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

TCVN 10542:2014

ISO/IEC 27004:2009

Xuất bản lần 1

CÔNG NGHỆ THÔNG TIN – CÁC KỸ THUẬT AN TOÀN – QUẢN LÝ AN TOÀN THÔNG TIN – ĐO LƯỜNG

Information technology – Security techniques – Information security management - Measurement

HÀ NỘI – 2014

Mục lục

Lời nói đầu

TCVN 10542:2014 hoàn toàn tương đương với ISO/IEC 27004:2009

TCVN 10542:2014 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 – Quản lý an toàn thông tin – Đo lường

Information technology – Security techniques – Information security management - Measurement

1 Phạm vi áp dụng

Tiêu chuẩn này cung cấp hướng dẫn cho việc phát triển và sử dụng các số đo, phép đo để đánh giá hiệu lực của một hệ thống quản lý an toàn thông tin (ISMS) đã triển khai và các biện pháp quản lý hay nhóm các biện pháp quản lý, theo quy định tại tiêu chuẩn TCVN ISO/IEC 27001:2009.

Tiêu chuẩn này khuyến nghị áp dụng đối với tất cả các tổ chức ở mọi loại hình và quy mô.

CHÚ THÍCH: Tài liệu này sử dụng các dạng bằng lời cho việc diễn tả các điều khoản (như "phải", "phải không", "nên", "không nên", "cần", "không cần", "có thể" và "không thể") được chuẩn hóa trong chỉ dẫn ISO/IEC, Phần 2, 2004, Phụ lục H. Xem ISO/IEC 27000:2009, Phụ lục A.

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, Công nghệ thông tin – Các kỹ thuật an toàn - Hệ thống quản lý an toàn thông tin - Các yêu cầu *(Information technology – Security techniques – Information security management systems – Requirements)*.

3 Thuật ngữ và định nghĩa

3.1
Mô hình phân tích (analytical model)

Thuật toán hoặc phép tính kết hợp một hay nhiều số đo cơ bản (base measure) và/hoặc số đo dẫn xuất với các tiêu chí quyết định đi kèm.

[ISO/IEC 15939:2007]

3.2
Thuộc tính (attribute)

Các đặc tính hoặc đặc điểm của một đối tượng mà có thể phân biệt một cách định lượng hoặc định tính bởi con người hoặc thiết bị tự động (automated means).

đích sử dụng cụ thể hoặc ứng dụng đã được thỏa mãn.

3.18
Sự xác minh (Verification)

Sự xác nhận, thông qua việc cung cấp các bằng chứng khách quan, rằng các yêu cầu cụ thể đã được thỏa mãn.

[ISO/IEC 9000:2005]

CHÚ THÍCH: Cũng còn được gọi là việc kiểm tra tuân thủ.

4 Cấu trúc tiêu chuẩn

Tiêu chuẩn này giải thích về các số đo và các hoạt động đo lường cần thiết để đánh giá hiệu lực của các yêu cầu ISMS cho ban quản lý đối với các biện pháp quản lý an toàn thông tin một cách phù hợp và tương xứng theo yêu cầu nêu trong tiêu chuẩn TCVN ISO/IEC 27001:2009, 4.2.

Tiêu chuẩn này được cấu trúc như sau:

- Tổng quan về Chương trình đo lường an toàn thông tin và Mô hình đo lường an toàn thông tin (Điều 5);
- Trách nhiệm của ban quản lý trong đo lường an toàn thông tin (Điều 6);
- Các cấu trúc phép đo và các quy trình (như việc lập kế hoạch và phát triển, triển khai, hoạt động, vận hành và cải tiến các phép đo: trao đổi các kết quả phép đo) để triển khai trong Chương trình đo lường an toàn thông tin (Điều 7 – 10);

Ngoài ra, Phụ lục A cung cấp một mẫu ví dụ về cấu trúc phép đo trong đó các thành phần là các yếu tố của mô hình đo lường an toàn thông tin (xem Điều 7). Phụ lục B cung cấp các ví dụ cấu trúc phép đo về các biện pháp quản lý cụ thể hay các quy trình của ISMS, sử dụng mẫu cung cấp trong Phụ lục A.

Những ví dụ này giúp tổ chức trong việc làm thế nào để triển khai Đo lường hệ thống an toàn thông tin và làm thế nào để ghi lại các hành động đo và các kết quả từ chúng.

5 Tổng quan về đo lường an toàn thông tin

5.1 Các mục tiêu của đo lường an toàn thông tin

Các mục tiêu của đo lường an toàn thông tin trong bối cảnh của ISMS bao gồm:

a) Ước lượng hiệu lực của các biện pháp quản lý hay nhóm các biện pháp quản lý đã triển khai (xem 4.2.2 d trong Hình 1);

b) Ước lượng hiệu lực của ISMS đã triển khai (xem 4.2.3 b trong Hình 1);

c) Xác minh mức độ đáp ứng các yêu cầu an toàn thông tin đã xác định (xem 4.2.3 c trong Hình 1);

3.11
Hàm đo (measurement function)

Thuật toán hoặc tính toán được thực hiện để kết hợp hai hoặc nhiều số đo cơ bản.

[ISO/IEC 15939:2007]

3.12
Phương pháp đo (measurement method)

Trình tự logic của các phép toán, được mô tả một cách tổng quát, được sử dụng trong việc định lượng một thuộc tính đối với một thang đo đo xác định.

[ISO/IEC 15939:2007]

CHÚ THÍCH: Loại phương pháp đo phụ thuộc vào bản chất của các phép toán được sử dụng để định lượng một thuộc tính. Hai loại phương pháp được phân biệt:

- Chủ quan: việc định lượng liên quan tới chủ định của con người;
- Khách quan: việc định lượng dựa trên các nguyên tắc số học.

3.13
Kết quả đo (measurement results)

Một hoặc nhiều chỉ báo và các giải thích đi kèm nhằm giải quyết một nhu cầu thông tin.

3.14
Đối tượng (object)

Đề mục được đặc trưng hóa thông qua đo lường các thuộc tính của nó.

3.15
Thang đo (scale)

Tập hợp có thứ tự các giá trị liên tục hay rời rạc, hoặc là một tập các phân loại mà các thuộc tính được ánh xạ tới.

[ISO/IEC 15939:2007]

CHÚ THÍCH: Loại thang đo phụ thuộc vào bản chất của mối quan hệ giữa các giá trị trên thang đo. Bốn loại thang đo thường được định nghĩa là:

- Danh định: các giá trị đo là giá trị rõ ràng;
- Thứ tự: các giá trị đo là các hạng/bậc;
- Khoảng đoạn: các giá trị đo có các khoảng bằng nhau tương ứng với các số lượng như nhau của thuộc tính;
- Tỷ lệ: các giá trị đo có những khoảng cách bằng nhau tương ứng với các số lượng bằng nhau của thuộc tính, với giá trị bằng không thì không tương ứng với thuộc tính nào.

3.16
Đơn vị đo (unit of measurement)

Lượng cụ thể, được xác định và chấp nhận theo quy ước, với lượng này, các lượng khác cùng loại được so sánh để diễn tả mối tương quan về độ lớn với lượng đó.

[ISO/IEC 15939:2007]

3.17
Hợp lệ (validation)

Sự xác nhận, thông qua việc cung cấp các bằng chứng khách quan, rằng các yêu cầu cho một mục

đích sử dụng cụ thể hoặc ứng dụng đã được thỏa mãn.

3.18
Sự xác minh (Verification)

Sự xác nhận, thông qua việc cung cấp các bằng chứng khách quan, rằng các yêu cầu cụ thể đã được thỏa mãn.

[ISO/IEC 9000:2005]

CHÚ THÍCH: Cũng còn được gọi là việc kiểm tra tuân thủ.

4 Cấu trúc tiêu chuẩn

Tiêu chuẩn này giải thích về các số đo và các hoạt động đo lường cần thiết để đánh giá hiệu lực của các yêu cầu ISMS cho ban quản lý đối với các biện pháp quản lý an toàn thông tin một cách phù hợp và tương xứng theo yêu cầu nêu trong tiêu chuẩn TCVN ISO/IEC 27001:2009, 4.2.

Tiêu chuẩn này được cấu trúc như sau:

- Tổng quan về Chương trình đo lường an toàn thông tin và Mô hình đo lường an toàn thông tin (Điều 5);
- Trách nhiệm của ban quản lý trong đo lường an toàn thông tin (Điều 6);
- Các cấu trúc phép đo và các quy trình (như việc lập kế hoạch và phát triển, triển khai, hoạt động, vận hành và cải tiến các phép đo: trao đổi các kết quả phép đo) để triển khai trong Chương trình đo lường an toàn thông tin (Điều 7 – 10);

Ngoài ra, Phụ lục A cung cấp một mẫu ví dụ về cấu trúc phép đo trong đó các thành phần là các yếu tố của mô hình đo lường an toàn thông tin (xem Điều 7). Phụ lục B cung cấp các ví dụ cấu trúc phép đo về các biện pháp quản lý cụ thể hay các quy trình của ISMS, sử dụng mẫu cung cấp trong Phụ lục A.

Những ví dụ này giúp tổ chức trong việc làm thế nào để triển khai Đo lường hệ thống an toàn thông tin và làm thế nào để ghi lại các hành động đo và các kết quả từ chúng.

5 Tổng quan về đo lường an toàn thông tin

5.1 Các mục tiêu của đo lường an toàn thông tin

Các mục tiêu của đo lường an toàn thông tin trong bối cảnh của ISMS bao gồm:

a) Ước lượng hiệu lực của các biện pháp quản lý hay nhóm các biện pháp quản lý đã triển khai (xem 4.2.2 d trong Hình 1);

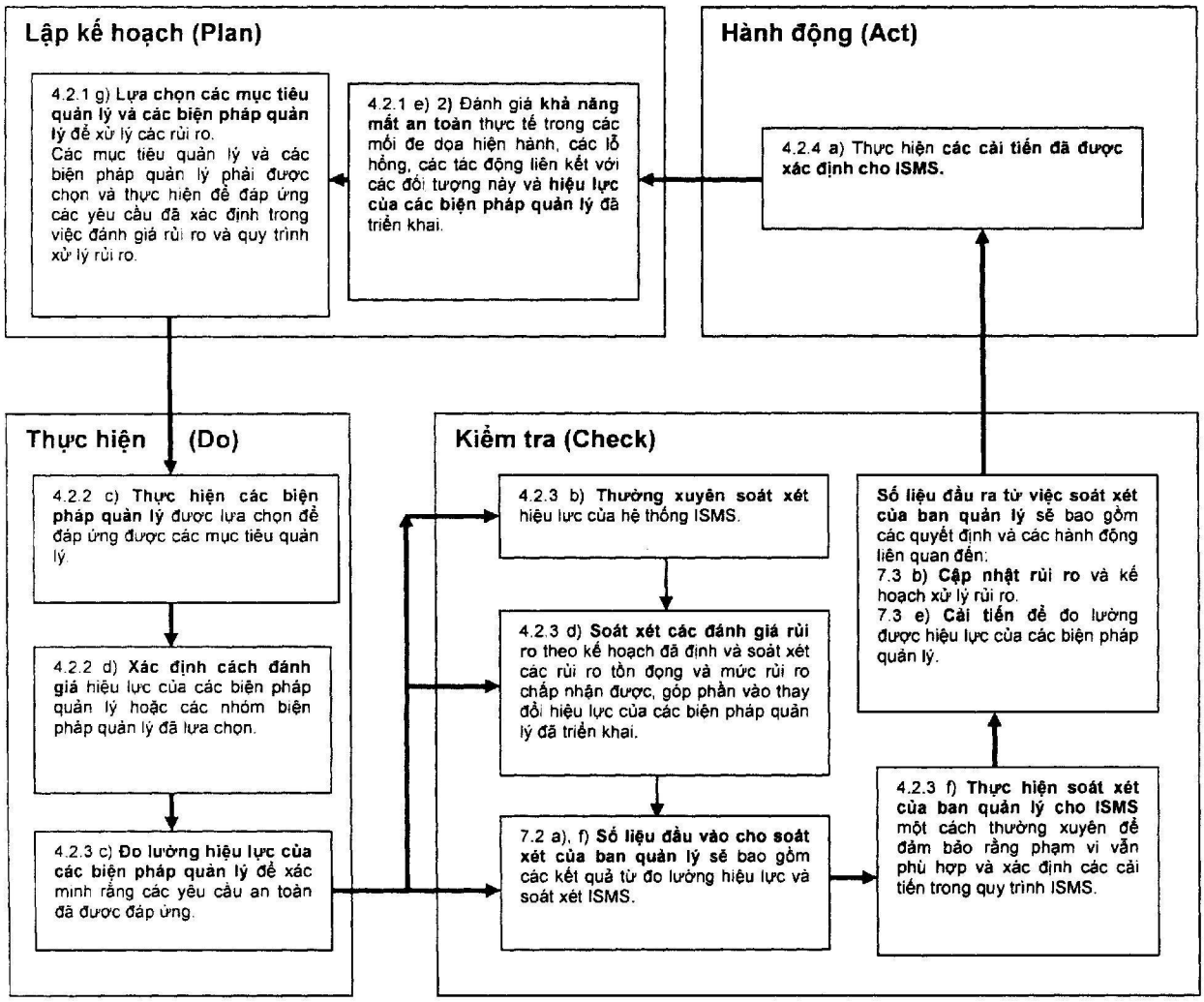
b) Ước lượng hiệu lực của ISMS đã triển khai (xem 4.2.3 b trong Hình 1);

c) Xác minh mức độ đáp ứng các yêu cầu an toàn thông tin đã xác định (xem 4.2.3 c trong Hình 1);

d) Tạo điều kiện thuận lợi cho việc thực hiện cải tiến an toàn thông tin về mặt quản lý rủi ro nghiệp vụ tổng thể của tổ chức;

e) Cung cấp thông tin đầu vào cho việc soát xét của ban quản lý để tạo điều kiện đưa ra các quyết định liên quan đến ISMS và việc điều chỉnh các cải tiến cần thiết đối với ISMS đã triển khai.

Hình 1 mô tả mối quan hệ giữa đầu vào - đầu ra theo chu kỳ của các hoạt động đo lường theo mô hình Lập kế hoạch - Thực hiện - Kiểm tra - Hành động (PDCA: Plan-Do-Check-Act), như quy định trong tiêu chuẩn TCVN ISO/IEC 27001:2009. Các số trong mỗi hình chính là mục con tương đương của TCVN ISO/IEC 27001:2009.



Hình 1 - Đầu vào và đầu ra trong ISMS theo mô hình PDCA về quản lý an toàn thông tin

Các tổ chức cần thiết lập các mục tiêu đo lường dựa trên một số cân nhắc, bao gồm:

a) Vai trò của an toàn thông tin trong hỗ trợ hoạt động nghiệp vụ tổng thể của tổ chức và những rủi ro hệ thống an toàn thông tin phải đối mặt;

b) Các yêu cầu của luật pháp, quy định và hợp đồng liên quan;

c) Cơ cấu tổ chức;

d) Chi phí và lợi ích của việc thực hiện các phép đo an toàn thông tin;

e) Tiêu chí chấp nhận rủi ro thông tin của tổ chức;

f) Yêu cầu cần so sánh một số ISMS của các tổ chức tương đương.

5.2 Chương trình đo lường an toàn thông tin

Tổ chức nên thiết lập và quản lý Chương trình đo lường an toàn thông tin để đạt được các mục tiêu đo lường đã thiết lập và chấp nhận thực hiện mô hình PDCA trong toàn bộ các hoạt động đo lường của tổ chức. Tổ chức cũng cần phát triển và triển khai các cấu trúc đo lường để có thể có được các kết quả đo khách quan và hữu ích dựa trên Mô hình đo lường an toàn thông tin (xem 5.4).

Chương trình đo lường an toàn thông tin và cấu trúc đo lường đã triển khai nên đảm bảo giúp tổ chức đạt được phép đo mục tiêu có liên quan và có thể lặp lại, và cung cấp kết quả đo cho các bên liên quan để xác định nhu cầu cải tiến ISMS đã triển khai, về cả phạm vi, các chính sách, các mục tiêu, các biện pháp quản lý, các quy trình và các thủ tục.

Chương trình đo lường an toàn thông tin bao gồm các quy trình sau đây:

a) Phát triển các số đo và phép đo (Điều 7);

b) Tiến hành đo lường (Điều 8);

c) Phân tích dữ liệu và lập báo cáo kết quả đo (Điều 9);

d) Ước lượng và cải tiến Chương trình đo lường an toàn thông tin (Điều 10).

Cơ cấu và cấu trúc hoạt động của Chương trình đo lường an toàn thông tin nên được quyết định trên cơ sở quy mô và sự phức tạp của ISMS. Trong mọi trường hợp, các vai trò và trách nhiệm đối với Chương trình đo lường an toàn thông tin nên được quy rõ cho người có đủ năng lực (xem 7.5.8).

Các số đo đã lựa chọn và đã thực hiện bởi Chương trình đo lường an toàn thông tin nên liên quan trực tiếp đến hoạt động của ISMS, đến các số đo khác, cũng như đến quy trình nghiệp vụ của tổ chức. Phép đo có thể được tích hợp vào các hoạt động thường xuyên hoặc được triển khai tại những khoảng thời gian xác định bởi ban quản lý ISMS.

