IEC 27002:2005).

Hướng dẫn

Các hoạt động được yêu cầu để triển khai các biện pháp quản lý đã chọn và thực hiện các hoạt động có liên quan đến ISMS khác nên được chính thức hóa trong một kế hoạch triển khai chi tiết trong bản dự án ISMS chính thức. Kế hoạch triển khai chi tiết có thể còn được hỗ trợ bằng các mô tả về công cụ và phương pháp triển khai đề xuất. Vì một dự án ISMS có sự tham gia của nhiều vai trò khác nhau trong tổ chức nên điều quan trọng là các hoạt động này phải được phân bổ rõ ràng cho các bên chịu trách nhiệm, và kế hoạch phải được trao đổi sớm trong cả dự án và trên toàn bộ tổ chức.

Giống như với tất cả các dự án khác, điều quan trọng là người chịu trách nhiệm về dự án phải đảm bảo phân bổ đủ nguồn lực cho dự án.

Đầu ra

Sản phẩm của hoạt động này là kế hoạch triển khai dự án ISMS chính thức.

Thông tin khác

Không có thông tin đặc biệt nào khác.

Phụ lục A

(Tham khảo)

Danh sách các hoạt động

Mục đích:

- đưa ra một danh sách các hoạt động được yêu cầu để thiết lập và triển khai ISMS,
- hỗ trợ giám sát tiến trình triển khai ISMS,
- đối chiếu các hoạt động triển khai ISMS liên quan với các yêu cầu tương ứng của TCVN ISO/IEC 27001:2009 (ISO/IEC 27001:2005).

Giai đoạn triển khai TCVN 10541:2014	Số bước	Hoạt động	Bước tiên quyết	Tài liệu đầu ra	Đối chiếu với TCVN ISO/IEC 27001:2009 (ISO/IEC 27001:2005)
5 Phê chuẩn cho khởi động dự án ISMS	1.	Thu thập các mục tiêu nghiệp vụ của tổ chức	Không có	Danh sách các mục tiêu nghiệp vụ của tổ chức	N/A
	2.	Thu thập hiểu biết về các hệ thống quản lý hiện hành	Không có	Mô tả về các hệ thống quản lý hiện hành	N/A
	3.	5.2 Xác định các mục tiêu, nhu cầu an toàn thông tin, các yêu cầu nghiệp vụ đối với ISMS	1, 2	Tóm tắt các mục tiêu, nhu cầu an toàn thông tin, các yêu cầu nghiệp vụ đối với ISMS	N/A
	4.	Thu thập các quy định, tuân thủ, và tiêu chuẩn theo ngành nghề áp dụng cho tổ chức	Không có	Tóm tắt các quy định, tuân thủ và yêu cầu theo ngành nghề áp dụng cho tổ chức	N/A
	5.	5.3 Xác định phạm vi ISMS sơ bộ	3, 4	Mô tả phạm vi ISMS sơ bộ (5.3.1)	N/A
				Định nghĩa các vai trò	N/A

Giai đoạn triển khai TCVN 10541:2014	Số bước	Hoạt động	Bước tiên quyết	Tài liệu đầu ra	Đối chiếu với TCVN ISO/IEC 27001:2009 (ISO/IEC 27001:2005)
				và trách nhiệm đối với ISMS (5.3.2)	
	6.	5.4 Xây dựng tình huống nghiệp vụ và kế hoạch dự án trình ban quản lý phê	5	Tình huống nghiệp vụ và kế hoạch dự án đề xuất	N/A
	7.	Được ban quản lý phê chuẩn và cam kết khởi động dự án triển khai ISMS	6	Phê chuẩn của ban quản lý cho khởi động dự án triển khai ISMS	N/A
6 Xác định phạm vi, các giới hạn và chính sách ISMS	8.	6.2 Xác định phạm vi và các giới hạn về tổ chức	7	• Mô tả các giới hạn về tổ chức • Cấu trúc và chức năng của tổ chức • Thông tin trao đổi trong các giới hạn • Các quy trình nghiệp vụ và trách nhiệm đối với các tài sản thông tin trong và ngoài phạm vi ISMS	4.2.1.a)
	9.	6.3 Xác định phạm vi và các giới hạn về công nghệ thông tin và truyền thông (ICT)	7	• Mô tả các giới hạn ICT • Mô tả các hệ thống thông tin và mạng viễn thông trong và ngoài phạm vi ISMS	4.2.1.a)

Giai đoạn triển khai TCVN 10541:2014	Số bước	Hoạt động	Bước tiên quyết	Tài liệu đầu ra	Đối chiếu với TCVN ISO/IEC 27001:2009 (ISO/IEC 27001:2005)
	10.	6.4 Xác định phạm vi và các giới hạn vật lý	7	• Mô tả các giới hạn vật lý ISMS • Mô tả đặc điểm của tổ chức và các địa điểm thuộc trong và ngoài phạm vi ISMS	4.2.1.a)
	11.	6.5 Phối hợp phạm vi và các giới hạn để nhận được phạm vi và các giới hạn ISMS	8, 9, 10	Tài liệu mô tả phạm vi và các giới hạn của ISMS	4.2.1.a)
	12.	6.6 Phát triển chính sách ISMS và được ban quản lý phê chuẩn	11	Chính sách ISMS đã được ban quản lý phê chuẩn	4.2.1.b)
7 Tiến hành phân tích các yêu cầu an toàn thông tin	13.	7.2 Xác định các yêu cầu an toàn thông tin cho quy trình ISMS	12	Danh sách các quy trình chính, các chức năng, vị trí, các hệ thống thông tin, các mạng truyền thông	N/A
				Các yêu cầu của tổ chức về bí mật, tính sẵn sàng và toàn vẹn	N/A
				Các yêu cầu của tổ chức theo hợp pháp, quy định và hợp đồng và các yêu cầu an toàn thông tin nghiệp vụ	4.2.1.c) 1)

Giai đoạn triển khai TCVN 10541:2014	Số bước	Hoạt động	Bước tiên quyết	Tài liệu đầu ra	Đối chiếu với TCVN ISO/IEC 27001:2009 (ISO/IEC 27001:2005)
				Danh sách các điểm yếu đã được xác định của tổ chức	4.2.1.d) 3)
	14.	7.3 Xác định các tài sản thuộc phạm vi ISMS	13	Mô tả các quy trình chính của tổ chức	N/A
				Định danh các tài sản thông tin của các quy trình chính	4.2.1.d)1)
				Phân loại các quy trình/tài sản trọng yếu	N/A
	15.	7.4 Tiến hành đánh giá an toàn thông tin	14	• Tài liệu về tình trạng và đánh giá hiện trạng an toàn thông tin của tổ chức, bao gồm cả các biện pháp quản lý an toàn thông tin hiện hành • Tài liệu về các thiếu sót đã được ước lượng và đánh giá của tổ chức	4.2.1.e)2)
8 Tiến hành đánh giá rủi ro và lập kế hoạch xử lý rủi ro	16.	8.2 Tiến hành đánh giá rủi ro	15	• Phạm vi của đánh giá rủi ro • Phương pháp đánh giá rủi ro đã được chấp thuận, cùng với bối cảnh quản lý	4.2.1.c)1)

Giai đoạn triển khai TCVN 10541:2014	Số bước	Hoạt động	Bước tiên quyết	Tài liệu đầu ra	Đối chiếu với TCVN ISO/IEC 27001:2009 (ISO/IEC 27001:2005)
				rủi ro chiến lược của tổ chức • Chỉ tiêu chấp nhận rủi ro	
	17.	8.3 Chọn lựa mục tiêu và biện pháp quản lý	16	Tài liệu đánh giá rủi ro mức cao	4.2.1.e)3)
				Xác định nhu cầu đánh giá rủi ro chuyên sâu	N/A
				Tài liệu đánh giá rủi ro chuyên sâu	4.2.1.e)3)
				Các kết quả đánh giá rủi ro được thu thập	N/A
	18.	8.4 Phê chuẩn cho triển khai và vận hành ISMS	17	Các rủi ro và các phương án xử lý rủi ro đã được xác định	4.2.1.f)
				Các mục tiêu quản lý và biện pháp quản lý được chọn để giảm rủi ro	4.2.1.g)
	19.	Ban quản lý phê chuẩn các rủi ro tồn đọng	18	Phê chuẩn bằng văn bản của ban quản lý về các rủi ro tồn đọng đề xuất (đầu ra của 8.4)	4.2.1.h)
	20.	Ban quản lý phê chuẩn	19	Sự phê chuẩn cho	4.2.1.i)

Giai đoạn triển khai TCVN 10541:2014	Số bước	Hoạt động	Bước tiên quyết	Tài liệu đầu ra	Đối chiếu với TCVN ISO/IEC 27001:2009 (ISO/IEC 27001:2005)
		cho triển khai và vận hành ISMS		triển khai và vận hành ISMS bằng văn bản của ban quản lý (đầu ra của 8.4)	
	21.	Chuẩn bị thông báo áp dụng	18	Báo cáo áp dụng	4.2.1.j)
9 Thiết kế ISMS	22.	9.2 Thiết kế an toàn thông tin về tổ chức	20	Cơ cấu tổ chức, và các vai trò và trách nhiệm liên quan đến an toàn thông tin về tổ chức	5.1.c)
				• Định danh hệ thống tài liệu liên quan đến ISMS • Các mẫu hồ sơ ISMS, các hướng dẫn sử dụng và lưu trữ	4.3
				Tài liệu chính sách an toàn thông tin	ISO/IEC 27002; 5.1.1
				Điểm mốc của các thủ tục và chính sách an toàn thông tin (và nếu có thể thì cả các kế hoạch phát triển các chính sách, thủ tục cụ thể...)	