5.3 Các yếu tố giúp thành công

Sau đây là một số yếu tố góp phần vào sự thành công của Chương trình đo lường an toàn thông tin tạo điều kiện thuận lợi để cải tiến ISMS một cách liên tục:

a) Cam kết của ban quản lý hỗ trợ các nguồn lực thích hợp;

b) Sự tồn tại của các quy trình và các thủ tục của ISMS;

c) Một tiến trình có thể lặp lại, có khả năng thu thập và báo cáo/ thông báo dữ liệu có ý nghĩa để cung cấp thông tin cho việc xác định các xu hướng có liên quan trong một khoảng thời gian cụ thể;

d) Các số đo có thể định lượng được dựa trên các mục tiêu của ISMS;

e) Các dữ liệu có thể thu thập dễ dàng cho phép đo;

f) Ước lượng tính hiệu lực của Chương trình đo lường an toàn thông tin và triển khai cải tiến đã định;

g) Duy trì việc thu thập, phân tích và báo cáo dữ liệu đo lường một cách định kỳ, theo cách có ý nghĩa;

h) Việc sử dụng các kết quả đo bởi các bên liên quan để xác định nhu cầu cần cải tiến ISMS đã triển khai, bao gồm cả về phạm vi, các chính sách, các mục tiêu, các biện pháp quản lý, các quy trình và các thủ tục;

i) Việc chấp nhận thông tin phản hồi về kết quả đo từ các bên liên quan;

j) Ước lượng sự hữu dụng của các kết quả đo và thực hiện các cải tiến đã xác định.

Ngay sau khi triển khai thành công, Chương trình đo lường an toàn thông tin có thể:

1) Chứng tỏ sự tuân thủ của một tổ chức với các yêu cầu pháp lý hoặc các quy định hiện hành và các nghĩa vụ hợp đồng;
2) Hỗ trợ xác định các vấn đề an toàn thông tin trước đó không bị phát hiện hoặc không biết;
3) Trợ giúp trong việc đáp ứng các báo cáo quản lý cần thiết khi nêu rõ các số đo cho các hành động hiện tại và từ trước đó;
4) Được sử dụng như đầu vào cho quy trình quản lý rủi ro an toàn thông tin, các đánh giá nội bộ ISMS và các soát xét của ban quản lý.

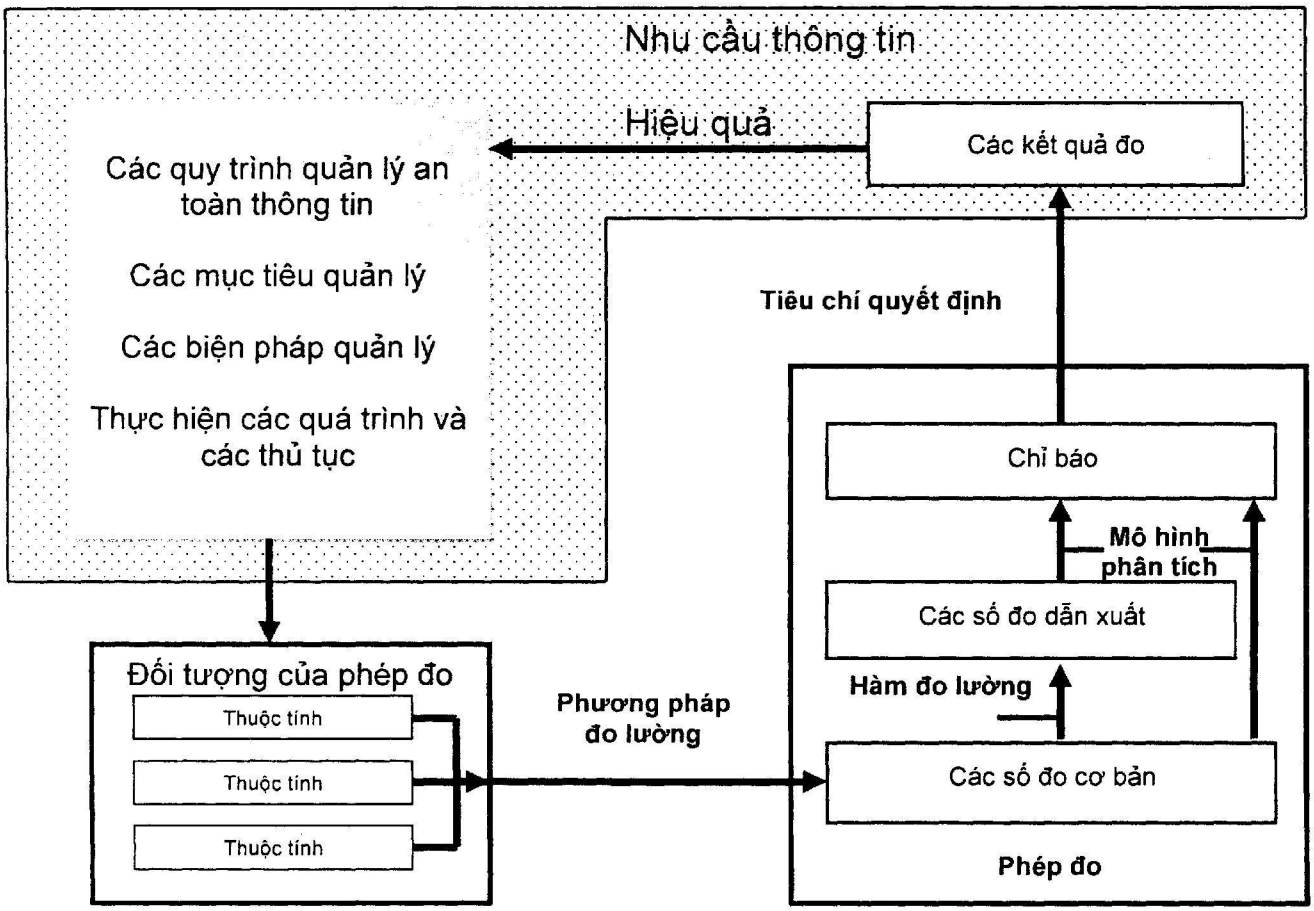
5.4 Mô hình đo lường an toàn thông tin

CHÚ THÍCH: Các khái niệm của mô hình đo lường an toàn thông tin và các cấu trúc phép đo sử dụng trong tiêu chuẩn này dựa trên những khái niệm trong ISO/IEC 15939. Thuật ngữ "sản phẩm thông tin" được sử dụng trong ISO/IEC 15939 là đồng nghĩa với "các kết quả đo" trong tiêu chuẩn này và "quy trình đo lường" được sử dụng trong ISO/IEC 15939 là đồng nghĩa với "Chương trình đo lường" trong tiêu chuẩn này.

5.4.1 Tổng quan về mô hình đo lường

Mô hình đo lường an toàn thông tin là một cấu trúc liên kết một nhu cầu thông tin tới các đối tượng có liên quan của phép đo và các thuộc tính của chúng. Đối tượng đo lường có thể bao gồm các quy trình, các thủ tục, các dự án và các nguồn lực đã lập kế hoạch hoặc đã triển khai.

Mô hình đo lường an toàn thông tin mô tả làm sao để các thuộc tính liên quan được định lượng và chuyển đổi thành các chỉ báo cung cấp cơ sở cho việc ra quyết định. Hình 2 mô tả mô hình đo lường an toàn thông tin.



Hình 2 Mô hình đo lường an toàn thông tin

CHÚ THÍCH: Điều 7 cung cấp chi tiết thông tin về các thành phần riêng của mô hình đo lường an toàn thông tin.

Các điều tiếp theo dưới đây sẽ giới thiệu về các thành phần của mô hình. Chúng cũng cung cấp các ví dụ về cách sử dụng những thành phần này.

Các nhu cầu thông tin hay mục đích của đo lường được sử dụng trong các ví dụ ở trong các Bảng 1 tới Bảng 4 của các phần sau đây là để đánh giá tình trạng nhận thức của các cá nhân có liên quan về tuân thủ các chính sách an toàn thông tin của tổ chức (Mục tiêu quản lý A.8.2 và Các biện pháp quản lý A.8.2.1 và A.8.2.2 của TCVN ISO/IEC 27001:2009).

5.4.2 Số đo cơ bản và phương pháp đo

Một số đo cơ bản là số đo đơn giản nhất có thể có được. Một số đo cơ bản là kết quả của việc áp dụng một phương pháp đo lường tới các thuộc tính được lựa chọn của một đối tượng của phép đo. Đối tượng của phép đo có thể có nhiều thuộc tính, chỉ một số trong đó có thể cung cấp các giá trị hữu ích để được gán cho một số đo cơ bản. Một thuộc tính đã cho có thể được sử dụng cho nhiều số đo cơ bản khác nhau.

Một phương pháp đo là một trình tự logic của các phép toán được sử dụng để định lượng một thuộc tính tương ứng với một thang đo xác định. Phép toán có thể bao gồm các hoạt động như đếm số lần xảy ra hay việc quan sát thời gian đã qua.

Một phương pháp đo có thể áp dụng nhiều thuộc tính cho một đối tượng đo lường. Ví dụ về một đối tượng đo lường bao gồm nhưng không giới hạn bởi:

- Khả năng của các biện pháp quản lý đã triển khai trong ISMS;
- Tình trạng của các tài sản thông tin được bảo vệ bởi các biện pháp quản lý;
- Khả năng của các quy trình đã triển khai trong ISMS;
- Hành vi của các cá nhân chịu trách nhiệm đối với ISMS đã triển khai;
- Các hoạt động của các đơn vị trong tổ chức chịu trách nhiệm về an toàn thông tin;
- Mức độ hài lòng của các bên quan tâm.

Một phương pháp đo có thể sử dụng các đối tượng đo lường của phép đo và các thuộc tính từ nhiều nguồn khác nhau, chẳng hạn như:

- Các kết quả phân tích rủi ro và đánh giá rủi ro;
- Các câu hỏi và các cuộc phỏng vấn cá nhân;
- Các báo cáo kiểm tra nội bộ hoặc từ bên ngoài;
- Các bản ghi sự kiện, như các nhật ký đăng nhập (logs), các báo cáo thống kê và các lưu vết kiểm tra;
- Các báo cáo sự cố, cụ thể là các sự cố có thể xảy ra tác động;
- Các kết quả kiểm tra, ví dụ từ thâm nhập thử nghiệm (penetration testing hay pentest), khai thác tâm lý, các công cụ đánh giá tuân thủ và các công cụ kiểm tra an toàn thông tin;
- Các bản ghi từ các thủ tục và các chương trình có liên quan tới an toàn thông tin của tổ chức, như các kết quả đào tạo về nhận thức an toàn thông tin.

Bảng 1 - 4 dưới đây trình bày các ứng dụng của mô hình an toàn thông tin cho các biện pháp quản lý sau:

- "Biện pháp quản lý 2" tham chiếu đến biện pháp quản lý A.8.2.1 Trách nhiệm của Ban quản lý trong TCVN ISO/IEC 27001:2009 ("Ban quản lý cần phải yêu cầu các cá nhân, người của nhà thầu bên thứ ba chấp hành an toàn thông tin phù hợp với các thủ tục và các chính sách an toàn thông tin đã được thiết lập của tổ chức"); được thực hiện như sau: "Tất cả cá nhân trong tổ chức có liên quan đến ISMS phải ký thỏa thuận người dùng trước khi được cấp quyền truy cập đến một hệ thống thông tin";
- "Biện pháp quản lý 1" tham chiếu đến biện pháp quản lý A.8.2.2 "Nhận thức, giáo dục và đào tạo về an toàn thông tin" trong TCVN ISO/IEC 27001:2009 ("Tất cả cá nhân của tổ chức, người

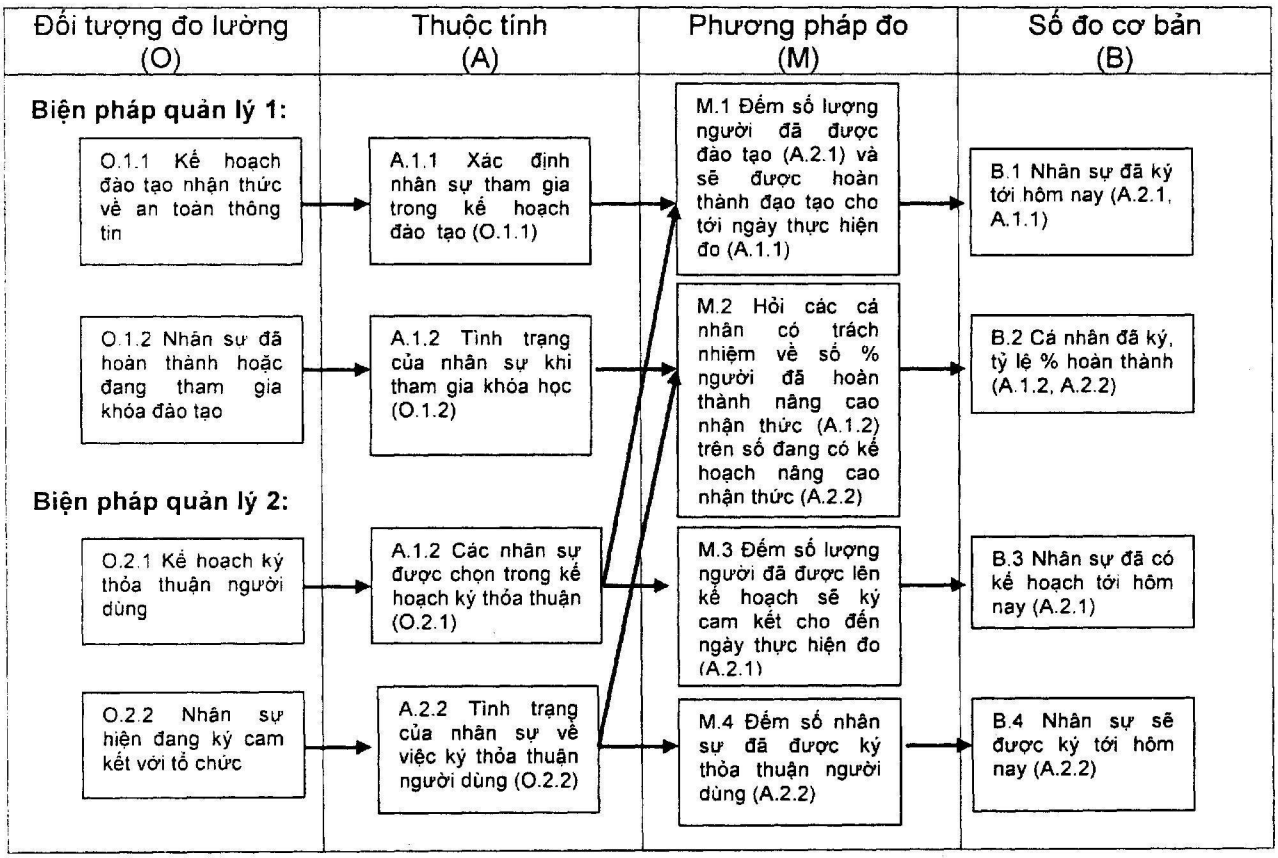
của nhà thầu và bên thứ ba phải được đào tạo nhận thức và cập nhật thường xuyên những thủ tục, chính sách đảm bảo an toàn thông tin của tổ chức như một phần công việc bắt buộc"); được thực hiện như sau: "Tất cả cá nhân liên quan đến ISMS phải được đào tạo nâng cao nhận thức an toàn thông tin trước khi được cấp quyền truy cập vào hệ thống thông tin".

Các cấu trúc phép đo tương ứng được mô tả như trong B.1.

CHÚ THÍCH: Bảng 1 - 4 bao gồm các cột khác nhau (Bảng 1 có bốn cột; Bảng 2-4 có ba cột), mỗi cột được gán một chữ cái chỉ định. Mỗi ô trong từng cột được gán một chỉ số chỉ định. Các tổ hợp chữ cái chỉ định và chữ số chỉ định được sử dụng trong các ô tiếp theo để tham chiếu đến các ô trước đó. Các mũi tên chỉ các luồng dữ liệu giữa các thành phần riêng biệt của mô hình đo lường an toàn thông tin trong các ví dụ cụ thể.

Bảng 1 bao gồm một ví dụ về các mối quan hệ giữa đối tượng của phép đo, thuộc tính, phương pháp đo và số đo cơ bản cho đo lường các đối tượng đã thiết lập cho các biện pháp quản lý đã triển khai như đã mô tả ở trên.

Bảng 1 - Ví dụ về số đo cơ bản và phương pháp đo



5.4.3 Số đo dẫn xuất và hàm đo lường

Số đo dẫn xuất là kết hợp của hai hoặc nhiều số đo cơ bản. Một số đo cơ bản có thể phục vụ như đầu vào một số số đo dẫn xuất.

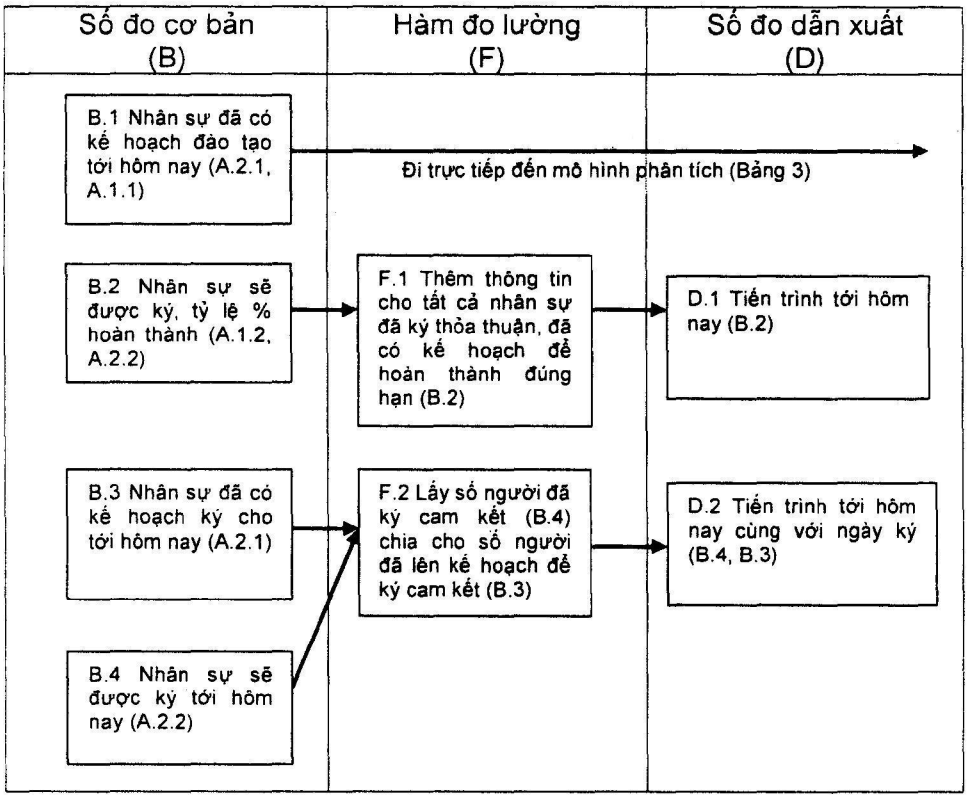
Hàm đo lường là một sự tính toán được sử dụng để kết hợp các số đo cơ bản với nhau để tạo ra số đo dẫn xuất.