Giai đoạn triển khai TCVN 10541:2014	Số bước	Hoạt động	Bước tiên quyết	Tài liệu đầu ra	Đối chiếu với TCVN ISO/IEC 27001:2009 (ISO/IEC 27001:2005)
	23.	9.3 Thiết kế an toàn thông tin vật lý và ICT	20, 21	Kế hoạch triển khai các biện pháp quản lý an toàn thông tin vật lý và ICT	4.2.2.c)
	24.	9.4 Thiết kế an toàn thông tin ISMS cụ thể	22, 23	Các thủ tục về lập hồ sơ và các quy trình soát xét của ban quản lý	7.1
	25.			Các mô tả về hoạt động đánh giá, giám sát và đo lường	4.2.3.a); 4.2.3.b); 6
	26.			Chương trình giáo dục, đào tạo và nâng cao nhận thức về an toàn thông tin	5.2.2
	27.	9.5 Đưa ra kế hoạch dự án ISMS chính thức	25	Kế hoạch dự án triển khai được ban quản lý phê chuẩn về các quy trình triển khai	N/A
	28.	Kế hoạch dự án ISMS chính thức	28	Kế hoạch triển khai dự án ISMS cụ thể, bao gồm việc thực hiện các hoạt động đã được hoạch định về an toàn thông tin vật lý, ICT và tổ chức cùng các yêu cầu ISMS cụ thể về việc	

Giai đoạn triển khai TCVN 10541:2014	Số bước	Hoạt động	Bước tiên quyết	Tài liệu đầu ra	Đối chiếu với TCVN ISO/IEC 27001:2009 (ISO/IEC 27001:2005)
				triển khai ISMS theo các kết quả của các hoạt động được đề cập trong TCVN 10541:2014.	

Phụ lục B

(Tham khảo)

Các vai trò và trách nhiệm về an toàn thông tin

Phụ lục này đưa ra các hướng dẫn bổ sung về vai trò và trách nhiệm liên quan đến an toàn thông tin trong một tổ chức. Ban đầu, các vai trò sẽ được đề cập trên quan điểm tổ chức để triển khai ISMS. Sau đó, sẽ đưa ra một bảng tổng hợp thông tin và cung cấp các ví dụ chung về các vai trò và trách nhiệm.

1 Vai trò của ban an toàn thông tin

Ban an toàn thông tin nên có vai trò lớn nhất đối với ISMS trong mỗt tổ chức. Ban an toàn thông tin nên chịu trách nhiệm xử lý các tài sản thông tin của tổ chức, và nên có đủ hiểu biết về an toàn thông tin để chỉ đạo, giám sát, và hoàn thành các nhiệm vụ cần thiết.

Dưới đây là những ví dụ cụ thể về vai trò của ban an toàn thông tin:

a) quản lý rủi ro, xây dựng kế hoạch về các tài liệu ISMS, chịu trách nhiệm xác định nội dung của các tài liệu này và yêu cầu sự chấp thuận từ ban quản lý;

b) lập kế hoạch mua trang thiết bị mới và/ hoặc quyết định về việc tái sử dụng các thiết bị hiện có của tổ chức;

c) xử lý các vấn đề có thể phát sinh;

d) xem xét các cải tiến xuất hiện từ việc triển khai và đo lường tiếp theo của ISMS;

e) đưa ra định hướng chiến lược cho ISMS (cả trong quá trình triển khai dự án và vận hành ISMS), và

f) làm cầu nối giữa quản lý cấp cao và nhóm dự án triển khai và các cá nhân quản lý an toàn thông tin.

2 Vai trò của nhóm lập kế hoạch an toàn thông tin

Nhóm chịu trách nhiệm về ISMS trong giai đoạn lập kế hoạch dự án này nên gồm các thành viên có hiểu biết rộng về các tài sản thông tin quan trọng thuộc phạm vi ISMS, và có đủ kiến thức để cân nhắc cách xử lý các thông tin loại này. Ví dụ, khi quyết định cách thức xử lý các tài sản thông tin, có thể sẽ có nhiều quan điểm khác nhau giữa các phòng ban thuộc phạm vi ISMS, vì vậy có thể cần phải điều chỉnh các tác động tích cực và tiêu cực của dự án. Nhóm này được yêu cầu hoạt động như một bộ phận điều phối các xung đột qua các giới hạn phòng ban. Để thực hiện công việc này, các thành viên cần có các kỹ năng giao tiếp được hình thành trên cơ sở kinh nghiệm và các năng lực phối hợp của họ, cũng như kiến thức sâu sắc về an toàn thông tin.

3 Các chuyên gia và tư vấn viên bên ngoài

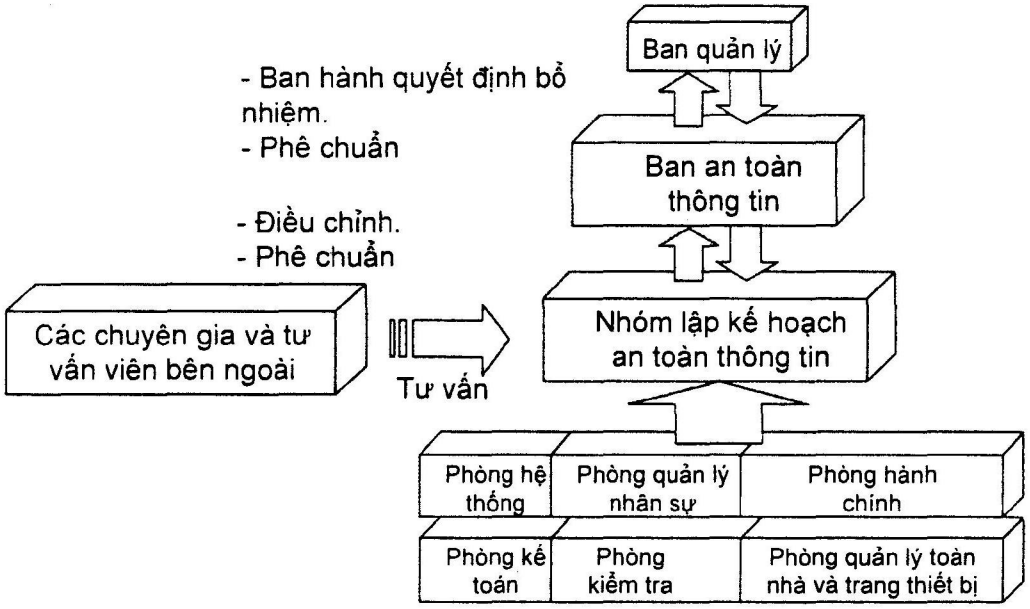
Mỗi tổ chức có thể lựa chọn thành viên thực hiện các nhiệm vụ trên (nếu có thể, mỗi thành viên sẽ thực hiện một vai trò) trước khi thiết lập ISMS. Tuy nhiên, các thành viên đều phải có kiến thức và kinh nghiệm sâu rộng về lĩnh vực an toàn thông tin như "công nghệ thông tin", "các quyết định về quản trị" và "có hiểu biết về tổ chức". Mỗi người chịu trách nhiệm về các công việc nhất định trong tổ chức đều có thể có hiểu biết tốt nhất về lĩnh vực chuyên môn của họ. Rất nhiều chuyên viên là các chuyên gia trong các lĩnh vực cụ thể ở tổ chức của họ nên được tham khảo ý kiến về ISMS vì ISMS cũng được sử dụng trong những linh vực riêng của họ. Cũng cần có sự cân đối giữa yêu cầu về chuyên môn và kiến thức rộng để đáp ứng các mục tiêu của tổ chức. Các tư vấn viên bên ngoài có thể đưa ra những gợi ý dựa trên quan điểm vĩ mô của họ về tổ chức và kinh nghiệm từ các tình huống tương tự, mặc dù họ thường không nhất thiết phải có kiến thức sâu về các đặc trưng của tổ chức và những chi tiết về hoạt động của một tổ chức. Các thuật ngữ được sử dụng ở các ví dụ trên, ví dụ Ban an toàn thông tin và Nhóm Lập kế hoạch an toàn thông tin, hoàn toàn không phải là vấn đề quan trọng. Nhưng chức năng của mỗi bộ phận này nên được hiểu rõ. Lý tưởng nhất là các cấu trúc nội bộ nên phối hợp an toàn thông tin, trao đổi và làm việc gần gũi với từng phòng kỹ thuật.