Thang đo và đơn vị của số đo dẫn xuất phụ thuộc vào các thang đo và các đơn vị của các số đo cơ bản có liên quan cũng như làm thế nào chúng được kết hợp với nhau bởi các hàm đo lường.

Hàm đo lường có thể liên quan đến một loạt các kỹ thuật, chẳng hạn như tính trung bình các số đo cơ bản, áp dụng các trọng số cho các số đo cơ bản, hoặc gán các giá trị định tính cho các số đo cơ bản. Hàm đo lường có thể kết hợp các số đo cơ bản sử dụng các thang đo khác nhau, chẳng hạn như tỷ lệ phần trăm và các kết quả đánh giá định tính.

Một ví dụ về mối quan hệ của các thành phần khác của việc ứng dụng mô hình đo lường an toàn thông tin như số đo cơ bản, hàm đo lường và các số đo dẫn xuất được trình bày trong Bảng 2.

Bảng 2 - Ví dụ về số đo dẫn xuất và hàm đo lường

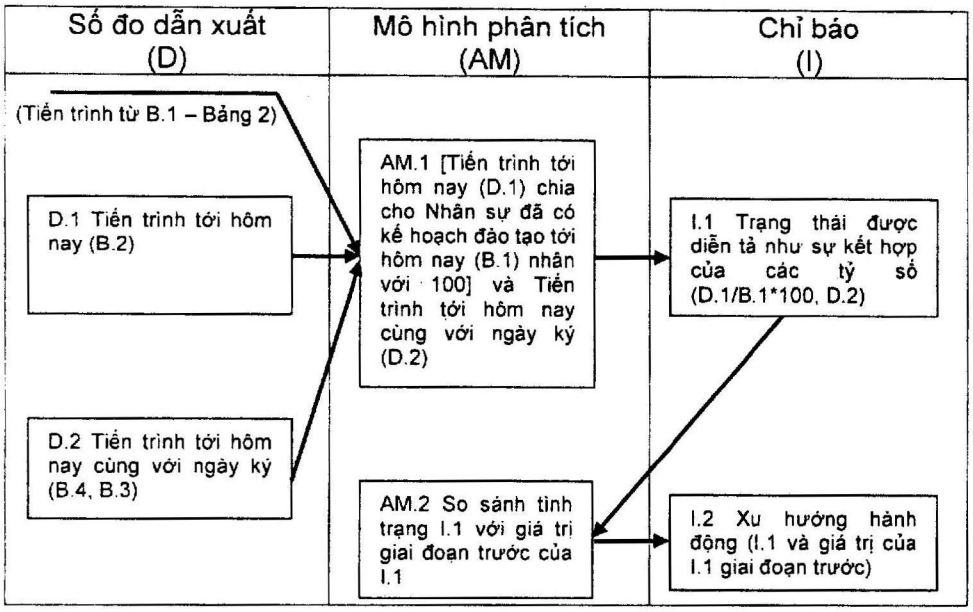


5.4.4 Chỉ báo và mô hình phân tích

Chỉ báo là một số đo cung cấp một ước đoán hoặc ước lượng các thuộc tính xác định được rút ra từ một mô hình phân tích đối với một nhu cầu thông tin cụ thể. Các chỉ báo thu được bằng cách áp dụng một mô hình phân tích cho một số đo cơ bản hay số đo dẫn xuất và kết hợp chúng với các tiêu chí quyết định. Thang đo và phương pháp đo ảnh hưởng đến sự lựa chọn của các kỹ thuật phân tích được sử dụng để tạo ra các chỉ báo.

Một ví dụ về các mối quan hệ giữa các số đo dẫn xuất, mô hình phân tích và các chỉ báo cho ứng dụng nô hình đo lường an toàn thông tin được trình bày trong Bảng 3.

Bảng 3 - Ví dụ về chỉ báo và mô hình phân tích



CHÚ THÍCH: Nếu một chỉ báo được biểu diễn dưới dạng đồ thị, biểu diễn này nên đảm bảo để người khiếm thị sử dụng được, hoặc sử dụng được khi tạo các bản sao đơn sắc. Để làm được điều này, các mô tả chỉ báo nên bao gồm các màu sắc, bóng mờ, kiểu chữ hoặc các phương pháp hiển thị khác.

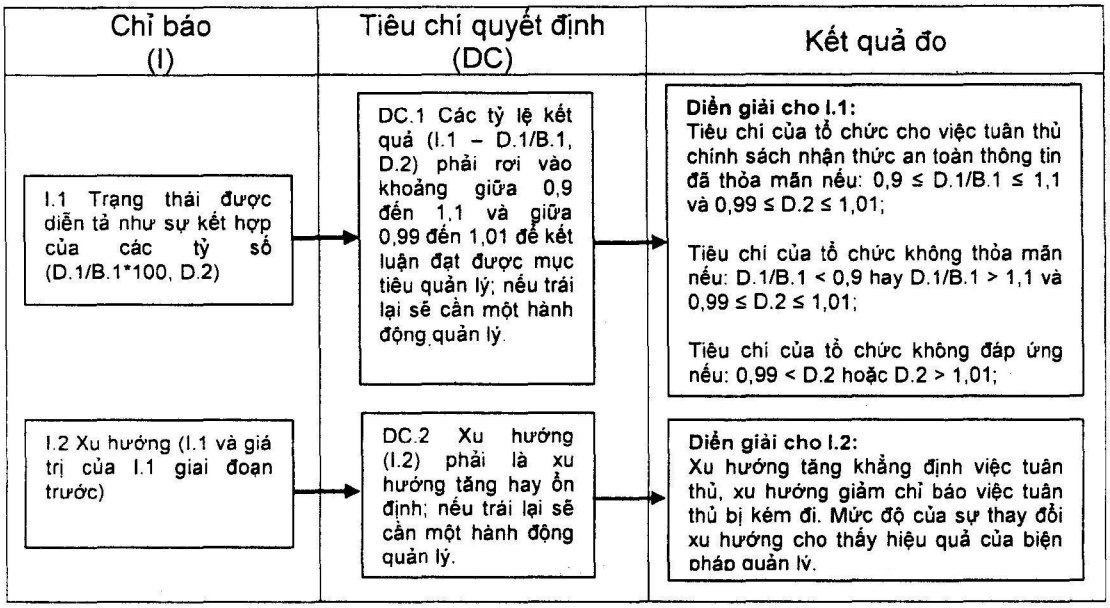
5.4.5 Kết quả đo và tiêu chí quyết định

Các kết quả đo được phát triển từ việc diễn giải các chỉ báo khả dụng dựa trên tiêu chí quyết định và nên được xem xét trong bối cảnh các mục tiêu đo lường tổng thể của việc đánh giá các hiệu lực của ISMS. Tiêu chí quyết định được sử dụng để xác định các hành động cần thiết hay các soát xét kỹ hơn, cũng như để diễn tả mức tin tưởng của kết quả đo. Tiêu chí quyết định cũng có thể được áp dụng cho một chuỗi các chỉ báo, ví dụ để thực hiện phân tích xu hướng dựa trên các chỉ báo nhận được từ những thời điểm khác nhau.

Các mục tiêu chỉ ra đặc tả chất lượng chi tiết, có thể áp dụng được cho tổ chức hay cho cả các bên liên quan, được lấy từ các đối tượng an toàn thông tin như các mục tiêu của ISMS, và các mục tiêu quản lý và cần được thiết lập và đáp ứng để đạt được các mục tiêu này.

Một ví dụ về mối quan hệ giữa các thành phần quyết định của việc áp dụng mô hình đo lường an toàn thông tin (như chỉ báo, tiêu chí quyết định và các kết quả đo) được trình bày trong Bảng 4.

Bảng 4 - Ví dụ về kết quả đo và mô hình phân tích



6 Trách nhiệm của ban quản lý

6.1 Giới thiệu chung

Ban quản lý chịu trách nhiệm xây dựng Chương trình đo lường an toàn thông tin (ISMP), có liên quan tới nhiều bên khác nhau (xem 7.5.8) trong các hoạt động đo, chấp nhận các kết quả đo như số liệu đầu vào của quy trình soát xét của ban quản lý và sử dụng kết quả đo trong các hoạt động cải tiến trong ISMS.

Để có được những điều trên, ban quản lý nên:

a) Thiết lập các mục tiêu cho ISMP;

b) Thiết lập chính sách cho ISMP;

c) Thiết lập các vai trò và trách nhiệm cho ISMP;

d) Cung cấp các nguồn lực phù hợp để thực hiện đo lường bao gồm nhân lực, ngân quỹ, các công cụ và cơ sở hạ tầng;

e) Đảm bảo rằng các mục tiêu của ISMP là đạt được;

f) Đảm bảo rằng các công cụ và thiết bị được sử dụng để thu thập dữ liệu được bảo dưỡng hợp lý;

g) Thiết lập các mục đích đo lường cho từng cấu trúc phép đo;

h) Đảm bảo rằng phép đo cung cấp đủ các thông tin cho các bên liên quan về hiệu lực của ISMS và nhu cầu cải tiến ISMS đã triển khai, bao gồm phạm vi, các chính sách, các mục tiêu, các biện pháp quản lý, các quy trình và các thủ tục;

i) Đảm bảo rằng phép đo mang lại đủ thông tin cho các bên liên quan về hiệu lực của các biện pháp quản lý hay nhóm biện pháp quản lý và nhu cầu cải tiến những biện pháp quản lý đã triển khai.

Ban quản lý nên đảm bảo các kết quả đo không bị chi phối bởi chính người sở hữu thông tin (xem 7.5.8) thông qua việc gán các vai trò và trách nhiệm. Điều này có thể có được thông qua việc chia tách các nhiệm vụ, hay nếu điều này là không thể thì thông qua việc sử dụng các tài liệu chi tiết mà cho phép kiểm tra độc lập.

6.2 Quản lý nguồn lực

Ban quản lý nên phân chia và cung cấp các nguồn lực để hỗ trợ các hoạt động cần thiết trong đo lường, như việc thu thập dữ liệu, phân tích, lưu trữ, lập báo cáo và phát hành. Việc phân bổ nguồn lực sẽ bao gồm việc chỉ định:

a) Những người có trách nhiệm liên quan đến mọi khía cạnh của Chương trình đo lường an toàn thông tin;

b) Hỗ trợ nguồn tài chính phù hợp;

c) Hỗ trợ cơ sở hạ tầng phù hợp, như cơ sở hạ tầng vật lý và các công cụ sử dụng để thực hiện quy trình đo lường.

CHÚ THÍCH: Điều 5.2.1 của TCVN ISO/IEC 27001:2009 xác định yêu cầu trong việc cung cấp các nguồn lực cho việc triển khai và hoạt động của ISMS.

6.3 Tập huấn, nhận thức và năng lực về đo lường

Ban quản lý nên đảm bảo rằng:

a) Các bên liên quan (xem 7.5.8) được đào tạo tương xứng với vai trò và trách nhiệm của họ trong việc thực thi Chương trình đo lường an toàn thông tin và có chất lượng phù hợp để thực hiện các vai trò và trách nhiệm của họ.

b) Các bên liên quan hiểu rằng nhiệm vụ của họ bao gồm việc đưa ra các đề xuất cho việc cải tiến trong Chương trình đo lường an toàn thông tin đã triển khai.

7 Phát triển các số đo và phép đo

7.1 Giới thiệu chung

Phần này cung cấp hướng dẫn trong việc làm sao để phát triển các số đo và phép đo nhằm mục đích đánh giá hiệu lực của ISMS đã triển khai và các biện pháp quản lý hay nhóm các biện pháp quản lý và việc xác định các bộ cấu trúc phép đo cụ thể cho tổ chức. Các hành động cần để phát triển các số đo và phép đo nên được xây dựng và lập thành tài liệu, bao gồm những nội dung sau:

a) Xác định phạm vi của phép đo (xem 7.2);

b) Nhận dạng nhu cầu thông tin (xem 7.3);

c) Lựa chọn mục tiêu của phép đo và các thuộc tính của nó (xem 7.4);

d) Phát triển cấu trúc của phép đo (xem 7.5);

e) Ứng dụng cấu trúc bài đo (xem 7.6);

f) Thiết lập cách thu thập dữ liệu và các quy trình phân tích dữ liệu và các công cụ (xem 7.7);

g) Thiết lập cách tiếp cận thực hiện phép đo và tài liệu hướng dẫn (xem 7.8).

Khi thiết lập các hoạt động này, tổ chức cần tính đến các nguồn lực tài chính, nhân lực và cơ sở hạ tầng (môi trường vật lý và các công cụ).

7.2 Xác định phạm vi đo lường

Tùy thuộc vào khả năng và nguồn lực của tổ chức, phạm vi ban đầu của các hoạt động đo lường của tổ chức sẽ được giới hạn ở những biện pháp quản lý cụ thể, các tài sản thông tin được bảo vệ bởi các biện pháp quản lý cụ thể, các hành động cụ thể cho an toàn thông tin đã được xác định mức ưu tiên cao nhất bởi ban quản lý. Theo thời gian, phạm vi của các hoạt động đo lường sẽ được mở rộng cho nhiều thành phần hơn của ISMS đã triển khai và các biện pháp quản lý hay nhóm các biện pháp quản lý, có xem xét tới mức ưu tiên cảu các bên tham gia đo lường.

Các bên liên quan nên được xác định và tham gia vào việc xác định phạm vi đo lường. Các bên liên quan có thể là trong nội bộ hoặc bên ngoài của các đơn vị tổ chức, như giám đốc dự án, giám đốc hệ thống thông tin hoặc người quyết định an toàn thông tin. Những kết quả đo cụ thể dành cho hiệu lực của các biện pháp quản lý riêng hay của nhóm các biện pháp quản lý nên được xác định và được trao đổi tới các bên liên quan.

Tổ chức có thể xem xét việc giới hạn một số kết quả đo để thông báo tới người quyết định trong một giai đoạn thời gian đã định để đảm bảo khả năng của chúng tác động tới việc cải tiến ISMS dựa trên các kết quả đo đã được báo cáo. Một số lượng kết quả đo vượt quá mức sẽ ảnh hưởng đến khả năng của người ra quyết định trong việc ưu tiên và chú trọng vào các hành động cải tiến hệ thống trong tương lai. Các kết quả đo phải được ưu tiên dựa trên mức độ quan trọng của nhu cầu thông tin tương ứng và các mục tiêu ISMS liên quan.

CHÚ THÍCH: Phạm vi phép đo liên quan tới phạm vi của ISMS đã thiết lập theo 4.2.1 a) của TCVN ISO/IEC 27001:2009.

7.3 Xác định nhu cầu thông tin

Mỗi cấu trúc phép đo nên tương ứng tới ít nhất một nhu cầu thông tin. Một ví dụ về nhu cầu thông tin, diễn tả bắt đầu từ mục đích của phép đo và kết thúc là các tiêu chí quyết định liên quan, được biểu diễn trong Phụ lục A.

Các hành động sau cần được thực hiện để xác định các nhu cầu thông tin liên quan:

a) Kiểm tra ISMS và các quy trình của nó, như:

1) Chính sách và các mục tiêu của ISMS, các mục tiêu quản lý và các biện pháp quản lý;

2) Các yêu cầu của luật pháp, quy định và hợp đồng liên quan và các yêu cầu tổ chức cho an toàn thông tin;

3) Các kết quả của quá trình quản lý rủi ro an toàn thông tin, như được mô tả trong TCVN ISO/IEC 27001:2009.

b) Chọn mức ưu tiên các nhu cầu thông tin đã xác định dựa trên tiêu chí, như:

1) Các mức ưu tiên xử lý rủi ro;

2) Khả năng và nguồn lực của tổ chức;

3) Sự quan tâm của các bên liên quan;

4) Chính sách an toàn thông tin;

5) Thông tin được yêu cầu để đáp ứng các yêu cầu của pháp luật, quy định và hợp đồng liên quan;

6) Giá trị của thông tin trong mối liên quan với chi phí của phép đo;

c) Chọn một nhóm thông tin cần được giải quyết trong các hành động đo lường căn cứ vào danh sách mức ưu tiên;

d) Lập tài liệu và trao đổi các nhu cầu thông tin đã được chọn cho các bên liên quan.

Tất cả các số đo liên quan áp dụng cho ISMS đã triển khai, các biện pháp quản lý hay nhóm các biện pháp quản lý nên được triển khai trên cơ sở các nhu cầu thông tin đã được chọn.

7.4 Lựa chọn đối tượng và thuộc tính

Một đối tượng đo lường và các thuộc tính của nó nên được xác định trong bối cảnh tổng thể và phạm vi của ISMS. Cần lưu ý rằng một đối tượng đo lường có thể có nhiều thuộc tính.

Đối tượng và thuộc tính của nó được sử dụng bởi số đo nên được chọn dựa trên mức ưu tiên của các nhu cầu thông tin tương ứng.

Các giá trị gán cho một số đo cơ bản liên quan có được bằng việc áp dụng phương pháp đo phù hợp cho các thuộc tính được lựa chọn. Việc lựa chọn này nên đảm bảo rằng:

- Các số đo cơ bản liên quan và phương pháp đo thích hợp được xác định;
- Các kết quả đo có nhiều ý nghĩa có thể được phát triển dựa trên các giá trị thu được và các số đo đã phát triển.