4 Người sở hữu tài sản thông tin

Nên chỉ định mỗi các nhân sở hữu từng quy trình và ứng dụng chuyên môn của tổ chức; người này đóng vai trò là "chủ sở hữu tài sản thông tin" đối với tất cả các vấn đề về an toàn thông tin liên quan đến dữ liệu xử lý trong từng quy trình cụ thể. Đầu mối liên lạc hoặc người sở hữu quy trình phải chịu trách nhiệm, ví dụ, đối với các nhiệm vụ được giao phó và thông tin xử lý trong các quy trình mà họ đã được chỉ định.

Trong trường hợp chia sẻ rủi ro, phòng tránh rủi ro và ngăn chặn rủi ro, nên thực hiện các hành động cần thiết trên các khía cạnh an toàn về tổ chức. Nếu đã quyết định chuyển giao rủi ro thì nên tiến hành các hành động phù hợp sử dụng các hợp đồng, hợp đồng bảo hiểm và cơ cấu tổ chức ví dụ quan hệ đối tác và liên doanh.

Hình B.1 đưa ra một ví dụ về cơ cấu tổ chức để thiết lập ISMS. Các vai trò và trách nhiệm chính trong tổ chức cũng được đưa ra cho ví dụ này.



Hình B.1 – Ví dụ về cơ cấu tổ chức để thiết lập ISMS

Tương tác với tổ chức

Tất cả các bên tham gia đều nên soát xét và quen thuộc với các yêu cầu bảo vệ tài sản của tổ chức. Các bên tham gia vào việc phân tích về tổ chức nên gồm những người có kiến thức cao về tổ chức và môi trường hoạt động của tổ chức. Những người này nên được lựa chọn từ nhiều bộ phận trong tổ chức và gồm:

a) quản lý cấp cao (ví dụ: COO và CFO);

b) các thành viên Ban an toàn thông tin;

c) các thành viên nhóm lập kế hoạch an toàn thông tin;

d) những người quản lý chuyên môn (ví dụ: trưởng các phòng ban trong tổ chức);

e) người sở hữu các quy trình (tức là người đại diện cho các khu vực vận hành quan trọng);

f) các chuyên gia và các tư vấn viên bên ngoài.

Các ví dụ về vai trò và trách nhiệm chung đối với an toàn thông tin

An toàn thông tin có ảnh hưởng rộng lớn đến toàn bộ tổ chức. Do vậy, việc xác định rõ các trách nhiệm đối với an toàn thông tin là vô cùng quan trọng quyết định sự triển khai thành công. Vì có rất nhiều vai trò và trách nhiệm liên quan đến an toàn thông tin nên sự hiểu rõ về các vai trò khác nhau sẽ là nền tảng để có thể hiểu được một số hoạt động sẽ được mô tả tiếp theo trong tiêu chuẩn này. Bảng dưới đây sẽ đưa ra các vai trò và trách nhiệm về an toàn thông tin. Cần lưu ý rằng, các thông tin về các vai trò được nêu ra chỉ là có ý nghĩa chung, các triển khai ISMS cụ thể sẽ có những mô tả cụ thể.

Bảng B.1 – Danh sách các ví dụ về các vai trò và trách nhiệm đối với an toàn thông tin

Vai trò	Mô tả tóm tắt trách nhiệm
Quản lý cấp cao (COO, CEO, CSO và CFO)	đưa ra tầm nhìn, các quyết định chiến lược và điều phối hoạt động để định hướng và quản lý tổ chức
Quản lý chuyên môn	chịu trách nhiệm cao nhất về các chức năng tổ chức
Giám đốc an toàn thông tin	chịu trách nhiệm chung và quản lý về an toàn thông tin nhằm đảm bảo xử lý đúng các tài sản thông tin
Ban an toàn thông tin (các thành viên)	xử lý các tài sản thông tin và có vai trò cao nhất về ISMS trong tổ chức
Nhóm lập kế hoạch an toàn thông tin (các thành viên)	chịu trách nhiệm trong suốt quá trình thiết lập hệ thống ISMS. Nhóm này làm việc với các phòng ban và giải quyết các vướng mắc, chồng chéo cho đến khi hệ thống ISMS đã được thiết lập.
Các bên liên quan	theo quan điểm mô tả các vai trò khác về an toàn thông tin, các bên liên quan về cơ bản được xác định ở đây là các cá nhân/ tổ chức nằm ngoài hoạt động thông thường của tổ chức - chẳng hạn như hội đồng quản trị, chủ sở hữu (cả những người nắm giữ về mặt tổ chức nếu tổ chức là bộ phận của một nhóm hoặc một tổ chức chính phủ, và/hoặc những người nắm giữ trực tiếp ví dụ các bên liên quan trong một tổ chức cá thể). Ngoài ra, các bên liên quan có thể là các công ty có nhiều chi nhánh, khách hàng, nhà cung cấp hoặc các tổ chức công như cơ quan kiểm soát tài chính của chính phủ hoặc sàn chứng khoán.
Quản trị hệ thống	người chịu trách nhiệm quản trị hệ thống IT
Giám đốc IT	người quản lý tất cả các nguồn lực IT (ví dụ, trưởng phòng IT)
An toàn vật lý	người chịu trách nhiệm về an toàn vật lý, ví dụ trụ sở... thường được gọi là Người quản lý trang thiết bị
Quản lý rủi ro	cá nhân/các cá nhân chịu trách nhiệm về khung quản lý rủi ro của tổ chức, bao gồm ước lượng rủi ro, xử lý rủi ro và giám sát rủi ro.
Cố vấn pháp lý	chịu trách nhiệm về các khía cạnh pháp lý của các rủi ro an toàn thông tin.
Nguồn nhân lực	Cá nhân/các cá nhân có trách nhiệm chung về đội ngũ lao động.

Vai trò	Mô tả tóm tắt trách nhiệm
Lưu trữ tài liệu	Tất cả các tổ chức đều có các tài liệu lưu trữ chứa các thông tin quan trọng cần được giữ lại trong thời gian dài. Các thông tin này có thể được lưu trữ trong các phương tiện khác nhau và phải có một người nào đó phải chịu trách nhiệm đảm bảo an toàn cho các tài liệu lưu trữ này.
Dữ liệu cá nhân	Nếu có quy định của luật pháp quốc gia thì có thể cần có một người chịu trách nhiệm liên lạc với ban thanh tra dữ liệu, hoặc các cơ quan tương tự có chức năng giám sát các vấn đề về tính cá nhân và tính toàn vẹn.
Nhân viên phát triển hệ thống	Nếu tổ chức phát triển các hệ thống thông tin riêng thì phải có người chịu trách nhiệm cho việc phát triển này.
Chuyên viên/ Chuyên gia	Các chuyên viên và chuyên gia chịu trách nhiệm về các công việc nào đó trong tổ chức phải được tham khảo ý kiến về khía cạnh về ISMS liên quan đến lĩnh vực của họ vì điều đó có liên quan đến việc sử dụng ISMS trong các lĩnh vực riêng của họ.
Tư vấn viên bên ngoài	Các tư vấn viên bên ngoài có thể được ra các gợi ý dựa trên quan điểm vĩ mô của họ về tổ chức và các kinh nghiệm công nghiệp. Tuy nhiên, các tư vấn viên có thể không có các kiến thức chuyên sâu về tổ chức và các nghiệp vụ của tổ chức.
Nhân viên/đội ngũ lao động/người sử dụng	Mỗi nhân viên đều có trách nhiệm như nhau về duy trì an toàn thông tin tại nơi làm việc và trong phạm vi môi trường của họ.
Đánh giá viên	Đánh giá viên có trách nhiệm ước lượng và đánh giá ISMS.
Đào tạo viên	Đào tạo viên có trách nhiệm triển khai các chương trình đào tạo và nâng cao nhận thức về an toàn thông tin.
Người chịu trách nhiệm về IT hoặc IS nội bộ	Trong các tổ chức lớn, thường có một người thuộc nội bộ tổ chức phải chịu trách nhiệm nội bộ về các vấn đề IT, và có thể cả đối với sự an toàn thông tin.
Đại sứ (người có tầm ảnh hưởng)	Đây không phải là một vai trò trách nhiệm cụ thể, tuy nhiên trong các tổ chức lớn, giai đoạn triển khai có thể phải có sự giúp đỡ to lớn từ những người có kiến thức sâu về việc triển khai ISMS. Họ có thể hỗ trợ kiến thức và đưa ra các lý do triển khai ISMS. Họ có thể có ảnh hưởng đến quan điểm về đường hướng triển khai và có thể được coi là các "đại sứ".

Phụ lục C

(Tham khảo)

Thông tin về đánh giá nội bộ

Phụ lục này đưa ra hướng dẫn bổ sung hỗ trợ lập kế hoạch đánh giá.