Các đặc tính của các thuộc tính được chọn quyết định loại phương pháp đo nào cần được sử dụng để thu được các giá trị để gán cho các số đo cơ bản (cả về định tính hay về định lượng).

Đối tượng được lựa chọn và các thuộc tính nên được lập thành tài liệu, cùng với các lý do của việc lựa chọn.

Dữ liệu mô tả đối tượng của phép đo và các thuộc tính tương ứng nên được sử dụng như các giá trị để gán cho các số đo cơ bản. Ví dụ về các đối tượng của phép đo bao gồm nhưng không bị giới hạn trong:

- Các sản phẩm và các dịch vụ;
- Các quy trình;
- Các tài sản khả dụng như các phương tiện, các ứng dụng và các hệ thống thông tin như được xác định trong TCVN ISO/IEC 27001:2009 (Kiểm kê tài sản, A.7.1.1);
- Các ban nghiệp vụ;
- Các chi nhánh;
- Các dịch vụ bên thứ ba.

Các thuộc tính nên được xem xét để đảm bảo rằng:

a) Các thuộc tính đã được chọn cho phép đo là phù hợp;

b) Việc thu thập dữ liệu đã được xác định để đảm bảo đủ số lượng các thuộc tính để đạt được bài đo hiệu quả.

Chỉ các thuộc tính có liên quan tới các số đo cơ bản tương ứng mới được lựa chọn. Mặc dù việc lựa chọn các thuộc tính cần cân nhắc đến mức độ khó trong việc thu được các thuộc tính cho phép đo, việc lựa chọn thuộc tính không nên chỉ trên cơ sở dễ dàng lấy được dữ liệu hay dễ dàng đo lường thuộc tính.

7.5 Phát triển cấu trúc phép đo

7.5.1 Giới thiệu chung

Mục 7.5 này chỉ rõ về sự phát triển cấu trúc phép đo từ 7.5.2 (lựa chọn số đo) tới 7.5.8 (các bên liên quan).

7.5.2 Lựa chọn số đo

Các số đo có khả năng thỏa mãn nhu cầu thông tin đã chọn nên được xác định. Các số đo đã xác định nên được định nghĩa đủ chi tiết để cho việc lựa chọn các số đo là thực hiện được. Các số đo mới được xác định có thể tương thích với số đo đã có.

CHÚ THÍCH: Việc xác định của các số đo cơ bản có liên quan chặt chẽ với việc xác định các đối tượng của phép đo và các thuộc tính của chúng.

Các số đo đã xác định có khả năng thỏa mãn nhu cầu thông tin đã chọn nên được lựa chọn. Thông tin về bối cảnh cần thiết để diễn giải hoặc đơn giản hóa các số đo cũng nên được xác định.

CHÚ THÍCH: Nhiều sự kết hợp khác nhau của các số đo (như các số đo cơ bản, các số đo dẫn xuất và các chỉ báo) có thể được lựa chọn để giải quyết một nhu cầu thông tin cụ thể.

Các số đo được chọn cần phản ánh mức ưu tiên của các nhu cầu thông tin. Các tiêu chí mẫu có thể được sử dụng cho việc lựa chọn của các số đo bao gồm:

- Việc dễ dàng thu thập dữ liệu;
- Khả năng sẵn sàng của nguồn nhân lực để thu thập và quản lý dữ liệu;
- Khả năng sẵn sàng của các công cụ phù hợp;
- Số các chỉ báo tiềm năng liên quan đã được hỗ trợ bởi số đo cơ bản;
- Việc dễ dàng diễn giải;
- Số người sử dụng các kết quả đo đã tiến hành;
- Bằng chứng về sự phù hợp của số đo với mục đích hay các nhu cầu thông tin;
- Chi phí để thu thập, quản lý và phân tích dữ liệu.

7.5.3 Phương pháp đo

Đối với mỗi số đo cơ bản nên có một phương pháp đo xác định. Phương pháp đo này được sử dụng để định lượng một đối tượng đo lường thông qua việc chuyển đổi các thuộc tính thành giá trị để được gán vào số đo cơ bản.

Một phương pháp đo có thể là chủ quan hay khách quan. Các phương pháp chủ quan dựa trên việc định lượng liên quan tới chủ định của con người, trong khi phương pháp khách quan sử dụng việc định lượng dựa trên các quy tắc số học như việc đếm mà có thể được thực hiện thông qua con người hay các phương tiện máy móc tự động.

Phương pháp đo định lượng các thuộc tính thành các giá trị bằng việc áp dụng một thang đo đo phù hợp. Mỗi thang đo sử dụng các đơn vị đo lường. Chỉ những số lượng được diễn tả trong cùng một đơn vị của đo lường được so sánh trực tiếp với nhau.

Quy trình xác minh đối với mỗi phương pháp đo nên được thiết lập và lập thành tài liệu. Việc xác minh này nên đảm bảo một mức độ tin cậy cho giá trị có được bằng việc áp dụng phương pháp đo đối với một thuộc tính của đối tượng của phép đo và được gán cho một số đo cơ bản. Nếu cần khẳng định tính hợp lệ của giá trị, các công cụ đã được sử dụng để có được các thuộc tính nên được chuẩn hóa và được kiểm định sau các khoảng thời gian xác định.

Độ chính xác của phương pháp đo nên được tính đến và các độ lệch hay sự thay đổi liên quan phải được ghi lại.

Một phương pháp đo nên nhất quán theo thời gian sao cho các giá trị đã gán cho một số đo cơ bản tại những thời điểm khác nhau là tương xứng và các giá trị đã gán cho một số đo dẫn xuất và một chỉ báo cũng là tương xứng.

7.5.4 Hàm đo lường

Với mỗi số đo dẫn xuất riêng biệt, một hàm đo lường nên được xác định và được áp dụng cho hai hay nhiều giá trị được gán cho các số đo cơ bản. Hàm đo lường được sử dụng để chuyển giá trị đã được

gán cho một hay nhiều số đo cơ bản về giá trị để gán cho một số đo dẫn xuất. Trong một số trường hợp, một số đo cơ bản cũng có thể góp phần trực tiếp cho mô hình phân tích để bổ sung cho một số đo dẫn xuất.

Một hàm đo lường (ví dụ một phép tính toán) có thể bao gồm nhiều kỹ thuật, như lấy trung bình cộng các giá trị được gán cho các số đo cơ bản, áp dụng các trọng số cho các giá trị được gán cho các số đo cơ bản, hoặc gán các giá trị định tính cho các giá trị đã được gán cho các số đo cơ bản trước khi kết hợp chúng vào thành giá trị để gán cho một số đo dẫn xuất. Hàm đo lường có thể kết hợp các giá trị đã được gán cho các số đo cơ bản sử dụng các thang đo khác nhau, như tỷ lệ phần trăm và các kết quả đánh giá định tính.

7.5.5 Mô hình phân tích

Với mỗi chỉ báo, một mô hình phân tích nên được xác định nhằm mục đích chuyển đổi một hay nhiều giá trị đã ấn định cho một số đo cơ bản hay số đo dẫn xuất thành giá trị để được gán cho chỉ báo.

Mô hình phân tích kết hợp các số đo liên quan để cho ra một kết quả có ý nghĩa đối với các bên liên quan.

Tiêu chí quyết định được áp dụng cho một chỉ báo cũng nên được xét đến khi xác định mô hình phân tích.

Đôi khi một mô hình phân tích có thể chỉ đơn giản như việc chuyển đổi một giá trị đơn gán cho một số đo dẫn xuất sang giá trị để gán cho một chỉ báo.

7.5.6 Các chỉ báo

Các giá trị được gán cho các chỉ báo sẽ được tạo ra bằng cách kết hợp các giá trị đã được gán cho số đo dẫn xuất và diễn giải những giá trị này dựa trên các tiêu chí quyết định. Đối với mỗi chỉ báo sẽ được thông báo tới người yêu cầu đo, một bản định dạng cho biểu diễn các chỉ báo như một phần của bản định dạng báo cáo (xem 7.7) nên được xác định.

Các bản định dạng cho biểu diễn các chỉ báo sẽ mô tả trực quan các số đo và cung cấp một giải thích bằng lời cho các chỉ báo. Các bản định dạng cho biểu diễn các chỉ báo nên được tùy biến để đáp ứng nhu cầu thông tin của bên nhận.

7.5.7 Tiêu chí quyết định

Tiêu chí quyết định tương ứng với mỗi chỉ báo nên được xác định và được lập thành tài liệu dựa trên các mục tiêu an toàn thông tin, để đưa ra hướng dẫn khả thi cho các bên liên quan. Hướng dẫn này nên chỉ rõ những mong muốn về tiến trình và các ngưỡng cho khởi đầu các hành động cải tiến dựa trên chỉ báo này.

Tiêu chí quyết định tạo ra một mục đích mà qua đó sự thành công (xem 5.3) được đánh giá và cung cấp hướng dẫn về việc diễn giải các chỉ báo liên quan tới sự tiếp cận mục đích đó.

Các mục đích cần được thiết lập cho từng hạng mục về khả năng của các quy trình ISMS và các biện pháp quản lý, việc đạt được các mục tiêu và hiệu lực của ISMS được ước lượng.

Ban quản lý có thể quyết định không thiết lập các mục đích cho các chỉ báo cho tới khi dữ liệu khởi đầu được thu thập. Một khi các hành động khắc phục dựa trên dữ liệu khởi đầu được xác định, các tiêu chí quyết định phù hợp và các mốc triển khai có thể được định nghĩa và thiết thực cho một ISMS xác định. Nếu tiêu chí quyết định không thể được thiết lập tại điểm đó, ban quản lý nên ước lượng xem đối tượng đo và các số đo tương ứng có cung cấp giá trị như đã mong muốn cho tổ chức hay không.

Việc thiết lập tiêu chí quyết định có thể thuận tiện nếu có dữ liệu lịch sử gắn với các số đo đã xây dựng hoặc lựa chọn. Các xu hướng đã được quan sát trong quá khứ sẽ cung cấp nhận thức rõ hơn vào trong phạm vi của các hoạt động đã tồn tại trước đó và hướng dẫn việc đưa ra các tiêu chí quyết định có tính thực tế. Tiêu chí quyết định có thể được rút ra từ các dữ liệu trước đó, từ các dự án tương tự, từ kinh nghiệm hoặc được tính toán như các giới hạn kiểm soát theo thống kê hoặc giới hạn về sự tin cậy thống kê.

7.5.8 Các bên liên quan

Với mỗi số đo cơ bản/ số đo dẫn xuất, các bên liên quan thích hợp nên được xác định và lập thành tài liệu. Các bên liên quan có thể bao gồm:

a) Người yêu cầu đo: Ban quản lý hay các bên quan tâm yêu cầu hay mong muốn thông tin về hiệu lực của một ISMS, các biện pháp quản lý hay nhóm các biện pháp quản lý;

b) Người soát xét phép đo: cá nhân hay đơn vị tổ chức kiểm tra tính hợp lệ và xác định các cấu trúc của phép đo đã tiến hành là phù hợp cho việc đánh giá hiệu lực của ISMS, các biện pháp quản lý hay nhóm các biện pháp quản lý;

c) Người sở hữu thông tin: cá nhân hay một đơn vị tổ chức sở hữu thông tin về một đối tượng đo lường và các thuộc tính và chịu trách nhiệm về đo lường đó;

d) Bộ phận thu thập thông tin: cá nhân hay tổ chức chịu trách nhiệm trong việc thu thập, ghi chép, lưu trữ dữ liệu;

e) Bộ phận trao đổi thông tin: cá nhân hay tổ chức chịu trách nhiệm cho việc phân tích dữ liệu và trao đổi các kết quả đo.

7.6 Cấu trúc phép đo

Về tối thiểu, đặc tả kỹ thuật về cấu trúc phép đo lường nên bao gồm những thông tin sau:

a) Mục đích của phép đo;

b) Mục tiêu quản lý đạt được từ các biện pháp quản lý, các biện pháp quản lý đặc trưng, nhóm các biện pháp quản lý và quy trình của ISMS được đo;

c) Đối tượng của phép đo;

d) Dữ liệu cần được thu thập và sử dụng;

e) Quy trình cho việc thu thập và phân tích;

f) Quy trình cho việc lập báo cáo kết quả đo, gồm cả các định dạng báo cáo đo;

g) Vai trò và trách nhiệm của các bên liên quan;

h) Chu kỳ cho việc soát xét đo lường để đảm bảo tính hữu dụng của chúng trong mối quan hệ với nhu cầu thông tin.

Phụ lục A đưa ra một ví dụ về cấu trúc chung của phép đo kết hợp các điểm a) tới h). Phụ lục B cung cấp những ví dụ về cấu trúc các phép đo cụ thể được áp dụng để đánh giá quy trình ISMS và các biện pháp quản lý.

7.7 Thu thập, phân tích dữ liệu và lập báo cáo kết quả đo

Các thủ tục cho việc thu thập, phân tích dữ liệu và các quy trình cho việc lập báo cáo kết quả đo đã tiến hành nên được thiết lập. Những công cụ hỗ trợ, thiết bị và công nghệ đo kiểm cũng nên được thiết lập, nếu được yêu cầu. Những thủ tục, công cụ, thiết bị và công nghệ đo kiểm này được đề cập trong những bước sau:

a) Thu thập dữ liệu, bao gồm lưu trữ và xác minh dữ liệu (xem 8.3). Các thủ tục nên xác định cách thức dữ liệu được thu thập bằng việc sử dụng phương pháp đo, hàm đo lường và mô hình phân tích, cũng như cách thức và vị trí chúng sẽ được lưu trữ cùng với mọi thông tin về ngữ cảnh cần thiết để hiểu và xác minh dữ liệu. Việc xác minh dữ liệu có thể được thực hiện bằng việc kiểm tra dữ liệu dựa vào danh sách kiểm tra đã được cấu trúc để xác minh rằng dữ liệu thiếu là ít nhất và giá trị đã gán cho mỗi số đo là hợp lệ;

   CHÚ THÍCH: Việc xác minh các giá trị được gán cho các số đo cơ bản có liên quan gần gũi với việc xác minh phương pháp đo lường (xem 7.5.3).

b) Phân tích dữ liệu và lập báo cáo kết quả đo đã tiến hành. Các thủ tục cần chỉ rõ các kỹ thuật phân tích dữ liệu (xem 9.2), tần suất, định dạng và các phương pháp lập báo cáo kết quả đo. Những loại công cụ có thể cần thiết để thực hiện phân tích dữ liệu cũng nên được xác định.

Các ví dụ về định dạng báo cáo kết quả đo bao gồm:

- Các bảng ghi điểm để cung cấp thông tin chiến lược bằng cách tích hợp các chỉ báo mức cao;
- Các bảng chỉ số thực thi và tính toán ít tập trung vào các mục tiêu chiến lược và gắn nhiều hơn với hiệu lực của các biện pháp quản lý và quy trình cụ thể;
- Các báo cáo, từ dạng đơn giản và tĩnh như là danh sách của các số đo trong một khoảng thời gian đã định, đến phức tạp như báo cáo với các thông tin tóm tắt ở các nhóm lồng nhau và các thông tin chuyên sâu hay các đường liên kết động. Những báo cáo đo được sử dụng tốt nhất khi người sử dụng cần xem dữ liệu thô ở dạng dễ đọc;
- Các mức đo biểu diễn các giá trị động bao gồm các cảnh báo, các thành phần đồ thị và các nhãn biểu diễn điểm mốc.

7.8 Triển khai đo lường và xây dựng tài liệu đo

Phương pháp tiếp cận đo lường tổng thể nên được lập thành tài liệu trong một kế hoạch triển khai. Kế hoạch triển khai này nên bao gồm các thông tin tối thiểu sau:

a) Triển khai Chương trình đo lường an toàn thông tin ISMP cho tổ chức;

b) Đặc tả về đo lường bao gồm:

1) Cấu trúc đo lường chung cho tổ chức;

2) Cấu trúc đo lường riêng cho tổ chức;

3) Định nghĩa dải giá trị và các thủ tục cho việc thu thập và phân tích dữ liệu;

c) Kế hoạch thời gian để thực hiện các hoạt động đo lường;

d) Các bản ghi được tạo thông qua thực hiện các hoạt động đo, bao gồm dữ liệu đã được thu thập và các bản ghi phân tích;

e) Các định dạng báo cáo kết quả đo sẽ được báo cáo tới ban quản lý/ các bên liên quan (xem ISO/IEC 27001:2005 Điều 7 "Soát xét của ban quản lý").

8 Hoạt động đo lường

8.1 Giới thiệu chung

Hoạt động đo lường an toàn thông tin liên quan tới các hoạt động cần thiết để đảm bảo các kết quả đo đã triển khai cung cấp thông tin chính xác liên quan đến hiệu lực của ISMS đã triển khai, các biện pháp quản lý hay nhóm biện pháp quản lý và sự cần thiết của các hành động cải tiến phù hợp.

Các hoạt động này bao gồm:

a) Tích hợp các thủ tục đo lường vào tất cả các hoạt động của ISMS;

b) Thu thập, lưu trữ và xác minh dữ liệu.

8.2 Tích hợp các thủ tục

Chương trình đo lường an toàn thông tin cần được tích hợp toàn diện vào trong ISMS và được sử dụng bởi ISMS. Các thủ tục đo lường cần được kết hợp với hoạt động của ISMS bao gồm:

a) Định nghĩa và tài liệu về các vai trò, thẩm quyền và trách nhiệm, xu thế phát triển, khả năng triển khai và việc duy trì đo lường an toàn thông tin;

b) Thu thập dữ liệu, và nếu cần hiệu chỉnh những hoạt động hiện hành của ISMS liên quan đến các hoạt động tạo và thu thập dữ liệu;

c) Trao đổi về những thay đổi trong hoạt động thu thập dữ liệu cho các bên liên quan;

d) Việc duy trì khả năng của Bộ phận thu thập thông tin và sự hiểu biết về các loại dữ liệu yêu cầu, công cụ thu thập dữ liệu và các trình tự thu thập dữ liệu;

e) Việc phát triển các chính sách và các thủ tục xây dựng các quy định việc sử dụng phép đo trong tổ chức, việc công bố các thông tin đo lường, việc đánh giá và soát sét Chương trình đo lường an toàn thông tin;

f) Tích hợp phân tích dữ liệu và lập báo cáo đo vào trong các quy trình liên quan để đảm bảo các hoạt động được diễn ra theo đúng khả năng;

g) Việc giám sát, soát xét và ước lượng các kết quả đo;

h) Việc thiết lập một quy trình cho những lần đo và bổ sung những lần đo mới để đảm bảo rằng những đợt đo luôn được thực hiện trong tổ chức;

i) Việc thiết lập của một quy trình nhằm xác định thời hạn hữu dụng của những dữ liệu trong quá khứ để làm cơ sở cho xác định xu hướng phân tích trong giai đoạn tiếp theo.

8.3 Thu thập, lưu trữ và xác minh dữ liệu

Thu thập, lưu trữ và xác minh dữ liệu bao gồm các hoạt động sau:

a) Thu thập dữ liệu yêu cầu trong những khoảng thời gian đều đặn sử dụng một phương pháp đo đã chỉ định;

b) Lập tài liệu thu thập dữ liệu, bao gồm:

1) Ngày tháng, thời gian và vị trí thu thập dữ liệu;

2) Bộ phận thu thập thông tin;

3) Người sở hữu thông tin;

4) Thông tin tranh cãi hữu dụng nảy sinh trong quá trình thu thập dữ liệu;

5) Thông tin dùng cho việc xác minh dữ liệu và tính hợp lệ đo lường.

c) Xác minh dữ liệu đã thu thập dựa trên tiêu chí lựa chọn số đo và tiêu chí hợp lệ cấu trúc phép đo.

Dữ liệu đã thu thập và mọi thông tin về bối cảnh cần thiết nên được kết hợp và lưu trữ trong các báo cáo đo để làm cơ sở cho phân tích dữ liệu.

9 Phân tích dữ liệu và lập báo cáo kết quả đo

9.1 Giới thiệu chung

Dữ liệu đã thu thập nên được phân tích để phát triển các kết quả đo và các kết quả đo được phát triển nên được thông báo tới các bên liên quan.

Hành động này bao gồm như sau:

a) Phân tích dữ liệu và việc phát triển kết quả đo;

b) Thông báo các kết quả đo tới các bên liên quan.

9.2 Phân tích dữ liệu và phát triển các kết quả đo

Dữ liệu thu thập được nên được phân tích và chuyển sang dạng tiêu chí quyết định. Dữ liệu này có thể được gộp lại, chuyển đổi hoặc giải mã trước khi phân tích. Trong quá trình này, dữ liệu nên được xử lý để xuất ra bộ chỉ báo. Một số kỹ thuật phân tích có thể được áp dụng. Độ sâu phân tích nên được quyết định bởi bản chất của dữ liệu và các nhu cầu thông tin.

CHÚ THÍCH: Việc hướng dẫn cho việc thực hiện phân tích thống kê có thể tìm thấy trong ISO/TR 10017 (Hướng dẫn về các kỹ thuật thống kê cho ISO 9001).

Các kết quả phân tích dữ liệu nên được diễn giải. Người phân tích kết quả (bộ phận trao đổi thông tin) nên có khả năng đưa ra một số kết luận bước đầu dựa trên các kết quả đo. Tuy nhiên, do bộ phận trao đổi thông tin có thể không trực tiếp liên quan vào quy trình quản lý và kỹ thuật, những kết luận này cần được soát xét bởi các bên liên quan khác. Tất cả những diễn giải nên tính đến bối cảnh đo lường.

Việc phân tích dữ liệu nên xác định ra những khác biệt giữa các kết quả đo thực tế và kết quả mong muốn của hệ thống ISMS đã triển khai. Những khác biệt đã được xác định sẽ chỉ ra những điểm cần thiết cho việc cải tiến ISMS đã triển khai, bao gồm phạm vi, các chính sách, các mục tiêu, các biện pháp quản lý, các quy trình và các thủ tục.

Những chỉ báo thể hiện sự không tuân thủ hay khả năng thực hiện kém cần được nhận ra và được phân loại như sau:

a) Kế hoạch xử lý rủi ro không thực hiện hoặc thực hiện không thích đáng, các hoạt động và quản lý các biện pháp quản lý hay những quy trình ISMS (ví dụ các biện pháp quản lý và các quy trình ISMS có thể bỏ qua bởi những cảnh báo);

b) Lỗi đánh giá rủi ro:

   1) Các biện pháp quản lý hay các quy trình của ISMS là không hiệu quả bởi vì chúng không đủ để đối phó với những nguy cơ đã ước tính được những cảnh báo (ví dụ như khả năng xảy ra nguy cơ đã được đánh giá thấp); hoặc đối phó với những nguy cơ mới;

   2) Các biện pháp quản lý hay các quy trình của ISMS không được thực thi, bởi vì những cảnh báo đã không nhận thấy.

Những báo cáo được sử dụng để thông báo các kết quả của đo lường tới các bên liên quan nên được chuẩn bị sử dụng các định dạng báo cáo phù hợp (xem 7.7) tuân theo kế hoạch triển khai Chương trình đo lường an toàn thông tin.

Những kết luận của việc phân tích cần được soát xét bởi các bên liên quan để đảm bảo diễn giải phù hợp với dữ liệu đo. Các kết quả của việc phân tích dữ liệu cần được lập thành tài liệu để thông báo tới các bên liên quan.

9.3 Trao đổi các kết quả đo

Bộ phận trao đổi thông tin nên quyết định cách thức thông báo các kết quả đo an toàn thông tin, như sau:

- Những kết quả đo nào là được thông báo trong nội bộ hay ra ngoài;
- Lập danh sách những số đo tương ứng với từng bên liên quan, những bên quan tâm;
- Các kết quả đo cụ thể cần được cung cấp và thể thức trình bày theo nhu cầu của từng nhóm;
- Cách thức thu nhận các thông tin phản hồi từ các bên liên quan được sử dụng cho việc ước lượng tính hiệu dụng của các kết quả đo và hiệu lực của Chương trình đo lường an toàn thông tin.

Các kết quả đo lường nên được thông báo tới nhiều bên liên quan trong nội bộ, bao gồm nhưng không hạn chế trong:

- Những người yêu cầu đo (xem 7.5.8);
- Những người sở hữu thông tin (xem 7.5.8);
- Người phụ trách quản lý rủi ro an toàn thông tin, đặc biệt tại nơi các lỗi về đánh giá rủi ro được xác định;
- Người có trách nhiệm đối với những khu vực đã xác định có nhu cầu cải tiến.

Tổ chức trong một số trường hợp có thể được yêu cầu phân phát báo cáo các kết quả đo tới các đối tác bên ngoài, bao gồm các cơ quan quản lý, các bên liên quan, các khách hàng và các nhà cung cấp. Khuyến nghị rằng, những báo cáo trong các kết quả đo được phân phát ra ngoài chỉ chứa dữ liệu phù hợp cho việc phát hành ra bên ngoài và đã được sự đồng ý bởi ban quản lý và các bên liên quan trước khi phát hành.

10 Ước lượng và cải tiến Chương trình đo lường an toàn thông tin

10.1 Giới thiệu chung

Tổ chức nên ước lượng tại những thời điểm đã định trong kế hoạch những nội dung sau:

a) Hiệu lực của Chương trình đo lường an toàn thông tin để đảm bảo rằng nó:

   1) Đưa ra những kết quả đo theo một cách hiệu quả;
   2) Đã được thực hiện theo kế hoạch;
   3) Chỉ ra những thay đổi trong ISMS đã triển khai và/hoặc biện pháp quản lý;
   4) Chỉ ra những thay đổi về môi trường (như các yêu cầu, quy định pháp lý hoặc công nghệ).

b) Sự hữu ích của các kết quả đo đã phát triển đảm bảo rằng chúng thỏa mãn các nhu cầu thông tin có liên quan.

Ban quản lý nên chỉ rõ tần suất cho việc ước lượng, rà soát sửa đổi theo chu kỳ và thiết lập các cơ chế cho việc rà soát sửa đổi này (xem 7.2 trong TCVN ISO/IEC 27001:2009).

Các hành động liên quan sẽ bao gồm:

1) Xác định tiêu chí ước lượng cho Chương trình đo lường an toàn thông tin (xem 10.2);
2) Giám sát, soát xét và ước lượng đo lường (xem 10.3) và;
3) Thực hiện các cải tiến (xem 10.4).

10.2 Xác định tiêu chí ước lượng cho Chương trình đo lường an toàn thông tin

Tổ chức nên định rõ tiêu chí cho việc ước lượng hiệu lực của Chương trình đo lường an toàn thông tin cũng như tính hiệu dụng của các kết quả ước lượng đã phát triển. Các tiêu chí nên được xác định từ lúc bắt đầu triển khai Chương trình đo lường an toàn thông tin, có tính đến bối cảnh mục tiêu kỹ thuật và nghiệp vụ của tổ chức.

Những tiêu chí phù hợp nhất khi tổ chức ước lượng và cải tiến Chương trình đo lường an toàn thông tin đã triển khai là:

- Những thay đổi trong mục tiêu nghiệp vụ của tổ chức;
- Những thay đổi để phù hợp với các yêu cầu về chính sách, luật pháp và các ràng buộc trong an toàn thông tin;
- Những thay đổi trong các yêu cầu của tổ chức về an toàn thông tin;
- Những thay đổi về những rủi ro an toàn thông tin tới tổ chức;
- Việc gia tăng khả năng sự cần có của dữ liệu tinh hoặc phù hợp và/hoặc các phương pháp thu thập dữ liệu cho các mục đích của đo lường;
- Những thay đổi để phù hợp với đối tượng đo và các thuộc tính của nó.

Tiêu chí sau có thể được áp dụng để ước lượng các kết quả đo đã phát triển:

a) Các kết quả đo là:

   1) Dễ hiểu;

   2) Được thông báo đúng thời gian;

   3) Khách quan, có tính so sánh và có thể tái sử dụng.

b) Các quy trình đã thiết lập để phát triển các kết quả đo là:

   1) Được định nghĩa tốt;

   2) Dễ dàng để vận hành hoạt động;

   3) Việc kế tiếp nhau phù hợp.

c) Các kết quả đo là hữu dụng cho việc nâng cao an toàn thông tin;

d) Các kết quả đo đáp ứng nhu cầu thông tin tương ứng của tổ chức.

10.3 Giám sát, soát xét và ước lượng chương trình

Tổ chức nên giám sát, soát xét và ước lượng Chương trình đo lường an toàn thông tin của mình dựa vào tiêu chí đã được thiết lập (xem 10.2).

Tổ chức nên xác định các nhu cầu tiềm năng để cải tiến ISMP đã triển khai, bao gồm:

a) Soát xét hay sửa đổi cấu trúc đo lường đã chấp nhận hiện không còn thích hợp;

b) Phân bổ lại nguồn lực để hỗ trợ cho Chương trình đo lường an toàn thông tin.

Tổ chức cũng cần xác định các nhu cầu tiềm năng để cải tiến ISMS, bao gồm phạm vi, chính sách, mục tiêu, biện pháp quản lý, quy trình và thủ tục; các quyết sách quản lý đã thành văn để cho phép so sánh và phân tích xu hướng trong suốt quá trình soát xét tiếp sau.

Các kết quả của việc ước lượng này và những nhu cầu tiềm năng đã nhận thấy cho việc cải tiến nên được thông báo tới các bên liên quan để cho phép tạo ra các quyết định cần thiết cho những điểm cải tiến cần thiết.

Tổ chức cần đảm bảo rằng đã thu nhận phản hồi thông tin từ các bên liên quan về các kết quả của việc ước lượng này và những nhu cầu tiềm năng đã nhận thấy cho những cải tiến. Tổ chức cần hiểu rằng thông tin phản hồi là một trong những thông tin đầu vào quan trọng của Chương trình đo lường an toàn thông tin.

10.4 Thực hiện các cải tiến chương trình

Tổ chức cần đảm bảo rằng các bên liên quan nhận ra những cải tiến cần thiết của Chương trình đo lường an toàn thông tin (xem 7.3 e trong TCVN ISO/IEC 27001:2009). Những cải tiến đã nhận thấy cần được sự chấp thuận bởi ban quản lý. Những kế hoạch đã được chấp thuận này cần được chuyển thành tài liệu và được gửi tới các bên liên quan.

Tổ chức cũng cần bảo đảm rằng những cải tiến được chấp thuận của Chương trình đo lường an toàn thông tin được triển khai đúng theo kế hoạch. Tổ chức có thể áp dụng các kỹ thuật quản lý dự án để hoàn thành những cải tiến.

Phụ lục A

(Tham khảo)

Mẫu cấu trúc phép đo an toàn thông tin

Phụ lục A cung cấp mẫu ví dụ về cấu trúc của phép đo an toàn thông tin bao gồm các thành phần như đã xác định tại 7.5 cũng như được mô tả tại 5.4. Các tổ chức có thể sửa đổi mẫu cho phù hợp với các yêu cầu cụ thể.

Thông tin chung của phép đo	
Tên phép đo	Tên phép đo
Số hiệu	Số định danh duy nhất, cụ thể cho tổ chức
Mục đích	Mô tả các lý do về sự cần thiết của phép đo
Mục tiêu biện pháp quản lý	Mục tiêu cho các biện pháp quản lý/quy trình (đã có kế hoạch hoặc đã được triển khai)
Biện pháp quản lý (1)	Biện pháp quản lý/quy trình cần đo lường
Biện pháp quản lý (2)	Tùy chọn: biện pháp quản lý/ quy trình cao hơn, nếu áp dụng (đã lập kế hoạch hoặc đã được triển khai)
Đối tượng của phép đo và các thuộc tính	
Đối tượng	Đối tượng (thực thể) được đặc trưng thông qua đo lường các thuộc tính của nó. Một đối tượng bao gồm các quy trình, các kế hoạch, các dự án, các nguồn lực, các hệ thống, và các thành phần.
Thuộc tính	Tính chất hoặc đặc trưng của đối tượng của phép đo có thể được phân biệt về định lượng hoặc định tính bởi con người hoặc bởi tự động.
Thông tin đặc tả về số đo cơ bản (cho mỗi số đo cơ bản [từ 1 đến n])	
Số đo cơ bản	Một số đo cơ bản được xác định theo một thuộc tính và phương pháp đo cụ thể để định lượng thuộc tính (ví dụ như số người đã được đào tạo, số lượng địa điểm, chi phí tính đến nay). Khi dữ liệu được thu thập, một giá trị được gán cho một số đo cơ bản.
Phương pháp đo	Trình tự logic các hoạt động được sử dụng để định lượng một thuộc tính với một thang đo cụ thể.
Loại phương pháp đo	Tùy thuộc bản chất các hoạt động đã được sử dụng để định lượng một thuộc tính mà có hai phương pháp đo: - Chủ quan: định lượng liên quan tới chủ định của con người. - Khách quan: định lượng dựa trên các quy tắc số học.
Thang đo	Tập hợp có thứ tự các giá trị hoặc phân loại mà các số đo cơ bản được ánh xạ đến.
Loại thang đo	Tùy thuộc bản chất bản chất mối quan hệ giữa các giá trị trong thang mà phân thành bốn loại thang đo phổ biến: Danh định; thứ tự; khoảng đoạn; tỷ lệ.
Đơn vị đo	Lượng cụ thể, được xác định và chấp nhận theo quy ước, với lượng này, các lượng khác cùng loại được so sánh để diễn tả mối tương quan về độ lớn với lượng đó.
Thông tin đặc tả về số đo dẫn xuất	
Số đo dẫn xuất	Một số đo được rút ra từ hai hoặc nhiều hơn số đo cơ bản.
Hàm đo lường	Thuật toán hoặc tính toán được thực hiện để kết hợp hai hoặc nhiều số đo cơ bản. Thang đo và đơn vị của số đo dẫn xuất tùy thuộc thang đo và đơn vị của các số đo cơ bản đã được kết hợp cũng như cách chúng được kết hợp với nhau qua hàm.
Thông tin đặc tả về chỉ báo	
Chỉ báo	Số đo cung cấp những ước tính hay ước lượng của các thuộc tính xác định thông qua mô hình phân tích với những nhu cầu thông tin cần thiết. Các chỉ báo là cơ sở để phân tích và đưa ra quyết định.
Mô hình phân tích	Thuật toán hoặc tính toán kết hợp một hoặc nhiều số đo cơ bản hoặc

	các số đo dẫn xuất với tiêu chí quyết định phù hợp; Điều này dựa trên sự hiểu biết hoặc giả thiết về mối quan hệ dự tính giữa số đo cơ bản hoặc số đo dẫn xuất hoặc trạng thái của chúng. Mô hình phân tích sẽ đưa ra ước đoán hay ước lượng liên quan đến mỗi nhu cầu thông tin cụ thể.
Thông tin đặc tả về tiêu chí quyết định	
Tiêu chí quyết định	Ngưỡng, mục tiêu, hoặc các mẫu được sử dụng để xác định sự cần thiết phải hành động hay điều tra thêm, hoặc để mô tả mức chính xác của kết quả đo lường cụ thể. Tiêu chí quyết định giúp giải thích các kết quả của phép đo.
Kết quả phép đo	
Giải thích chỉ báo	Mô tả cách thức một chỉ báo mẫu được diễn giải như thế nào.
Định dạng báo cáo đo	Định dạng báo cáo đo nên được xác định và lập thành tài liệu. Định dạng báo cáo đo mô tả các theo dõi mà tổ chức hoặc người sở hữu thông tin có thể muốn ghi lại. Định dạng báo cáo đo sẽ mô tả một cách trực quan các số đo và cung cấp giải thích rõ ràng về các chỉ báo. Định dạng báo cáo đo nên được tùy chỉnh theo khách hàng yêu cầu thông tin.
Các bên liên quan	
Người yêu cầu đo	Ban quản lý hoặc các bên quan tâm yêu cầu hoặc cần thông tin về hiệu lực của một hệ thống ISMS, các biện pháp quản lý hoặc nhóm biện pháp quản lý.
Người soát xét kết quả đo	Cá nhân hoặc tổ chức kiểm tra tính hợp lệ cho các cấu trúc phép đo đã phát triển là phù hợp cho việc đánh giá hiệu lực của một hệ thống ISMS, các biện pháp quản lý hoặc nhóm biện pháp quản lý.
Người sở hữu thông tin	Cá nhân hoặc tổ chức sở hữu thông tin về một đối tượng của phép đo và chịu trách nhiệm về phép đo.
Bộ phận thu thập thông tin	Cá nhân hoặc tổ chức chịu trách nhiệm về thu thập, ghi chép và lưu trữ dữ liệu.
Bộ phận trao đổi thông tin	Cá nhân hoặc tổ chức chịu trách nhiệm phân tích dữ liệu và trao đổi các kết quả phép đo.
Tần suất thực hiện	
Tần suất thu thập dữ liệu	Mức độ thường xuyên thu thập dữ liệu.
Tần suất phân tích dữ liệu	Mức độ thường xuyên phân tích dữ liệu.
Tần suất lập báo cáo các kết quả đo	Mức độ thường xuyên của các kết quả đo được lập báo cáo (mức này có thể thấp hơn Tần suất thu thập dữ liệu).
Tần suất sửa đổi phép đo	Ngày sửa đổi phép đo (thời hạn hiệu lực của tính hợp lệ của phép đo hoặc các thay đổi của phép đo)
Tần suất thực hiện phép đo	Xác định định kỳ thực hiện phép đo.