Triển khai ISMS phải được đánh giá thường xuyên bằng các hình thức đánh giá nội bộ và độc lập. Các cuộc đánh giá này cũng phục vụ mục đích đối chiếu và đánh giá những các hoạt động đã triển khai trên thực tế. Để triển khai ISMS, phải hoạch định các hình thức đánh giá ISMS.

Trong mỗi cuộc đánh giá ISMS, các kết quả đánh giá nên được xác định dựa trên bằng chứng. Vì vậy, nên ấn định khoảng thời gian phù hợp trong quá trình vận hành ISMS để thu thập được bằng chứng phù hợp.

Đánh giá ISMS nội bộ phải được triển khai và thực hiện thường xuyên để đánh giá xem các mục tiêu quản lý, biện pháp quản lý, các quy trình và thủ tục ISMS có tuân thủ các yêu cầu của tiêu chuẩn TCVN ISO/IEC 27001:2009 (ISO/IEC 27001:2005) và các quy định hoặc điều luật liên quan không, có tuân thủ các yêu cầu an toàn thông tin đã xác định không, và có được triển khai và duy trì một cách hiệu lực không.

Tuy nhiên, các tổ chức có quy mô nhỏ có thể sẽ gặp khó khăn khi lựa chọn các đánh giá viên ISMS nội bộ. Nếu tổ chức không có đủ nguồn lực nội bộ có đủ kinh nghiệm để thực hiện các kiểm tra thì có thể sử dụng các chuyên gia bên ngoài. Khi tổ chức sử dụng đánh giá viên bên ngoài, nên xem xét xem các đánh giá viên bên ngoài có phải là những người thành thạo về đánh giá ISMS nội bộ không; tuy nhiên, họ có thể không có đủ kiến thức về môi trường tổ chức của tổ chức. Thông tin này phải được cung cấp bởi đội ngũ nội bộ. Ngoài ra, các đánh giá viên nội bộ có thể có khả năng thực hiện các đánh giá chi tiết về môi trường tổ chức của tổ chức, nhưng có thể lại không đủ kiến thức về việc thực hiện các cuộc đánh giá ISMS. Các tổ chức phải thấy được những đặc điểm và các khuyết điểm tiềm tàng của các đánh giá viên nội bộ so với các đánh giá viên bên ngoài thực hiện đánh giá ISMS nội bộ.

Hiệu lực và hiệu quả của các biện pháp quản lý được triển khai (xem TCVN 10542:2014 (ISO/IEC 27004:2009)) phải được đánh giá trong phạm vi của các cuộc đánh giá nội bộ.

Điều quan trọng là các cá nhân đã tham gia lập kế hoạch và thiết kế các mục tiêu an toàn thông tin không được tham gia đánh giá nội bộ, bởi vì sẽ khó khăn để tìm ra lỗi của chính mình. Vì vậy, các đơn vị hoặc cá nhân của tổ chức nằm ngoài phạm vi của các đánh giá ISMS nội bộ phải được ban quản lý chọn làm đánh giá viên. Các đánh giá viên nên lập kế hoạch, thực hiện, lập báo cáo và tiếp tục thực hiện các cuộc đánh giá ISMS nội bộ để có được cam kết của người quản lý. Tùy thuộc vào quy mô của tổ chức, có thể thuê đánh giá viên bên ngoài để tránh tình trạng các đánh giá viên nội bộ làm việc phiến diện.

Khi thực hiện đánh giá ISMS nội bộ, nên đánh giá xem ISMS có được vận hành một cách hiệu lực và được duy trì như kỳ vọng không. Các đánh giá viên phải xem xét tình trạng và tầm quan trọng của các mục tiêu quản lý, biện pháp quản lý, các quy trình và thủ tục được đánh giá, và kết quả của các cuộc đánh giá trước đó khi lên kế hoạch cho chương trình đánh giá.

Khi thực hiện đánh giá, phải lập tài liệu các chỉ tiêu, phạm vi áp dụng, tần suất và phương pháp đánh giá.

Tính khách quan và công bằng của quy trình đánh giá phải được đảm bảo khi lựa chọn đánh giá viên. Mỗi đánh giá viên yêu cầu phải có các năng lực sau khi thực hiện các quy trình đánh giá:

a) lập kế hoạch và thực hiện đánh giá;

b) lập báo cáo kết quả;

c) đề xuất hành động khắc phục và phòng ngừa,...

Ngoài ra, tổ chức cũng phải xác định trách nhiệm của đánh giá viên và danh sách các quy trình đánh giá trong các tài liệu thủ tục kiểm tra.

Mỗi người quản lý chịu trách nhiệm về một quy trình được đánh giá nên đảm bảo rằng những vấn đề không tuân thủ và các nguyên nhân của chúng đều được làm sáng tỏ ngay. Tuy nhiên, điều đó không có nghĩa là sự không tuân thủ nhất thiết phải được giải quyết ngay lập tức. Hơn nữa, các hành động khắc phục được thi hành đều phải được thẩm tra và có báo cáo về kết quả thẩm tra.

Trên quan điểm quản trị, đánh giá ISMS nội bộ có thể được thực hiện có hiệu lực nếu thuộc hoặc được kết hợp với các đánh giá nội bộ khác của tổ chức. Khi thực hiện các đánh giá nội bộ, cần tham khảo tại ISO/IEC 27006:2007 "Các yêu cầu đối với các tổ chức đánh giá và cấp chứng nhận ISMS".

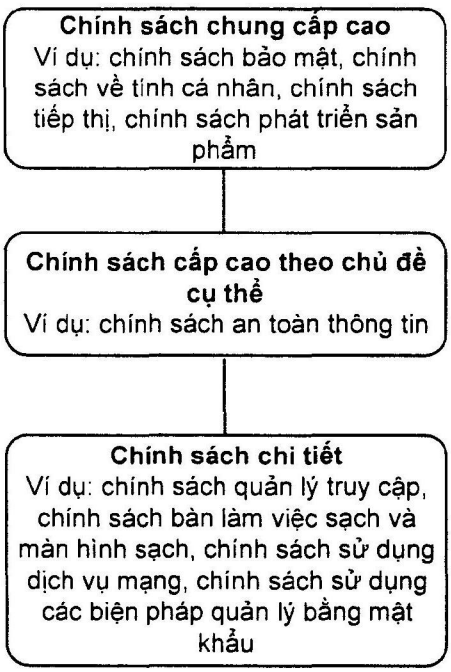
Phụ lục D

(Tham khảo)

Cấu trúc của các chính sách

Phụ lục này đưa ra hướng dẫn bổ sung về cấu trúc của các chính sách, bao gồm cả các chính sách an toàn thông tin.

Nhìn chung, chính sách là một tuyên bố của ban quản lý về mục đích và định hướng tổng thể (xem FCD 27000 và TCVN ISO/IEC 27002:2011 (ISO/IEC 27002:2005)). Nội dung của mỗi chính sách hướng dẫn các hành động và quyết định liên quan đến chủ đề của chính sách. Mỗi tổ chức có thể đưa ra nhiều chính sách; mỗi chính sách tập trung một lĩnh vực hoạt động quan trọng của tổ chức. Bên cạnh một số chính sách độc lập với nhau thì lại có các chính sách có mối quan hệ phân cấp. Về khía cạnh an toàn thì các chính sách thường được tổ chức theo phân cấp. Thông thường, chính sách an toàn của tổ chức là chính sách ở cấp cao nhất. Chính sách này được hỗ trợ bởi các chính sách cụ thể hơn, bao gồm cả các chính sách an toàn thông tin và chính sách hệ thống quản lý an toàn thông tin. Như vậy, chính sách an toàn thông tin có thể được hỗ trợ bởi các chính sách cụ thể hơn về các vấn đề liên quan đến các khía cạnh an toàn thông tin. Rất nhiều chính sách đã được đưa ra trong tiêu chuẩn ISO/IEC 27002:2011 (ISO/IEC 27002:2005), ví dụ như các chính sách an toàn thông tin liên quan đến kiểm soát truy cập, màn hình sạch và bàn làm việc sạch, sử dụng dịch vụ mạng, sử dụng các biện pháp quản lý mật khẩu. Trong một số trường hợp có thể bổ sung thêm các phân cấp chính sách khác. Hình dưới là một ví dụ về một kiểu phân cấp chính sách.