Phụ lục B

(Tham khảo)

Các ví dụ về cấu trúc các phép đo

Dưới đây cung cấp các ví dụ về cấu trúc các phép đo. Các ví dụ mẫu này được đưa ra để diễn tả việc áp dụng tiêu chuẩn này khi sử dụng mẫu tại Phụ lục A.

Bảng mục lục

Các quy trình và biện pháp quản lý liên quan (trong TCVN ISO/IEC 27001:2009 hay số biện pháp quản lý trong Phụ lục A)	**Các mẫu cấu trúc phép đo** (tham chiếu tại Phụ lục này)	**Tên mẫu cấu trúc phép đo**
Điều 4.2.2 h)	B.4.1	Hiệu lực của quản lý sự cố an toàn thông tin
Điều 5.2.2 d)	B.1.1	Nhân sự đã được đào tạo về ISMS
Điều 8.2	B.4.2	Triển khai các hành động khắc phục
Biện pháp quản lý A.6.1.8	B.3	Tiến trình soát xét ISMS
Biện pháp quản lý A.6.1.1 và A.6.1.2	B.5	Quản lý các cam kết
Biện pháp quản lý A.6.2.3	B.10	Các thỏa thuận đối với các bên thứ ba
Biện pháp quản lý A.8.2 và A.8.2.2	B.1.2	Đào tạo về an toàn thông tin
Biện pháp quản lý A.8.2 và A.8.2.2	B.1.3	Tuân thủ nhận thức an toàn thông tin
Biện pháp quản lý A.9.1.2	B.7	Biện pháp quản lý truy nhập vật lý
Biện pháp quản lý A.9.2.4	B.9	Quản lý bảo trì thường xuyên
Biện pháp quản lý A.10.4.1	B.6	Bảo vệ chống mã độc
Biện pháp quản lý A.10.10.1 và A.10.10.2	B.8	Soát xét các file log
Biện pháp quản lý A.11.3.1	B.2.1	Chất lượng mật khẩu – thiết lập thủ công
Biện pháp quản lý A.11.3.1	B.2.2	Chất lượng mật khẩu – thiết lập tự động

B.1 Đo lường về đào tạo ISMS

B.1.1 Nhân sự đã được đào tạo về ISMS

Thông tin chung của phép đo	
Tên phép đo	**Nhân sự đã được đào tạo về ISMS**
Số hiệu	Tùy theo quy định của tổ chức.
Mục đích	Để thiết lập các biện pháp quản lý tuân thủ với chính sách an toàn thông tin của tổ chức.
Mục tiêu biện pháp quản lý	Đào tạo, nhận thức và năng lực theo 5.2.2 [TCVN ISO/IEC 27001:2009].
Biện pháp quản lý (1)	5.2.2 d [TCVN ISO/IEC 27001:2009]. Đào tạo, nhận thức và năng lực. Tổ chức cần đảm bảo rằng: mọi cá nhân đã được phân công trách nhiệm trong hệ thống ISMS có đủ năng lực để thực hiện các nhiệm vụ được yêu cầu theo: d) lưu giữ hồ sơ về học vấn, quá trình đào tạo, các kỹ năng, kinh nghiệm và trình độ chuyên môn.
Biện pháp quản lý (2)	Tùy chọn: biện pháp quản lý thêm nữa trong cùng nhóm biện pháp, nếu áp dụng (đã lập kế hoạch hoặc đã được triển khai)
Đối tượng của phép đo và các thuộc tính	
Đối tượng	Cơ sở dữ liệu nhân sự.
Thuộc tính	Bản ghi, hồ sơ đào tạo.
Thông tin đặc tả về số đo cơ bản (cho mỗi số đo cơ bản [từ 1 đến n])	
Số đo cơ bản	Số nhân sự được đào tạo hệ thống ISMS theo kế hoạch đào tạo hàng năm. Số nhân sự cần phải đào tạo hệ thống ISMS.
Phương pháp đo	Đếm số lượng người đã được đào tạo về ISMS.
Loại phương pháp đo	Khách quan.
Thang đo	Bằng số.
Loại thang đo	Theo tỷ lệ.
Đơn vị đo	Nhân viên
Thông tin đặc tả về số đo dẫn xuất	
Số đo dẫn xuất	Tỷ lệ phần trăm nhân viên được đào tạo hệ thống ISMS
Hàm đo lường	Số nhân viên được đào tạo hệ thống ISMS / Số nhân viên cần phải đào tạo hệ thống ISMS * 100.
Thông tin đặc tả về chỉ báo	
Chỉ báo	Sử dụng mã màu với các bộ nhận dạng màu. Đồ thị dạng thanh mô tả tương ứng với nhiều giai đoạn lập báo cáo liên quan đến các ngưỡng (đỏ, vàng, xanh lá cây) được xác định tại mô hình phân tích. Số giai đoạn báo cáo được sử dụng trong đồ thị do tổ chức xác định.
Mô hình phân tích	Tỷ lệ 0-60%: màu đỏ; 60-90%: màu vàng; 90-100%: màu xanh lá cây. Đối với màu vàng, nếu tỷ lệ tăng không đạt tối thiểu 10% mỗi quý, chỉ báo tự động chuyển sang màu đỏ.
Thông tin đặc tả về tiêu chí quyết định	
Tiêu chí quyết định	Màu đỏ: cần thiết can thiệp, phải tiến hành phân tích nguyên nhân để

	xác định lý do chưa phù hợp và hiệu suất kém của đánh giá. Màu vàng: chỉ báo cần được theo dõi chặt chẽ để tránh các trượt giảm xuống màu đỏ. Màu xanh lá cây: không cần thiết phải hành động.
Kết quả đo	
Giải thích chỉ báo	Tùy theo tổ chức cụ thể.
Định dạng báo cáo đo	Đồ thị dạng thanh với các màu biểu thị dựa trên các tiêu chí quyết định. Tóm tắt ý nghĩa của các số đo và các hành động quản lý khả thi cần được ghi chú kèm theo đồ thị.
Các bên liên quan	
Người yêu cầu đo	Người quản lý chịu trách nhiệm đối với hệ thống ISMS.
Người soát xét phép đo	Người quản lý chịu trách nhiệm đối với hệ thống ISMS.
Người sở hữu thông tin	Người quản lý đào tạo – Ban nhân sự.
Bộ phận thu thập thông tin	Ban đào tạo – Phòng nhân sự.
Bộ phận trao đổi thông tin	Người quản lý chịu trách nhiệm đối với hệ thống ISMS.
Tần suất thực hiện	
Tần suất thu thập dữ liệu	Hàng tháng (vào ngày làm việc đầu tiên của tháng).
Tần suất phân tích dữ liệu	Hàng quý.
Tần suất lập báo cáo các kết quả đo	Hàng quý.
Tần suất sửa đổi phép đo	Soát xét sửa đổi hàng năm.
Tần suất thực hiện phép đo	Hàng năm.

B.1.2 Đào tạo về an toàn thông tin

Thông tin chung của phép đo	
Tên phép đo	**Đào tạo về an toàn thông tin**
Số hiệu	Tùy theo tổ chức.
Mục đích	Để ước lượng phù hợp với yêu cầu đào tạo về nhận thức an toàn thông tin hàng năm.
Mục tiêu biện pháp quản lý	Biên pháp quản lý theo A.8.2 [TCVN ISO/IEC 27001:2009]. Trong thời gian làm việc. Đảm bảo rằng mọi cá nhân của tổ chức, người của nhà thầu và bên thứ ba nhận thức được các mối nguy cơ và các vấn đề liên quan tới an toàn thông tin, trách nhiệm và nghĩa vụ pháp lý của họ và được trang bị các kiến thức, điều kiện cần thiết nhằm hỗ trợ chính sách an toàn thông tin của tổ chức trong quá trình làm việc và giảm thiểu các rủi ro do con người gây ra.
Biện pháp quản lý (1)	Biện pháp quản lý theo A.8.2.2 [TCVN ISO/IEC 27001:2009]. Nhận thức, giáo dục và đào tạo về an toàn thông tin. Tất cả các cá nhân trong tổ chức, người của nhà thầu và bên thứ ba cần phải được đào tạo nhận thức và cập nhật thường xuyên những thủ tục, chính sách đảm bảo an toàn thông tin của tổ chức như một phần công việc bắt buộc.

Đối tượng của phép đo và các thuộc tính	
Đối tượng	Cơ sở dữ liệu nhân sự.
Thuộc tính	Các giấy tờ trong hồ sơ đào tạo.
Thông tin đặc tả về số đo cơ bản	
Số đo cơ bản	Số cá nhân được đào tạo nâng cao nhận thức an toàn thông tin theo kế hoạch đào tạo hàng năm. Số cá nhân cần đào tạo nâng cao nhận thức an toàn thông tin.
Phương pháp đo	Đếm số lượng người đã xác nhận là "được đào tạo" nâng cao nhận thức an toàn thông tin.
Loại phương pháp đo	Khách quan
Thang đo	Số lượng
Loại thang đo	Theo tỷ lệ.
Đơn vị đo	Cá nhân.
Thông tin đặc tả về số đo dẫn xuất	
Số đo dẫn xuất	Tỷ lệ phần trăm cá nhân được đào tạo nâng cao nhận thức an toàn thông tin hàng năm.
Hàm đo lường	Số cá nhân được đào tạo nâng cao nhận thức an toàn thông tin / Số cá nhân cần phải đào tạo nâng cao nhận thức an toàn thông tin * 100.
Thông tin đặc tả về chỉ báo	
Chỉ báo	Đồ thị dạng thanh mô tả tương ứng với nhiều giai đoạn lập báo cáo liên quan đến các ngưỡng (đỏ, vàng, xanh lá cây) được xác định tại mô hình phân tích. Số giai đoạn báo cáo được sử dụng trong đồ thị do tổ chức xác định.
Mô hình phân tích	Tỷ lệ 0-60%: màu đỏ; 60-90%: màu vàng; 90-100%: màu xanh lá cây. Đối với màu vàng, nếu tỷ lệ tăng không đạt tối thiểu 10% mỗi quý, chỉ báo tự động chuyển sang màu đỏ.
Thông tin đặc tả về tiêu chí quyết định	
Tiêu chí quyết định	Màu đỏ: cần thiết can thiệp, phải tiến hành phân tích nguyên nhân để xác định lý do chưa phù hợp và hiệu suất kém của đánh giá. Màu vàng: chỉ báo cần được theo dõi chặt chẽ để tránh các trượt giảm xuống màu đỏ. Màu xanh lá cây: không cần thiết phải hành động.
Kết quả đo	
Giải thích chỉ báo	Tùy theo tổ chức.
Định dạng báo cáo đo	Đồ thị dạng thanh với các màu biểu thị dựa trên các tiêu chí quyết định. Tóm tắt ý nghĩa của các số đo và các hành động quản lý khả thi cần được ghi chú kèm theo đồ thị.
Các bên liên quan	
Người yêu cầu đo	Người quản lý chịu trách nhiệm đối với hệ thống ISMS, Ban quản lý an toàn thông tin, Ban quản lý đào tạo.
Người soát xét phép đo	Người quản lý an toàn thông tin.
Người sở hữu thông tin	Cán bộ an toàn thông tin và người quản lý đào tạo.
Bộ phận thu thập thông tin	Ban quản lý đào tạo – Phòng nhân sự.

Bộ phận trao đổi thông tin	Người quản lý chịu trách nhiệm đối với hệ thống ISMS.
Tần suất thực hiện	
Tần suất thu thập dữ liệu	Hàng tháng (vào ngày làm việc đầu tiên của tháng).
Tần suất phân tích dữ liệu	Hàng quý.
Tần suất lập báo cáo các kết quả đo	Hàng quý.
Tần suất sửa đổi phép đo	Soát xét sửa đổi hàng năm.
Tần suất thực hiện phép đo	Hàng năm.

B.1.3 Tuân thủ nhận thức an toàn thông tin

Thông tin chung của phép đo	
Tên phép đo	**Tuân thủ nhận thức an toàn thông tin.**
Số hiệu	Tùy theo quy định của tổ chức.
Mục đích	Đánh giá tình trạng tuân thủ chính sách nhận thức an toàn thông tin giữa những cá nhân có liên quan.
Mục tiêu biện pháp quản lý	Tiến trình A.8.2 [TCVN ISO/IEC 27001:2009]. Trong thời gian làm việc. Đảm bảo rằng mọi cá nhân của tổ chức, người của nhà thầu và bên thứ ba nhận thức được các mối nguy cơ và các vấn đề liên quan tới an toàn thông tin, trách nhiệm và nghĩa vụ pháp lý của họ và được trang bị các kiến thức, điều kiện cần thiết nhằm hỗ trợ chính sách an toàn thông tin của tổ chức trong quá trình làm việc và giảm thiểu các rủi ro do con người gây ra.
Biện pháp quản lý (1)	Tiến trình A.8.2.2 [TCVN ISO/IEC 27001:2009]. Nhận thức, giáo dục và đào tạo về an toàn thông tin. Tất cả các cá nhân trong tổ chức, người của nhà thầu và bên thứ ba cần phải được đào tạo nhận thức và cập nhật thường xuyên những thủ tục, chính sách đảm bảo an toàn thông tin của tổ chức như một phần công việc bắt buộc. (Triển khai) Tất cả các cá nhân có liên quan đối với hệ thống ISMS phải được đào tạo nhận thức an toàn thông tin trước khi được cấp quyền truy cập hệ thống thông tin.
Biện pháp quản lý (2)	Tiến trình A.8.2.1 [TCVN ISO/IEC 27001:2009]. Trách nhiệm ban quản lý. Ban quản lý cần phải yêu cầu các cá nhân, người của nhà thầu và bên thứ ba chấp hành an toàn thông tin phù hợp với các thủ tục và các chính sách an toàn thông tin đã được thiết lập của tổ chức. (Triển khai) Tất cả các cá nhân có liên quan đến ISMS phải ký thỏa thuận người dùng (cam kết) trước khi được cấp quyền truy cập hệ thống thông tin.
Đối tượng của phép đo và các thuộc tính	
Đối tượng	1.1. Kế hoạch hoặc lịch trình đào tạo nhận thức an toàn thông tin của tổ chức. 1.2. Các cá nhân đã hoàn thành hoặc đang trong quá trình đào tạo. 2.1. Kế hoạch/ lịch trình ký kết thỏa thuận người dùng. 2.2. Các cá nhân đã ký kết thỏa thuận.
Thuộc tính	1.1. Các cá nhân được xác định trong bản kế hoạch đào tạo. 1.2. Trạng thái của cá nhân liên quan đến quá trình đào tạo. 2.1. Các cá nhân được xác định trong kế hoạch ký kết thỏa thuận. 2.2. Trạng thái của cá nhân liên quan đến việc ký kết thỏa thuận.
Thông tin đặc tả về số đo cơ bản	
Số đo cơ bản	1.1. Số lượng cá nhân được lên kế hoạch đào tạo đến thời điểm hiện tại.

	1.2. Số lượng cá nhân đã ký xác nhận "được đào tạo". 2.1. Số lượng cá nhân được lên kế hoạch ký cam kết (xác định ký kết thỏa thuận đến nay.) 2.2. Số lượng cá nhân đã ký cam kết.
Phương pháp đo	1.1. Đếm số cá nhân theo lịch trình đã ký kết và hoàn thành các đào tạo cho đến nay. 1.2. Yêu cầu người có trách nhiệm cung cấp tỷ lệ phần trăm của những người phải được đào tạo và đã cam kết (trên tổng số nhân viên). 2.1. Đếm số nhân viên đã ký thoả thuận cho đến hôm nay. 2.2. Đếm số lượng cá nhân có thỏa thuận người dùng đã ký.
Loại phương pháp đo	1.1. Khách quan 1.2. Chủ quan 2.1. Khách quan 2.2. Khách quan.
Thang đo	1.1. Số nguyên từ 0 đến vô cùng 1.2. Số nguyên từ 0 đến 100 2.1. Số nguyên từ 0 đến vô cùng 2.2. Số nguyên từ 0 đến vô cùng
Loại thang đo	1.1. Theo thứ tự 1.2. Theo tỷ lệ 2.1. Theo thứ tự 2.2. Theo thứ tự
Đơn vị đo	1.1. Số lượng cá nhân 1.2. Tỷ lệ phần trăm 2.1. Số lượng cá nhân 2.2. Số lượng cá nhân
Thông tin đặc tả về số đo dẫn xuất	
Số đo dẫn xuất	1. Tiến trình tới nay (D.1: Tổng số nhân sự đã ký và số nhân sự đã có kế hoạch ký). 2. Tiến trình tới nay với việc ký kết thỏa thuận (D2 hay D1/B1*100: Tổng số nhân sự đã ký thoả thuận tới hôm nay).
Hàm đo lường	1. Bổ sung các tình trạng cho tất cả các nhân sự đã ký thỏa thuận, dự kiến sẽ được hoàn thành đến nay. 2. "Số lượng cá nhân đã ký kết thỏa thuận người dùng đến nay" chia cho "Số lượng cá nhân được xác định ký kết thỏa thuận đến nay".
Thông tin đặc tả về chỉ báo	
Chỉ báo	a) Các tình trạng đã thể hiện như một sự kết hợp của các tỷ lệ và; b) Xu hướng của đường biểu thị (tăng hoặc giảm).
Mô hình phân tích	a) [Tổng số nhân sự đã ký và đã có kế hoạch của Tiến trình đến nay (D.1) / (Số nhân sự đã có kế hoạch ký cho đến hôm nay (B.1)) * 100] và Tiến trình tới hôm nay cùng với ngày ký (D.2). b) So sánh tình trạng hiện tại và tình trạng trước đó.
Thông tin đặc tả về tiêu chí quyết định	
Tiêu chí quyết định	a) Các tỷ lệ kết quả so sánh nên giảm (theo độ dốc của đường biểu thị) tương ứng giữa 0,9 tới 1,1 và giữa 0,99 tới 1,01 để kết luận là đã đạt được mục tiêu quản lý và không cần có hành động can thiệp. b) Xu hướng của đường biểu thị là đi lên hoặc ổn định ngang.
Kết quả phép đo	
Giải thích chỉ báo	Giải thích cho chỉ báo a) như sau: - Tiêu chí của tổ chức về tuân thủ nhận thức an toàn thông tin thỏa mãn tỷ lệ tại 0,9 ≤ tỷ lệ thứ nhất ≤ 1,1 và 0,99 ≤ tỷ lệ thứ 2 ≤ 1,01; thể hiện bằng kiểu chữ thông thường. - Tiêu chí của tổ chức không thỏa mãn tỷ lệ tại [tỷ lệ thứ nhất < 0,9 hoặc tỷ lệ thứ nhất > 1,1] và 0,99 ≤ tỷ lệ so sánh thứ hai ≤

	1,01; thể hiện bằng kiểu chữ nghiêng. - Tiêu chí của tổ chức không đạt tại: [tỷ lệ thứ hai < 0,99 hoặc tỷ lệ thứ hai > 1,01]; thể hiện bằng kiểu chữ đậm. Giải thích cho chỉ báo b) như sau: - Xu hướng đi lên chỉ ra việc tuân thủ đã được cải tiến, xu hướng đi xuống chỉ ra việc tuân thủ kém đi. - Độ nghiêng của đường biểu thị cung cấp các thông tin về hiệu lực của việc triển khai biện pháp quản lý. - Xu hướng đồ thị thay đổi đột ngột cho thấy cần triển khai biện pháp quản lý để tìm ra nguyên nhân tăng hoặc giảm. Nếu có xu hướng giảm tiêu cực có thể yêu cầu người quản lý can thiệp. Xu hướng tăng hoặc tích cực cần được theo dõi để áp dụng.
Định dạng báo cáo đo	- Thể hiện bằng kiểu chữ chuẩn: tiêu chí đã thỏa mãn. - Thể hiện bằng kiểu chữ nghiêng: tiêu chí chưa thỏa mãn. - Thể hiện bằng kiểu chữ đậm: tiêu chí chưa đạt.
Các bên liên quan	
Người yêu cầu đo	Người quản lý chịu trách nhiệm đối với hệ thống ISMS. Ban quản lý an toàn thông tin. Ban quản lý đào tạo.
Người soát xét phép đo	Người quản lý an toàn thông tin.
Người sở hữu thông tin	Cán bộ an toàn thông tin và người quản lý đào tạo.
Bộ phận thu thập thông tin	Ban đào tạo – Phòng nhân sự.
Bộ phận trao đổi thông tin	Người quản lý chịu trách nhiệm đối với hệ thống ISMS.
Tần suất triển khai	
Tần suất thu thập dữ liệu	Hàng tháng (vào ngày làm việc đầu tiên của tháng).
Tần suất phân tích dữ liệu	Hàng quý.
Tần suất lập báo cáo các kết quả đo	Hàng quý.
Tần suất sửa đổi phép đo	Soát xét sửa đổi hàng năm.
Tần suất thực hiện phép đo	Hàng năm.

B.2 Đo lường các chính sách đặt mật khẩu

B.2.1 Chất lượng mật khẩu – kiểu thiết lập thủ công

Thông tin chung của phép đo	
Tên phép đo	**Đo lường Chất lượng mật khẩu – kiểu thiết lập thủ công**
Số hiệu	Tùy theo tổ chức.
Mục đích	Đánh giá mức an toàn của mật khẩu do người sử dụng thiết lập để truy cập hệ thống thông tin của tổ chức.
Mục tiêu biện pháp quản lý	Để hạn chế người sử dụng lựa chọn mật khẩu không an toàn.
Biện pháp quản lý (1)	Tiến trình A.11.3.1 [TCVN ISO/IEC 27001:2009]. Sử dụng mật khẩu. Người sử dụng phải được yêu cầu tuân thủ quy tắc thực hành an toàn tốt trong việc lựa chọn và sử dụng mật khẩu. **Triển khai:** Tất cả người sử dụng phải lựa chọn mật khẩu với độ mạnh tối thiểu như sau: - Độ dài lớn hơn 8 ký tự; - Không dựa trên thứ gì dễ dàng đoán biết hoặc có sử dụng thông tin về người liên quan, ví dụ: tên, số điện thoại, ngày tháng năm sinh...; - Không bao gồm các từ có trong từ điển; - Mật khẩu không bao gồm các ký tự liên tiếp giống hệt nhau, các ký tự đều là số hoặc các ký tự đều là chữ cái; Tất cả các tài khoản người sử dụng và mật khẩu của hệ thống thông tin trong tổ chức phải được quản lý bởi quản trị hệ thống hoặc nhân viên hệ thống.

Đối tượng của phép đo và các thuộc tính	
Đối tượng	Cơ sở dữ liệu mật khẩu người sử dụng.
Thuộc tính	Từng mật khẩu người sử dụng.
Thông tin đặc tả về số đo cơ bản	
Số đo cơ bản	1. Dựa trên số lượng mật khẩu đã đăng ký. 2. Dựa trên số lượng mật khẩu người sử dụng thỏa mãn các chính sách Chất lượng mật khẩu đề ra của tổ chức.
Phương pháp đo	1. Đếm số lượng mật khẩu trên cơ sở dữ liệu mật khẩu người sử dụng. 2. Hỏi từng người sử dụng về mật khẩu của họ có thỏa mãn chính sách Chất lượng mật khẩu đề ra của tổ chức hay không.
Loại phương pháp đo	1. Khách quan. 2. Chủ quan.
Thang đo	1. Số nguyên từ 0 đến vô cùng. 2. Số nguyên từ 0 đến vô cùng.
Loại thang đo	1. Theo thứ tự. 2. Theo thứ tự.
Đơn vị đo	1. Mật khẩu. 2. Mật khẩu.
Thông tin đặc tả về số đo dẫn xuất	
Số đo dẫn xuất	Tổng số lượng mật khẩu tuân theo chính sách Chất lượng mật khẩu của tổ chức.
Hàm đo lường	Tổng của: [Tổng số mật khẩu tuân theo chính sách chất lượng mật khẩu của tổ chức cho mỗi người sử dụng].
Thông tin đặc tả về chỉ báo	
Chỉ báo	a) Tỷ lệ mật khẩu phù hợp với chính sách Chất lượng mật khẩu của tổ chức. b) Tình trạng, xu hướng quan tâm đến chính sách Chất lượng mật khẩu.
Mô hình phân tích	a) Phân số của [Tổng số lượng mật khẩu người sử dụng đã tuân theo chính sách an toàn bảo mật của tổ chức] / [Tổng số lượng mật khẩu đã đăng ký]. b) So sánh tỷ lệ hiện tại với các tỷ lệ trước.
Thông tin đặc tả về tiêu chí quyết định	
Tiêu chí quyết định	Mục tiêu biện pháp quản lý đạt được và không phải hành động cần thiết nếu kết quả tỷ lệ là trên 0,9. Nếu tỷ lệ kết quả là giữa 0,8 và 0,9, mục tiêu chưa biện pháp quản lý được, nhưng có xu hướng ích cực. Nếu tỷ lệ kết quả dưới 0,8 cần có biện pháp can thiệp và hành động ngay.
Kết quả phép đo	
Giải thích chỉ báo	Giải thích cho chỉ báo a) như sau: - Tiêu chí của tổ chức về chính sách Chất lượng mật khẩu thỏa mãn: tỷ lệ > 0,9. - Tiêu chí của tổ chức về chính sách Chất lượng mật khẩu chưa thỏa mãn: 0,8≤ tỷ lệ ≤0,9. - Tiêu chí của tổ chức về chính sách Chất lượng mật khẩu chưa đáp ứng: tỷ lệ < 0,8. Giải thích cho chỉ báo b) như sau: - Xu hướng tăng cho thấy mức tuân thủ được cải tiến, ngược lại xu hướng giảm cho thấy mức tuân thủ xấu đi (Đồ thị). - Mức thay đổi của xu hướng cung cấp các thông tin về hiệu lực của việc triển khai biện pháp quản lý. - Xu hướng tiêu cực cần thiết biện pháp quản lý về nhận thức an toàn thông tin, hoặc các biện pháp kỹ thuật bắt buộc lựa chọn mật khẩu mạnh. - Xu hướng tăng hoặc tích cực cần được theo dõi, xem xét áp

	dụng để phù hợp với chính sách Chất lượng mật khẩu của tổ chức. Ảnh hưởng/ tác động của tiêu chuẩn này là không làm tăng các nguy cơ bảo mật. Nguyên nhân tiềm tàng bao gồm thiếu nhận thức về an toàn thông tin, sai sót của các biện pháp kỹ thuật và thiếu thời gian để thực thi các chính sách của hệ thống thông tin.
Định dạng báo cáo đo	Xu hướng của đường biểu thị mô tả số lượng mật khẩu phù hợp với chính sách Chất lượng mật khẩu của tổ chức, cùng với đường xu hướng của các báo cáo đo thường kỳ trước đó.
Các bên liên quan	
Người yêu cầu đo	Người quản lý chịu trách nhiệm đối với hệ thống ISMS. Người quản lý an toàn thông tin.
Người soát xét phép đo	Người quản lý an toàn thông tin.
Người sở hữu thông tin	Quản trị hệ thống.
Bộ phận thu thập thông tin	Cá nhân quản trị/ bảo mật hệ thống.
Bộ phận trao đổi thông tin	Cá nhân quản trị/ bảo mật hệ thống.
Tần suất triển khai	
Tần suất thu thập dữ liệu	Hàng năm.
Tần suất phân tích dữ liệu	Hàng năm.
Tần suất lập báo cáo các kết quả đo	Hàng năm.
Tần suất sửa đổi phép đo	Soát xét sửa đổi hàng năm.
Tần suất thực hiện phép đo	Hàng năm.

B.2.2 Chất lượng mật khẩu – kiểu thiết lập tự động

Thông tin chung của phép đo	
Tên phép đo	**Đo lường Chất lượng mật khẩu – kiểu thiết lập tự động**
Số hiệu	Tùy theo tổ chức.
Mục đích	Đề ra mức độ an toàn, độ mạnh mật khẩu khi người sử dụng thiết lập mật khẩu truy cập hệ thống thông tin của tổ chức.
Mục tiêu biện pháp quản lý	Để hạn chế người sử dụng lựa chọn mật khẩu không an toàn.
Biện pháp quản lý (1)	Tiến trình A.11.3.1 [TCVN ISO/IEC 27001:2009]. Sử dụng mật khẩu. Người sử dụng phải được yêu cầu tuân thủ quy tắc thực hành an toàn tốt trong việc lựa chọn và sử dụng mật khẩu. Triển khai: Tất cả người sử dụng phải lựa chọn mật khẩu với độ mạnh tối thiểu như sau: - Độ dài lớn hơn 8 ký tự; - Không dựa trên thứ gì dễ dàng đoán biết hoặc có sử dụng thông tin về người liên quan, ví dụ: tên, số điện thoại, ngày tháng năm sinh...; - Không bao gồm các từ có trong từ điển; - Mật khẩu không bao gồm các ký tự liên tiếp giống hệt nhau, các ký tự đều là số hoặc các ký tự đều là chữ cái; Tất cả các tài khoản người sử dụng và mật khẩu của hệ thống thông tin trong tổ chức phải được quản lý bởi nhân viên quản trị hệ thống hoặc nhân viên hệ thống.
Đối tượng của phép đo và các thuộc tính	
Đối tượng	Cơ sở dữ liệu nhân sự.
Thuộc tính	Bản ghi, hồ sơ đào tạo.
Thông tin đặc tả về số đo cơ bản	
Số đo cơ bản	1. Tổng số lượng các mật khẩu người sử dụng. 2. Tổng số lượng mật khẩu người sử dụng không thể bẻ khóa.
Phương pháp đo	1. Chạy câu lệnh truy vấn các bản ghi về thông tin tài khoản người sử dụng.

	2. Chạy chương trình/ câu lệnh bẻ khóa đối với các bản ghi về thông tin tài khoản người sử dụng bằng phương pháp bẻ khóa hỗn hợp.
Loại phương pháp đo	1. Khách quan. 2. Khách quan.
Thang đo	1. Số nguyên từ 0 đến vô cùng. 2. Số nguyên từ 0 đến vô cùng.
Loại thang đo	1. Theo thứ tự. 2. Theo thứ tự.
Đơn vị đo	1. Mật khẩu. 2. Mật khẩu.
Thông tin đặc tả về số đo dẫn xuất	
Số đo dẫn xuất	Không có.
Hàm đo lường	Không có.
Thông tin đặc tả về chỉ báo	
Chỉ báo	1. Tỷ lệ mật khẩu có thể bẻ khóa trong 4 giờ. 2. Xu hướng của "1. Tỷ lệ mật khẩu có thể bẻ khóa trong 4 giờ".
Mô hình phân tích	1. Là tỷ số [Số lượng mật khẩu không thể bẻ khóa] / [Tổng số lượng mật khẩu]. 2. So sánh tỷ lệ này với các tỷ lệ trước.
Thông tin đặc tả về tiêu chí quyết định	
Tiêu chí quyết định	Mục tiêu quản lý chất lượng mật khẩu đạt được và không cần có hành động cần thiết nếu kết quả tỷ lệ là trên 0,9. Nếu tỷ lệ kết quả là giữa 0,8 và 0,9 mục tiêu quản lý chưa quản lý được, nhưng có xu hướng tích cực. Nếu tỷ lệ kết quả dưới 0,8, cần có can thiệp và hành động ngay.
Kết quả phép đo	
Giải thích chỉ báo	Giải thích cho chỉ báo 1 như sau: - Tiêu chí của tổ chức về chính sách Chất lượng mật khẩu thỏa mãn: tỷ lệ > 0,9. - Tiêu chí của tổ chức về chính sách Chất lượng mật khẩu chưa thỏa mãn: 0,8 ≤ tỷ lệ ≤ 0,9. - Tiêu chí của tổ chức về chính sách Chất lượng mật khẩu chưa đáp ứng: tỷ lệ < 0,8. Giải thích cho chỉ báo 2 như sau: - Xu hướng tăng cho thấy mức tuân thủ được cải tiến, ngược lại xu hướng giảm cho thấy mức tuân thủ xấu đi. - Mức thay đổi của xu hướng cung cấp các thông tin về hiệu lực của việc triển khai biện pháp quản lý. - Xu hướng tiêu cực cần thiết phải có các biện pháp quản lý về nhận thức an toàn thông tin, hoặc các biện pháp kỹ thuật bắt buộc lựa chọn mật khẩu mạnh. - Xu hướng tăng hoặc tích cực cần được theo dõi, xem xét áp dụng để phù hợp với chính sách Chất lượng mật khẩu của tổ chức. Ảnh hưởng/ tác động của tiêu chí này là không làm tăng các nguy cơ bảo mật. Nguyên nhân tiềm tàng bao gồm thiếu nhận thức về an toàn thông tin, sai sót của các biện pháp kỹ thuật và thiếu thời gian để thực thi các chính sách của hệ thống thông tin.
Định dạng báo cáo đo	Xu hướng của đường biểu thị mô tả khả năng bẻ khóa mật khẩu, cùng với đường xu hướng của các báo cáo đo thường kỳ trước đó.
Các bên liên quan	
Người yêu cầu đo	Người quản lý chịu trách nhiệm đối với hệ thống ISMS. Người quản lý an toàn thông tin.
Người soát xét phép đo	Ban quản lý an toàn thông tin.
Người sở hữu thông tin	Quản trị hệ thống.
Bộ phận thu thập thông tin	Nhân viên an toàn thông tin.

Bộ phận trao đổi thông tin	Nhân việc an toàn thông tin.
Tần suất triển khai	
Tần suất thu thập dữ liệu	Hàng năm.
Tần suất phân tích dữ liệu	Hàng năm.
Tần suất lập báo cáo các kết quả đo	Hàng năm.
Tần suất sửa đổi phép đo	Soát xét sửa đổi hàng năm.
Tần suất thực hiện phép đo	Hàng năm.