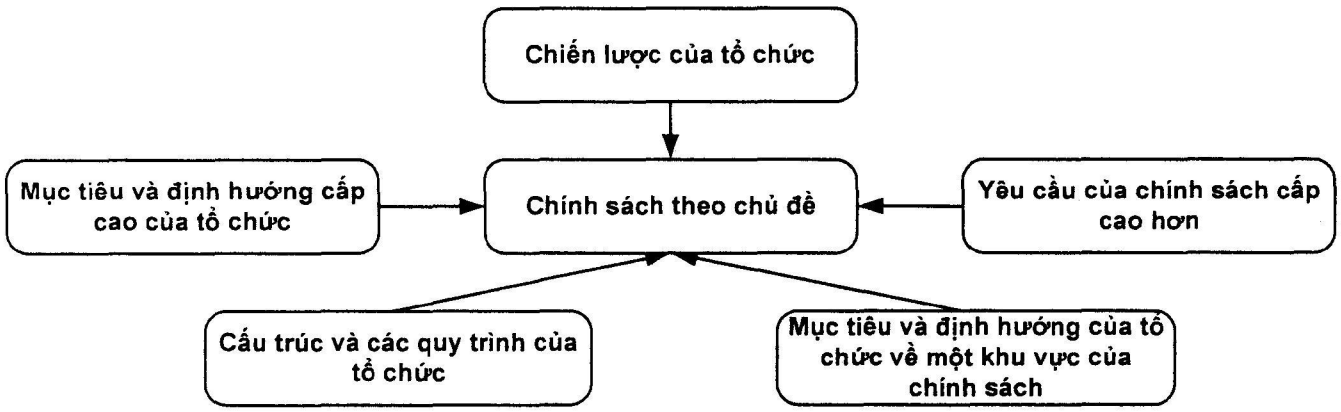
Hình D.1 – Phân cấp chính sách

TCVN ISO/IEC 27001:2009 (ISO/IEC 27001:2005) yêu cầu các tổ chức phải có cả chính sách ISMS và chính sách an toàn thông tin. Tuy nhiên, tiêu chuẩn này không thể hiện rõ mối quan hệ cụ thể giữa các chính sách này. Các yêu cầu đối với chính sách ISMS được đưa ra tại 4.2.1 của TCVN ISO/IEC 27001:2009 (ISO/IEC 27001:2005). Các hướng dẫn về các chính sách an toàn thông tin đã được đưa ra tại 4.1.1 của ISO/IEC 27002:2011 (ISO/IEC 27002:2005). Những chính sách này có thể được phát triển dưới dạng các chính sách cùng phân cấp, chính sách ISMS có thể là cấp thấp hơn của chính sách an toàn thông tin, hoặc chính sách an toàn thông tin là cấp thấp hơn của chính sách ISMS.

Nội dung của các chính sách đều được dựa trên nội dung hoạt động của tổ chức. Đặc biệt, các vấn đề sau đây nên được xem xét khi thiết lập từng chính sách trong khung chính sách của tổ chức:

1) các mục đích và mục tiêu của tổ chức;
2) các chiến lược đã được thông qua để đạt được mục tiêu;
3) cấu trúc và các quy trình đã được tổ chức thông qua;
4) các mục đích và mục tiêu liên quan đến chủ đề của chính sách;
5) các yêu cầu của các chính sách ở phân cấp liên quan cao hơn.

Các vấn đề được thể hiện trong hình bên dưới.



Hình D.2 – Các đầu vào để phát triển một chính sách

Mỗi chính sách có thể có cấu trúc như sau:

1. Tóm tắt chính sách: một hoặc hai câu tổng quan về chính sách (mục này có thể được gộp vào phần giới thiệu).
2. Giới thiệu: giải thích ngắn gọn về chủ đề của chính sách.
3. Phạm vi: mô tả các bộ phận hoặc các hoạt động của một tổ chức mà chính sách tác động đến. Nếu có thể thì phần phạm vi cần liệt kê các chính sách khác được hỗ trợ bởi chính sách này.
4. Các mục tiêu: mô tả ý nghĩa của chính sách.

5. Các nguyên tắc: mô tả các quy tắc liên quan đến các hành động, các quyết định để đạt được mục tiêu của chính sách. Trong một số trường hợp, có thể nên xác định các quy trình chính liên quan đến chủ đề của chính sách và sau đó cả các quy tắc thực thi các quy trình này.
6. Các trách nhiệm: mô tả những người chịu trách nhiệm đối với các hành động để đáp ứng các yêu cầu của chính sách. Trong một số trường hợp, có thể phải đưa ra cả mô tả về cơ cấu tổ chức cũng như trách nhiệm của các cá nhân theo các vai trò được phân bổ.
7. Các kết quả chính: mô tả các kết quả nghiệp vụ nếu đáp ứng được các mục tiêu đề ra.
8. Các chính sách liên quan: mô tả các chính sách khác liên quan đến việc đạt được các mục tiêu, thường dưới hình thức đưa ra thông tin chi tiết bổ sung liên quan đến các chủ đề cụ thể.

CHÚ THÍCH: Nội dung chính sách có thể được tổ chức theo nhiều cách khác nhau. Ví dụ, các tổ chức tập trung vào các vai trò và trách nhiệm có thể mô tả ngắn gọn các mục tiêu, và áp dụng các nguyên tắc đặc biệt với việc mô tả các trách nhiệm.

Dưới đây là một ví dụ về một chính sách an toàn thông tin, trong đó thể hiện cấu trúc và nội dung của chính sách.

Chính sách an toàn thông tin (ví dụ)

Tóm tắt chính sách

Thông tin phải luôn được bảo vệ, cho dù chúng ở dạng nào và cho dù chúng có được chia sẻ, trao đổi hoặc lưu trữ.

Giới thiệu

Thông tin có thể tồn tại dưới nhiều hình thức. Nó có thể được in hoặc viết trên giấy, được lưu trữ dưới dạng thông tin điện tử, được chuyển qua đường bưu điện hoặc bằng các phương tiện điện tử, được thể hiện trên phim, hoặc được nói ra trong các cuộc hội thoại.

An toàn thông tin là bảo vệ thông tin trước các mối đe dọa khác nhau để đảm bảo tính liên tục của hoạt động nghiệp vụ, giảm thiểu rủi ro, tối đa hóa lợi nhuận đầu tư và các cơ hội kinh doanh.

Phạm vi

Chính sách này hỗ trợ chính sách an toàn chung trong tổ chức.

Chính sách này áp dụng cho toàn bộ tổ chức.

Các mục tiêu an toàn thông tin

1. Chiến lược và các rủi ro an toàn thông tin về vận hành được thông hiểu và được xử lý để tổ chức có thể chấp nhận.
2. Sự bí mật của thông tin về khách hàng, các kế hoạch phát triển và tiếp thị sản phẩm được bảo vệ.
3. Sự toàn vẹn của các hồ sơ kiểm tra được đảm bảo.

4. Mạng nội bộ và các dịch vụ trang thông tin điện tử công cộng đáp ứng các tiêu chuẩn cụ thể.

Các nguyên tắc an toàn thông tin

1. Tổ chức khuyến khích xử lý rủi ro và chịu đựng một số rủi ro mà các tổ chức bảo thủ không chấp nhận trong trường hợp các rủi ro thông tin đều đã được thông hiểu, được giám sát và xử lý khi cần thiết. Chi tiết về cách tiếp cận thực hiện đánh giá và xử lý rủi ro đã được đề cạp trong chính sách ISMS.
2. Tất cả các nhân viên đều phải nhận thức và có trách nhiệm về an toàn thông tin liên quan đến vai trò công việc của họ.
3. Sẵn sàng cung cấp các biện pháp quản lý an toàn thông tin về các quy trình quản lý dự án và vận hành.
4. Các khả năng gian lận liên quan đến việc lạm dụng các hệ thống thông tin sẽ được xem xét trong quá trình quản lý tổng thể các hệ thống thông tin.
5. Các hồ sơ về tình trạng an toàn thông tin phải luôn sẵn sàng.
6. Các rủi ro an toàn thông tin sẽ được giám sát và các hành động sẽ được thực thi khi có những thay đổi gây ra các rủi ro vượt quá mức cho phép.
7. Chỉ tiêu về phân loại rủi ro và chấp nhận rủi ro được nêu trong chính sách ISMS.
8. Các tình trạng nằm ngoài sức chịu đựng của tổ chức có thể khiến tổ chức vi phạm các điều luật và quy định của luật pháp.

Các trách nhiệm

1. Ban lãnh đạo cấp cao chịu trách nhiệm đảm bảo an toàn thông tin trong toàn bộ tổ chức được xử lý thích đáng.
2. Mỗi người lãnh đạo cấp cao đều chịu trách nhiệm đảm bảo rằng các nhân viên cấp dưới của họ đều thực hiện bảo vệ thông tin theo đúng các tiêu chuẩn của tổ chức.
3. Giám đốc an toàn thông tin đưa ra gợi ý cho ban lãnh đạo cấp cao, cung cấp hỗ trợ chuyên môn cho đội ngũ nhân viên của tổ chức, và đảm bảo rằng các báo cáo về tình trạng an toàn thông tin trong tổ chức luôn sẵn sàng.
4. Mỗi nhân viên đều có các trách nhiệm về an toàn thông tin theo phận sự công việc mà họ đảm nhiệm.

Các kết quả chính

1. Các sự cố an toàn thông tin sẽ không làm phát sinh các chi phí không mong muốn và nghiêm trọng hoặc làm gián đoạn nghiêm trọng các dịch vụ và các hoạt động nghiệp vụ.
2. Các thiệt hại do gian lận sẽ được nhận biết và nằm trong các giới hạn chấp nhận.

3. Sự chấp nhận của khách hàng về các sản phẩm hoặc dịch vụ sẽ không bị ảnh hưởng bất lợi bởi những vấn đề liên quan đến an toàn thông tin.

Các chính sách liên quan

Các chính sách chi tiết sau đây cung cấp các nguyên tắc và hướng dẫn về các khía cạnh cụ thể của an toàn thông tin.

1. chính sách về hệ thống quản lý an toàn thông tin (ISMS)
2. chính sách về kiểm soát truy cập
3. chính sách bàn làm việc sạch và màn hình sạch
4. chính sách về phần mềm trái phép
5. chính sách liên quan đến các tập tin thu thập từ hoặc qua các mạng bên ngoài
6. chính sách liên quan đến mã điện thoại di động
7. chính sách về sao lưu
8. chính sách liên quan đến việc trao đổi thông tin giữa các tổ chức
9. chính sách liên quan đến việc sử dụng được phép các thiết bị truyền thông điện tử
10. chính sách về lưu trữ hồ sơ
11. chính sách về sử dụng các dịch vụ mạng
12. chính sách liên quan đến tính toán và truyền thông di động
13. chính sách về làm việc từ xa
14. chính sách về sử dụng biện pháp quản lý mật khẩu
15. chính sách về tuân thủ
16. chính sách về bản quyền phần mềm
17. chính sách về loại bỏ phần mềm
18. chính sách về bảo vệ dữ liệu và quyền riêng tư

Tất cả các chính sách đều hỗ trợ:

- xác định rủi ro, bằng cách cung cấp danh sách cơ bản của các biện pháp quản lý, chúng có thể được sử dụng để xác định những lỗ hổng trong thiết kế và triển khai hệ thống; và
- xử lý rủi ro, bằng cách hỗ trợ xác định các biện pháp xử lý các khiếm khuyết và các mối đe dọa đã được xác định.

Cả hai quy trình Xác định rủi ro và Xử lý rủi ro đều đã được xác định trong phần Các nguyên tắc của chính sách. Tham khảo Chính sách ISMS để có thêm thông tin chi tiết.

Phụ lục E

(Tham khảo)

Giám sát và đo lường

Phụ lục này đưa ra các hướng dẫn bổ sung hỗ trợ lập kế hoạch và thiết kế giám sát, đánh giá an toàn thông tin.

Thông tin về Thiết lập giám sát và đo lường

Thiết kế các yêu cầu ISMS cụ thể phải bao gồm cả chương trình giám sát và đo kiểm đối với ISMS để hỗ trợ việc soát xét của ban quản lý.

Thiết kế giám sát:

Hình E.1 – Quy trình giám sát

Chuẩn bị và phối hợp: định danh các tài sản có liên quan cần giám sát

Cần lưu ý rằng giám sát là một quy trình liên tục, và do vậy, khi thiết kế cần quan tâm đến việc thiết lập quy trình giám sát cũng như thiết kế các yêu cầu và các hoạt động giám sát thực tế. Các hoạt động này cần được phối hợp với nhau, và đó là một phần của thiết kế.

Dựa trên thông tin đã cho trong phạm vi và các tài sản đã được xác định, kết hợp với các kết quả từ những phân tích rủi ro và việc lựa chọn các biện pháp quản lý, có thể xác định được các mục tiêu giám sát. Những mục tiêu này phải bao gồm:

- Điều cần phát hiện
- Thời gian
- Điều cần chống lại

Trên thực tế, các hoạt động/quy trình tổ chức được thiết lập trước đó và các tài sản liên quan chính là phạm vi cơ bản của công việc giám sát (giải thích câu hỏi Điều cần chống lại ở trên). Để thiết kế giám sát, có thể cần phải lựa chọn các tài sản quan trọng dựa trên một quan điểm về an toàn thông tin nào

đó. Cũng cần lưu ý đến việc xử lý rủi ro và lựa chọn các biện pháp quản lý để tìm ra những gì cần phải được giám sát trong các tài sản và các hoạt động/quy trình tổ chức liên quan (giải thích cho câu hỏi Điều cần phát hiện và Khi nào).

Vì giám sát có thể có những khía cạnh pháp lý nên việc thiết kế giám sát phải được kiểm tra sao cho nó gặp bất cứ vấn đề pháp lý nào.

Để đảm bảo rằng công việc giám sát thực sự hiệu quả thì điều quan trọng là phải phối hợp và đưa ra thiết kế chính thức của tất cả các hoạt động/quy trình cần giám sát.

Giám sát các hoạt động:

Để duy trì một mức độ an toàn thông tin nhất định thì phải áp dụng chính xác các biện pháp quản lý an toàn thông tin đã được xác định là phù hợp; các sự cố an toàn phải được phát hiện và giải quyết kịp thời, và hiệu suất của hệ thống quản lý an toàn thông tin phải được giám sát thường xuyên. Các cuộc kiểm tra thường xuyên phải được thực hiện để xem liệu tất cả các biện pháp quản lý có đang được áp dụng và triển khai theo kế hoạch trong nội dung an toàn thông tin không. Các kiểm tra này phải kiểm tra xem các biện pháp quản lý kỹ thuật (ví dụ, các biện pháp liên quan đến cấu hình) và các biện pháp quản lý về tổ chức (ví dụ, các quy trình, thủ tục và các vận hành) có tuân thủ không. Các cuộc kiểm tra phải hướng việc tìm kiếm các biện pháp khắc phục các nhược điểm. Nếu các cuộc kiểm tra sẽ được chấp nhận thì điều quan trọng là tất cả các cá nhân tham gia phải nhận thức được cách làm việc này và đó chính là mục tiêu của các cuộc kiểm tra. Sự thảo luận về các giải pháp khả thi cho các vấn đề với sự tham gia của những cá nhân này trong suốt các cuộc kiểm tra và chuẩn bị sẵn các biện pháp khắc phục thích hợp cũng là vấn đề quan trọng.

Các cuộc kiểm tra phải được chuẩn bị kỹ lưỡng để đảm bảo rằng chúng có thể đạt được các mục tiêu một cách hiệu quả đến mức có thể trong khi đồng thời chỉ gây gián đoạn ít nhất đến guồng máy công việc. Triển khai chung của các cuộc kiểm tra phải được thống nhất trước với ban quản lý. Các hoạt động thiết kế có thể thuộc ba hình thức khác nhau cơ bản như sau:

- các báo cáo sự cố
- xác minh hoặc sự không tuân thủ của chức năng quản lý
- các cuộc kiểm tra thường xuyên khác

Hơn nữa, các kết quả từ các hoạt động này phải được thiết kế về cách thức xây dựng các báo cáo và cách thức báo cáo thông tin lên ban quản lý. Hệ thống tài liệu chính thức phải mô tả được thiết kế và các hoạt động cơ bản và các mục đích của chúng, cũng như các trách nhiệm liên quan.

Yêu cầu đối với kết quả giám sát

Các kết quả giám sát gồm:

a) Các báo cáo về các hoạt động giám sát theo mức độ chi tiết được yêu cầu

Cũng giống như mọi kết quả của các hoạt động giám sát, nên lập hồ sơ giám sát của ban quản lý. Tất cả các thông tin ban quản lý yêu cầu để hoàn thành các nhiệm vụ quản lý và giám sát của họ đều nên được ghi vào hồ sơ theo mức độ chi tiết được yêu cầu.

b) Các thông tin để ban quản lý đưa ra quyết định khi cần đối với các hành động tức thời

Các báo cáo trình lên ban quản lý phải luôn kết thúc bằng một danh sách các hành động được đề xuất theo thứ tự ưu tiên rõ ràng cùng với một đánh giá thực tế về chi phí dự kiến để triển khai từng hành động này. Điều đó sẽ đảm bảo rằng có thể nhận được các quyết định cần thiết từ ban quản lý mà không bị chậm trễ quá mức.

Xây dựng chương trình đo lường an toàn thông tin

Tổng quan về thiết kế chương trình đo lường an toàn thông tin

Quy trình đo lường nên được đưa vào chu trình ISMS của dự án hoặc tổ chức, và được sử dụng để thực hiện cải tiến liên tục các quy trình và kết quả liên quan trong dự án hoặc tổ chức đó. Quy trình này liên quan đến chương trình đo lường an toàn thông tin (TCVN 10542:2014 (ISO/IEC 27004:2009)). Thiết kế của chương trình này cần được xem xét trên quan điểm về chu trình ISMS. Hình dưới đây sẽ mô tả cách thức đưa quy trình đo lường vào chu trình ISMS.

Các chức năng sau đây là các chức năng cần có của hệ thống quản lý để đảm bảo thỏa mãn các vấn đề được yêu cầu và các mong muốn, ví dụ thực hiện cơ cấu PDCA; đo lường tính đúng đắn của các đầu ra và hiệu lực của nó; và cung cấp thông tin phản hồi về các kết quả đo lường cho người quản lý của các quy trình.

Để có các bài đo đúng, cần sử dụng các thông tin đã có trước, đặc biệt là:

a) chính sách ISMS, bao gồm cả phạm vi và giới hạn;

b) kết quả từ đánh giá rủi ro;

c) biện pháp quản lý được chọn;

d) các mục tiêu quản lý;

e) các mục tiêu an toàn thông tin cụ thể;

f) các quy trình cụ thể, các nguồn lực và phân loại của chúng.

Ban quản lý nên thiết lập và duy trì cam kết đối với quy trình đo lường tổng thể. Khi triển khai một quy trình đo lường, ban quản lý nên:

a) chấp nhận các yêu cầu về đo lường; xem TCVN 10542:2014 (ISO/IEC 27004:2009) để có thông tin cụ thể;

b) lưu ý đến các nhu cầu thông tin; xem TCVN 10542:2014 (ISO/IEC 27004:2009) để có thông tin cụ thể;

c) nhận được cam kết của đội ngũ nhân viên thông qua các hoạt động sau:

- Tổ chức nên thể hiện rõ cam kết thông qua, ví dụ, một chính sách đo lường cho tổ chức, phân bổ các trách nhiệm và nhiệm vụ, đào tạo, và phân bổ ngân quỹ và các nguồn lực khác.
- Nên chỉ định một cá nhân hoặc một đơn vị thuộc tổ chức chịu trách nhiệm về chương trình đo lường.
- Một cá nhân hoặc một đơn vị thuộc tổ chức chịu trách nhiệm công bố tầm quan trọng và các kết quả đo lường ISMS tới toàn bộ tổ chức để đảm bảo chúng được tổ chức chấp nhận và sử dụng, và việc này nên có sự hỗ trợ của ban quản lý.
- Đảm bảo rằng các dữ liệu đo lường ISMS được thu thập, phân tích, và báo cáo tới CIO và các bên liên quan khác.
- Giáo dục những người quản lý chuyên môn về việc sử dụng các kết quả đo lường ISMS cho các quyết định về chính sách, phân bổ nguồn lực, và ngân quỹ.

Thiết kế và chương trình đo lường an toàn thông tin nên có sự tham gia của các cá nhân sau:

a) Quản lý cấp cao

b) Những người sử dụng các sản phẩm an toàn thông tin

c) Những người phụ trách các hệ thống thông tin

d) Những người phụ trách an toàn thông tin

Chương trình đo lường an toàn thông tin được thiết lập để thu được các minh chứng về hiệu lực của ISMS, của các mục tiêu và biện pháp quản lý ISMS. Chương trình này đã được mô tả trong TCVN 10542:2014 (ISO/IEC 27004:2009).

Các kết quả đo lường phù hợp của Giai đoạn Lập kế hoạch nên được kiểm soát để thỏa mãn các mục tiêu này.

Mỗi tổ chức có thể có một chương trình đo lường an toàn thông tin phù hợp riêng tùy theo cấu trúc của tổ chức:

a) Quy mô của tổ chức

b) Mức độ phức tạp của tổ chức

c) Các rủi ro tổng thể/Nhu cầu của an toàn thông tin

Nhìn chung, tổ chức có quy mô càng lớn và càng phức tạp thì càng cần có chương trình đo lường với phạm vi rộng. Tuy nhiên, mức độ rủi ro tổng thể cũng ảnh hưởng đến phạm vi của chương trình đo lường. Nếu tác động của an toàn thông tin yếu kém là nghiêm trọng thì các tổ chức tương đối nhỏ có thể cần có chương trình đo lường toàn diện để kiểm soát hết các rủi ro hơn các tổ chức lớn không phải đối mặt với tác động tương tự. Phạm vi của chương trình đo lường có thể được ước lượng dựa trên các biện pháp quản lý được lựa chọn cần được kiểm soát và kết quả từ phân tích rủi ro.

Thiết kế chương trình đo lường an toàn thông tin

Người chịu trách nhiệm về chương trình đo lường an toàn thông tin nên quan tâm đến những vấn đề sau đây:

a) Phạm vi chương trình đo lường

b) Các bài đo

c) Thực hiện các bài đo

d) Thời gian thực hiện các bài đo

e) Báo cáo kết quả đo

Phạm vi của chương trình đo lường nên bao hàm phạm vi, các mục tiêu và biện pháp quản lý của ISMS. Việc đo lường ISMS nên được thiết lập theo đặc thù của từng tổ chức, tổ chức, địa điểm của tổ chức, các tài sản và công nghệ của tổ chức, và bao gồm các thông tin chi tiết và bằng chứng cụ thể về việc loại bỏ các đối tượng ra ngoài phạm vi ISMS. Các đối tương bị loại bỏ có thể là một biện pháp quản lý an toàn, một quy trình, một hệ thống, một khu vực chức năng, toàn bộ một cơ sở, một chi nhánh, hoặc một tổ chức gồm nhiều chi nhánh.

Khi lựa chọn một bài đo, điều Quy trình đo lường hệ thống an toàn thông tin trong TCVN 10542:2014 (ISO/IEC 27004:2009) đã quy định rằng điểm xuất phát chính là đối tượng của bài đo. Để thiết lập một chương trình đo lường, các đối tượng này nên được xác định rõ. Các đối tượng này có thể là một quy trình hoặc một nguồn lực (xem thêm chi tiết tại TCVN 10542:2014 (ISO/IEC 27004:2009)). Khi xác định chương trình này, các đối tượng đã được xác định bởi phạm vi ISMS thường được chia nhỏ để tìm ra các đối tượng thực sự cần được đánh giá. Quy trình xác định có thể được minh họa bằng ví dụ sau đây: Tổ chức là một đối tượng tổng thể - Quy trình tổ chức A/ hoặc hệ thống ICT X là một bộ phận của đối tượng đó và đại diện cho đối tượng – Các đối tượng thuộc quy trình có ảnh hưởng đến an toàn thông tin (con người, các quy định, hệ thống mạng, các ứng dụng, thiết bị...) nhìn chung là các đối tượng được đo lường nhằm thấy được hiệu quả của việc bảo vệ thông tin.

Khi triển khai thực hiện một Chương trình đo lường an toàn thông tin, cần lưu ý rằng các đối tượng được đo lường có thể thuộc nhiều quy trình tổ chức trong phạm vi ISMS, và do vậy có thể có tác động nhiều hơn tới hiệu lực của ISMS và các mục tiêu quản lý. Nhìn chung, các đối tượng này nên được phân cấp ưu tiên theo phạm vi của chương trình, chẳng hạn như Tổ chức an toàn thông tin và quy trình liên quan, phòng máy tính, các đồng nghiệp có liên quan đến an toàn thông tin...

Thời gian thực hiện đo lường có thể thay đổi, nhưng việc đo lường nên kết thúc hoặc được tổng kết vào một khoảng thời gian nhất định để khớp với chương trình soát xét của ban quản lý và quy trình cải tiến liên tục cũng như những mong đợi đối với ISMS. Thiết kế chương trình nên thể hiện rõ điều này.

Công tác báo cáo kết quả đánh giá nên được thiết kế sao cho việc công bố được đảm bảo theo TCVN 10542:2014 (ISO/IEC 27004:2009).

Thiết kế chương trình đo lường an toàn thông tin nên đi cùng với quy định về thủ tục đo lường, tài liệu này nên được ban quản lý phê chuẩn. Tài liệu này nên chứa các nội dung sau:

a) Các trách nhiệm về chương trình đo lường an toàn thông tin

b) Các trách nhiệm về truyền thông

c) Phạm vi đo lường

d) Cách thức thực hiện (phương pháp cơ bản được sử dụng, nội bộ thực hiện, thuê ngoài...)

e) Thời gian thực hiện

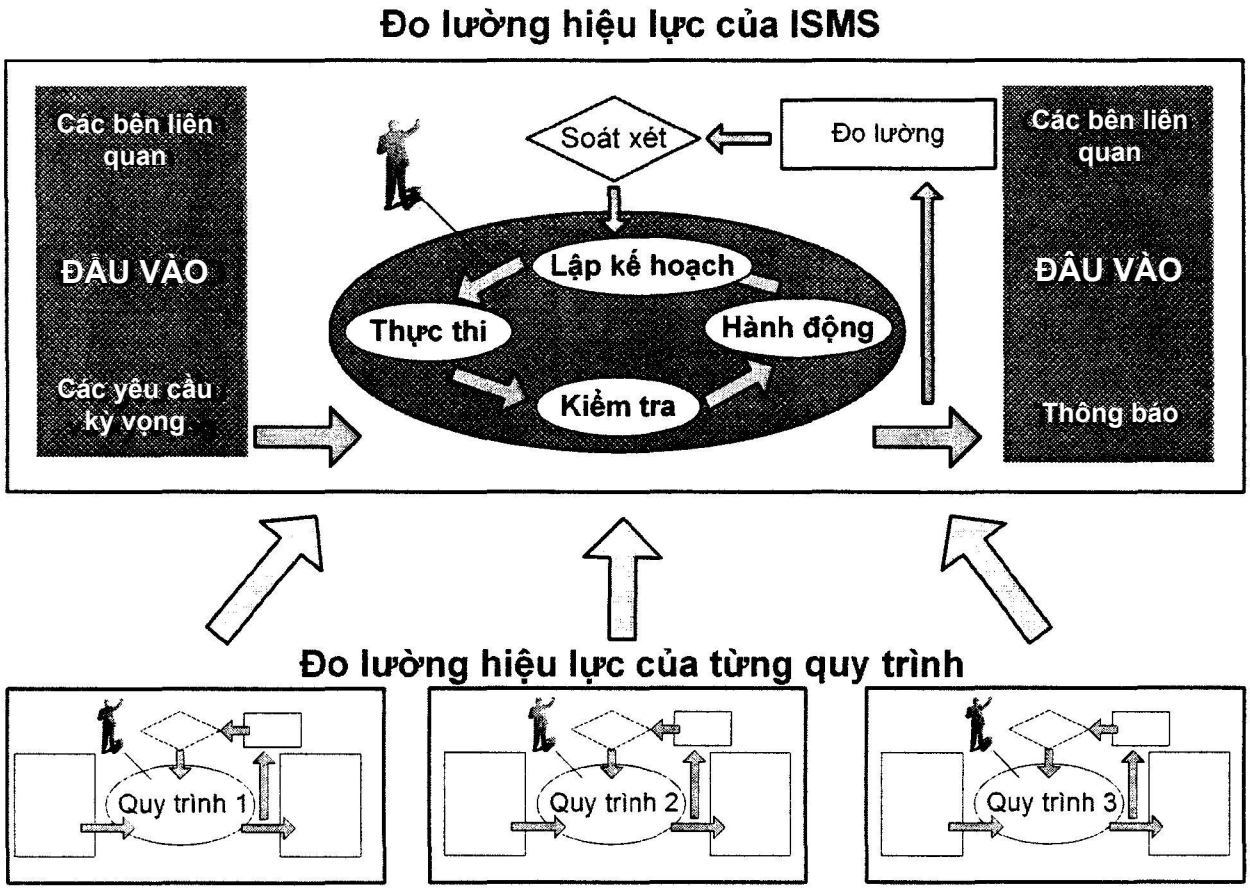
f) Các thức lập hồ sơ

Nếu tổ chức xây dựng các điểm đánh giá riêng thì chúng phải được ghi thành tài liệu và thuộc giai đoạn thiết kế, tham khảo thông tin chi tiết tại TCVN 10542:2014 (ISO/IEC 27004:2009). Tài liệu này chỉ mang tính chất tổng quan và không cần phải được ban quản lý ký vì các chi tiết có thể thay đổi khi triển khai.

Đo lường hiệu lực của ISMS

Khi thiết lập phạm vi của chương trình đo lường an toàn thông tin sẽ được triển khai, cần lưu ý không nên đưa ra số lượng đối tượng đo lường quá lớn. Nếu số lượng đối tượng lớn, có thể chia nhỏ chương trình thành nhiều bộ phận khác nhau. Phạm vi của các bộ phận này có thể được coi như là các phần đo lường riêng để so sánh, nhưng mục đích cơ bản của chúng thường là: kết hợp các phần đo lường để đưa ra dấu hiệu để đánh giá hiệu lực của ISMS. Các phạm vi nhỏ này thường là một đơn vị tổ chức và có thể được xác định bằng các giới hạn rõ ràng. Sự kết hợp các đối tượng tham gia vào các quy trình của tổ chức và các công việc đo lường các đối tượng thuộc các phạm vi nhỏ có thể hình thành một phạm vi phù hợp cho Chương trình đo lường an toàn thông tin. Vì vậy, hiệu lực của toàn bộ ISMS có thể được đo lường dựa trên việc đo lường các kết quả của hai hoặc nhiều quy trình/đối tượng này.

Vì mục tiêu là đo lường hiệu lực của ISMS nên điều quan trọng là phải đo lường được các mục tiêu quản lý và biện pháp quản lý. Số lượng phù hợp của các biện pháp quản lý chỉ là một khía cạnh, còn các biện pháp quản lý đó có đủ để đánh giá hiệu lực của ISMS không lại là một vấn đề khác (có thể có các lý do khác cho việc hạn chế phạm vi của Chương trình đo lường an toàn thông tin, như đã được đề cập trong TCVN 10542:2014 (ISO/IEC 27004:2009)).



Hình E.2 – Hai nội dung đo lường hiệu lực theo quy trình PDCA của ISMS và các quy trình ví dụ trong tổ chức

Khi sử dụng các kết quả đo lường để đánh giá hiệu lực của ISMS, các mục tiêu quản lý và biện pháp quản lý thì có một điều vô cùng quan trọng là ban quản lý phải nhận thức rõ về phạm vi của Chương trình đo lường an toàn thông tin. Người chịu trách nhiệm về chương trình đo lường nên được ban quản lý phê chuẩn phạm vi của Chương trình đo lường an toàn thông tin trước khi triển khai chương trình này.

CHÚ THÍCH 1: Yêu cầu liên quan đến việc đo lường hiệu lực trong TCVN ISO/IEC 27001:2009 (ISO/IEC 27001:2005) là "đánh giá các biện pháp quản lý hoặc nhóm các biện pháp quản lý" (Xem 4.2.2 d) của TCVN ISO/IEC 27001:2009 (ISO/IEC 27001:2005)).

CHÚ THÍCH 2: Yêu cầu liên quan đến hiệu lực của toàn bộ ISMS trong TCVN ISO/IEC 27001:2009 (ISO/IEC 27001:2005) chỉ là "soát xét hiệu lực của toàn bộ ISMS", và không yêu cầu "đánh giá toàn bộ ISMS".

Khi thực hiện đo lường trong thực tế, có thể sử dụng đội ngũ nhân viên nội bộ, bên ngoài, hoặc kết hợp cả hai. Quy mô, cấu trúc và văn hóa của mỗi tổ chức là những yếu tố cần xem xét khi đánh giá các nguồn lực nội bộ hoặc bên ngoài. Các tổ chức, công ty quy mô vừa và nhỏ có nhiều thuận lợi khi sử dụng hỗ trợ từ bên ngoài hơn là các tổ chức lớn. Tùy theo văn hóa của tổ chức, kết quả từ việc sử dụng nguồn lực bên ngoài có thể còn mang lại các kết quả có giá trị hơn. Nếu tổ chức thường tiến hành các đánh giá nội bộ, thì việc sử dụng các nguồn lực nội bộ sẽ thực sự có giá trị.

Thư mục tài liệu tham khảo

[1] TCVN ISO 9001:2008, Hệ thống quản lý chất lượng – Các yêu cầu

[2] TCVN ISO 14001:2005, Hệ thống quản lý môi trường – Các yêu cầu và hướng dẫn sử dụng

[3] TCVN 8709-1:2011, Công nghệ thông tin - Các kỹ thuật an toàn - Các tiêu chí đánh giá an toàn CNTT - Phần 1: Giới thiệu và mô hình tổng quát

[4] TCVN 8709-2:2011, Công nghệ thông tin - Các kỹ thuật an toàn - Các tiêu chí đánh giá an toàn CNTT - Phần 2: Các thành phần chức năng an toàn

[5] TCVN 8709-3:2011, Công nghệ thông tin - Các kỹ thuật an toàn - Các tiêu chí đánh giá an toàn CNTT - Phần 3: Các thành phần đảm bảo an toàn

[6] TCVN ISO/IEC 27001:2009 (ISO/IEC 27001:2005), Công nghệ thông tin - Hệ thống quản lý an toàn thông tin – Các yêu cầu

[7] ISO/IEC 15026 (all parts), Systems and software engineering – Systems and software assurance

[8] TCVN 8695 – 1:2011, Công nghệ thông tin – Quản lý dịch vụ – Phần 1: Các yêu cầu

[9] ISO/IEC 15443-1:2005, Information technology -- Security techniques – A framework for IT security assurance – Part 1: Overview and framework

[10] ISO/IEC 15443-2:2005, Information technology -- Security techniques – A framework for IT security assurance – Part 2: Assurance methods

[11] ISO/IEC 15443-3:2007, Information technology -- Security techniques – A framework for IT security assurance – Part 3: Analysis of assurance methods

[12] ISO/IEC 15939:2007, Systems and software engineering – Measurement process

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

[14] ISO/IEC 16326:2009, Systems and software engineering – Life cycle processes – Project management

[15] ISO/IEC 18045:2008, Information technology -- Security techniques – Methodology for IT security evaluation

[16] ISO/IEC TR 19791:2006, Information technology -- Security techniques – Security assessment of operational systems

[17] TCVN 10542:2014 (ISO/IEC 27004:2009), Công nghệ thông tin – Các kỹ thuật an toàn – Quản lý an toàn thông tin – Đo lường

[18] TCVN 10295:2014 (ISO/IEC 27005:2011), Công nghệ thông tin - Các kỹ thuật an toàn - Quản lý rủi ro an toàn thông tin

[19] ISO 21500, Project management – Guide to project management

[20] ISO/IEC 27006:2007, Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems ISO/IEC 18028-4, Information technology -- Security techniques – IT Netwwork security - Part 4: Securing remote access