B.3 Đo lường tiến trình soát xét ISMS

Thông tin chung của phép đo	
Tên phép đo	**Đo lường tiến trình soát xét ISMS**
Số hiệu	Tùy theo tổ chức.
Mục đích	Để đánh giá mức hoàn thành của việc soát xét độc lập hệ thống ISMS.
Mục tiêu biện pháp quản lý	Để quản lý an toàn thông tin trong tổ chức.
Biện pháp quản lý (1)	A.6.1.8 [TCVN ISO/IEC 27001:2009]. Tự soát xét về an toàn thông tin. Cách tiếp cận quản lý an toàn thông tin của tổ chức và việc triển khai của tổ chức (chẳng hạn như: các mục tiêu và các biện pháp quản lý, các chính sách, các quy trình và các thủ tục đảm bảo an toàn thông tin) phải được tự soát xét tần suất hoặc khi xuất hiện những thay đổi quan trọng liên quan đến an toàn thông tin. (Triển khai) Các phương pháp tiếp cận và triển khai quản lý an toàn thông tin của tổ chức được soát xét hàng quý bởi bên thứ ba có tư cách là nhà tư vấn về bảo mật.
Đối tượng đo lường và các thuộc tính	
Đối tượng	1. Các báo cáo soát xét của bên thứ ba. 2. Các kế hoạch soát xét của bên thứ ba.
Thuộc tính	1. Đã có báo cáo soát xét của bên thứ ba. 2. Đã có kế hoạch soát xét của bên thứ ba.
Thông tin đặc tả về số đo cơ bản	
Số đo cơ bản	1. Một số soát xét đã thực hiện của bên thứ ba. 2. Các kế hoạch soát xét đã thực hiện của bên thứ ba.
Phương pháp đo	1 Đếm số lượng các báo cáo đã tiến hành đánh giá thường xuyên bởi bên thứ ba. 2. Đếm số lượng các kế hoạch soát xét đã triển khai của bên thứ ba.
Loại phương pháp đo	1. Khách quan. 2. Khách quan.
Thang đo	1. Số nguyên từ 0 đến vô cùng. 2. Số nguyên từ 0 đến vô cùng.
Loại thang đo	1. Theo thứ tự. 2. Theo thứ tự.
Đơn vị đo	1. Soát xét. 2. Soát xét.
Thông tin đặc tả về số đo dẫn xuất	
Số đo dẫn xuất	Không có.
Hàm đo lường	Không có.
Thông tin đặc tả về chỉ báo	
Chỉ báo	Tỷ lệ các soát xét độc lập đã hoàn thành.
Mô hình phân tích	1. Là tỷ số [Các báo cáo soát xét đã thực hiện của bên thứ ba] / [Các kế hoạch soát xét đã thực hiện của bên thứ ba].
Thông tin đặc tả về tiêu chí quyết định	
Tiêu chí quyết định	Tỷ lệ kết quả của các chỉ báo sẽ giảm khoảng 0,8 và 1,1 để kết luận

	đạt được mục tiêu quản lý và không cần có hành động can thiệp; tỷ lệ chỉ báo cần đạt trên 0,6 để đáp ứng các điều kiện chính.
Kết quả phép đo	
Giải thích chỉ báo	Giải thích cho chỉ báo như sau: - Tiêu chí về quản lý an toàn thông tin trong tổ chức được soát xét kỹ lưỡng bởi bên thứ ba thỏa mãn: 0,8 ≤ tỷ lệ ≤ 1,1. - Tiêu chí về quản lý an toàn thông tin trong tổ chức được soát xét kỹ lưỡng bởi bên thứ ba chưa thỏa mãn: 0,6 ≤ tỷ lệ < 0,8 hoặc tỷ lệ > 1,1, cần thiết giám sát để đảm bảo phù hợp với tiến trình triển khai. - Tiêu chí chưa đáp ứng: 0 ≤ tỷ lệ < 0,6, cần thiết có hành động can thiệp để đảm bảo phù hợp với tiến trình triển khai. Nếu đến cuối quý thứ hai chỉ báo vẫn chưa thỏa mãn, cần thiết phải có hành động khắc phục và báo cáo đo với người quản lý chịu trách nhiệm hệ thống ISMS. Nếu đến cuối năm chỉ báo vẫn chưa thỏa mãn, cần thiết phải thông báo và yêu cầu hỗ trợ từ người quản lý cấp cao. Ảnh hưởng/tác động của tiêu chí này là không đáp ứng được sẽ làm giảm hiệu quả của quá trình soát xét quản lý. Nguyên nhân tiềm tàng bao gồm ngân sách thấp, triển khai không đúng kế hoạch, thiếu hụt nhân lực/ cam kết quản lý.
Định dạng báo cáo đo	Đồ thị dạng thanh mô tả giá trị qua các giai đoạn báo cáo phù hợp với các ngưỡng tiêu chí quyết định.
Các bên liên quan	
Người yêu cầu đo	Người quản lý chịu trách nhiệm đối với hệ thống ISMS. Người quản lý chất lượng hệ thống.
Người soát xét phép đo	Người quản lý an toàn thông tin.
Người sở hữu thông tin	Người quản lý an toàn thông tin.
Bộ phận thu thập thông tin	Kiểm tra viên nội bộ. Trưởng quản lý chất lượng.
Bộ phận trao đổi thông tin	Kiểm tra viên nội bộ. Các trưởng quản lý chất lượng chịu trách nhiệm đối với hệ thống ISMS.
Tần suất triển khai	
Tần suất thu thập dữ liệu	Hàng quý.
Tần suất phân tích dữ liệu	Hàng quý.
Tần suất lập báo cáo các kết quả đo	Hàng quý.
Tần suất sửa đổi phép đo	Soát xét và chỉnh sửa, cập nhật 2 năm/lần.
Tần suất thực hiện phép đo	Áp dụng trong 2 năm.

B.4 Đo lường việc cải tiến ISMS thường xuyên

B.4.1 Hiệu lực của quản lý sự cố an toàn thông tin

Thông tin chung của phép đo	
Tên phép đo	**Hiệu lực của quản lý sự cố an toàn thông tin**
Số hiệu	Tùy theo tổ chức.
Mục đích	Đánh giá hiệu lực của quản lý sự cố an toàn thông tin.
Mục tiêu biện pháp quản lý	Có khả năng nhanh chóng phát hiện các sự kiện an toàn thông tin và phản ứng với các sự cố an toàn thông tin.
Biện pháp quản lý (1)	4.2.2 h) [TCVN ISO/IEC 27001:2009] Triển khai các thủ tục và các biện pháp quản lý khác có khả năng nhanh chóng phát hiện các sự kiện an toàn thông tin và phản ứng với các sự cố an toàn thông tin.
Đối tượng đo lường và các thuộc tính	
Đối tượng	Hệ thống ISMS.
Thuộc tính	Từng sự cố riêng lẻ.
Thông tin đặc tả về số đo cơ bản	
Số đo cơ bản	Số lần xảy ra sự cố có thể chấp nhận được của tổ chức.

Phương pháp đo	Đếm các sự cố về an toàn thông tin được ghi nhận và báo cáo cho đến ngày đo.
Loại phương pháp đo	Khách quan
Thang đo	Số lượng
Loại thang đo	Theo thứ tự
Đơn vị đo	Sự cố
Thông tin đặc tả về số đo dẫn xuất	
Số đo dẫn xuất	Số sự cố vượt quá ngưỡng.
Hàm đo lường	So sánh tổng số lượng các sự cố với ngưỡng sự cố đặt ra.
Thông tin đặc tả về chỉ báo	
Chỉ báo	Biểu đồ đường bao gồm đường ngang không đổi thể hiện ngưỡng sự cố và đường thể hiện tổng số các sự cố theo các báo cáo đo.
Mô hình phân tích	Màu đỏ: tổng số các sự cố vượt quá ngưỡng (đi phía trên); Màu vàng: tổng số các sự cố nhỏ hơn ngưỡng trong khoảng 10%. Màu xanh lá cây: tổng số các sự cố nhỏ hơn ngưỡng 10% hoặc hơn.
Thông tin đặc tả về tiêu chí quyết định	
Tiêu chí quyết định	Màu đỏ: yêu cầu điều tra nguyên nhân tăng số lượng các sự cố ngay lập tức. Màu vàng: số lượng sự cố cần được giám sát, theo dõi chặt chẽ, nếu không có cải tiến cần thiết phải điều tra nguyên nhân. Màu xanh lá cây: không cần thiết phải hành động.
Kết quả phép đo	
Giải thích chỉ báo	Nếu màu đỏ xuất hiện trong 2 chu kì báo cáo đo, cần thiết phải soát xét các biện pháp quản lý sự cố an toàn thông tin để điều chỉnh, bổ sung các biện pháp phù hợp. Nếu xu hướng này không đảo ngược trong hai giai đoạn báo cáo đo tiếp theo, cần thiết phải có hành động khắc phục, chẳng hạn như đề nghị mở rộng phạm vi quản lý an toàn thông tin.
Định dạng báo cáo đo	Biểu đồ dạng đường kẻ.
Các bên liên quan	
Người yêu cầu đo	Ban quản lý hệ thống ISMS. Người quản lý chịu trách nhiệm đối với hệ thống ISMS. Ban quản lý an toàn thông tin. Ban quản lý sự cố an toàn thông tin.
Người soát xét phép đo	Người quản lý chịu trách nhiệm đối với hệ thống ISMS.
Người sở hữu thông tin	Người quản lý chịu trách nhiệm đối với hệ thống ISMS.
Bộ phận thu thập thông tin	Người quản lý sự cố an toàn thông tin.
Bộ phận trao đổi thông tin	Ban quản lý hệ thống ISMS.
Tần suất triển khai	
Tần suất thu thập dữ liệu	Hàng tháng.
Tần suất phân tích dữ liệu	Hàng tháng.
Tần suất lập báo cáo các kết quả đo	Hàng tháng.
Tần suất sửa đổi phép đo	6 tháng.
Tần suất thực hiện phép đo	Hàng tháng.

B.4.2 Triển khai các hành động khắc phục

Thông tin chung của phép đo	
Tên phép đo	**Triển khai các hành động khắc phục**
Số hiệu	Tùy theo tổ chức.
Mục đích	Đánh giá khả năng thực hiện của việc triển khai hành động khắc phục.
Mục tiêu biện pháp quản lý	8.2 [TCVN ISO/IEC 27001:2009] Hành động khắc phục Tổ chức phải thực hiện hành động loại bỏ các nguyên nhân không phù hợp đối với yêu cầu của hệ thống ISMS để ngăn ngừa khả năng tái diễn.
Biện pháp quản lý (1)	Thủ tục đã được lập thành tài liệu cho hành động khắc phục phải xác định các yêu cầu cho: a) Xác định các điểm không phù hợp; b) Tìm ra nguyên nhân của các điểm không phù hợp trên; c) Đánh giá sự cần thiết của các hành động đảm bảo điểm không phù hợp sẽ không xuất hiện trở lại; d) Quyết định và triển khai các hành động khắc phục cần thiết; e) Lập báo cáo kết quả thực hiện các hành động trên; f) Soát xét lại các hành động khắc phục đã triển khai. (đã triển khai) ..... Tổ chức xác định các hành động khắc phục yêu cầu và phát hành tài liệu báo cáo về hành động khắc phục nêu những điểm chưa phù hợp, các nguyên nhân của nó và thời gian cho hành động khắc phục. Khi nhận được báo cáo, người quản lý chịu trách nhiệm cho các khu vực có điểm không phù hợp đã được phát hiện được phải đảm bảo các hành động khắc phục được thực hiện không chậm trễ để loại bỏ những điểm không phù hợp và các nguyên nhân của chúng. Nếu hành động khắc phục không được triển khai như đã yêu cầu, nguyên nhân của việc không hành động này cần phải được xác định, cũng như các hành động thay thế hành động khắc phục nguyên bản phải được quyết định một cách phù hợp. Các hành động đã triển khai đúng ngày và kết quả cần phải được ghi lại thành văn bản. Nếu hành động khắc phục không được triển khai như kế hoạch đã định, lý do và các hành động thay thế cũng phải lập thành văn bản để báo cáo kịp thời đến người quản lý an toàn thông tin.
Đối tượng đo lường và các thuộc tính	
Đối tượng	Các báo cáo về hành động khắc phục.
Thuộc tính	Hạn triển khai hành động khắc phục trong báo cáo. Ngày triển khai hành động khắc phục được đưa vào trong báo cáo. Lý do trì hoãn và không hành động.
Thông tin đặc tả về số đo cơ bản	
Số đo cơ bản	1. Số hành động khắc phục đã được lên kế hoạch tới nay. 2. Số hành động khắc phục đã được thực hiện theo kế hoạch tới nay. 3. Số hành động khắc phục chưa được thực hiện có lý do tới nay.
Phương pháp đo	1. Đếm số hành động khắc phục đã có kế hoạch đã thực hiện tới nay. 2. Đếm số hành động khắc phục được ghi nhận như đã triển khai cho đến nay. 3. Đếm số hành động khắc phục được ghi nhận như đã kế hoạch nhưng chưa thực hiện, có lý do.
Loại phương pháp đo	1 - 3: Khách quan
Thang đo	1 - 3: Số nguyên từ 0 đến vô cùng.
Loại thang đo	1 - 3: Theo thứ tự.
Đơn vị đo	1 - 3: Hành động khắc phục.
Thông tin đặc tả về số đo dẫn xuất	
Số đo dẫn xuất	a) Hành động khắc phục chưa được triển khai cho đến nay. b) Hành động khắc phục chưa được triển khai không có lý do hợp lý.

Hàm đo lường	a) [Số hành động khắc phục đã được lên kế hoạch tới nay] - [Số hành động khắc phục đã thực hiện theo kế hoạch tới nay]. b) [Số hành động khắc phục không được triển khai theo kế hoạch có lý do] - [Số hành động khắc phục không được triển khai].
Thông tin đặc tả về chỉ báo	
Chỉ báo	a) Tình trạng thể hiện như một tỷ lệ của hành động khắc phục không được triển khai. b) Tình trạng thể hiện như một tỷ lệ của hành động khắc phục không được triển khai không có lý do. c) Xu hướng các trạng thái.
Mô hình phân tích	a) [Số hành động khắc phục không được triển khai đến nay] / [Số hành động khắc phục được lên kế hoạch đến nay]. b) [Số hành động khắc phục không được triển khai và không có lý do] / [Số hành động khắc phục được lên kế hoạch đến nay]. c) So sánh tình trạng với các tình trạng đánh giá trước.
Thông tin đặc tả về tiêu chí quyết định	
Tiêu chí quyết định	Để kết luận đạt được các mục tiêu và không cần hành động, tỷ lệ của chỉ báo a) và b) cần nằm tương ứng giữa 0,4 - 0,0 và giữa 0,2 - 0,0; xu hướng của chỉ số c) cần giảm so với 2 báo cáo đo thường kỳ trước đó. Các chỉ số c) cần được trình bày thể hiện so sánh với các chỉ số trước đây để đưa ra hướng áp dụng triển khai hành động khắc phục.
Kết quả phép đo	
Giải thích chỉ báo	Giải thích cho các chỉ báo a) và b) như sau: - Kế hoạch hành động khắc phục phải được triển khai trừ khi ưu tiên của tổ chức thay đổi dẫn đến cần thiết phải triển khai các hành động khắc phục khác hoặc chuyển hướng nguồn lực phân bổ để triển khai hành động khắc phục. Nếu hơn 40% hành động khắc phục không được triển khai bất kể lý do, hoặc hơn 20% hành động khắc phục không được triển khai không có lý do chính đáng, cần thiết phải có hành động quản lý. Hành động khắc phục không triển khai cần được kiểm tra để xác định nguyên nhân. Tùy thuộc vào tỷ lệ phần trăm không triển khai và lý do không triển khai, cần thiết phải có hành động ở mức cao hơn. Giải thích cho chỉ báo c) như sau: Một xu hướng trong việc thực hiện hành động khắc phục cần phải được xem xét cho bất kỳ suy giảm tổng thể trong hoạt động hoặc cải tiến đáng kể hiệu suất. Nếu tỷ lệ phần trăm của hành động khắc phục thực hiện giảm mạnh trong 2 báo cáo đo gần nhất, cần thiết có hành động quản lý bất kể các lý do không tuân thủ. Ảnh hưởng/tác động của tiêu chí ảnh hưởng đến việc cải tiến hệ thống ISMS. Nguyên nhân tiềm tàng bao gồm thiếu hụt nguồn lực, lập kế hoạch không chính xác, thiếu nhân sự có chuyên môn và cam kết quản lý.
Định dạng báo cáo đo	Đồ thị dạng thanh có ngăn với các đường biểu thị kết quả đo cho phép đưa ra các hành động quản lý thông qua tổng số lượng triển khai hành động khắc phục, tách ra thành đã triển khai, không triển khai có lý do chính đáng, không triển khai và không có lý do chính đáng.
Các bên liên quan	
Người yêu cầu đo	Người quản lý chịu trách nhiệm đối với hệ thống ISMS. Người quản lý an toàn thông tin.
Người soát xét phép đo	Người quản lý chịu trách nhiệm đối với hệ thống ISMS.
Người sở hữu thông tin	Người quản lý chịu trách nhiệm đối với hệ thống ISMS.
Bộ phận thu thập thông tin	Người quản lý chịu trách nhiệm đối với hệ thống ISMS.
Bộ phận trao đổi thông tin	Người quản lý chịu trách nhiệm đối với hệ thống ISMS.
Tần suất triển khai	

Tần suất thu thập dữ liệu	Hàng quý.
Tần suất phân tích dữ liệu	Hàng quý.
Tần suất lập báo cáo các kết quả đo	Hàng quý.
Tần suất sửa đổi phép đo	Soát xét sửa đổi hàng năm.
Tần suất thực hiện phép đo	Hàng năm.

B.5 Cam kết của ban quản lý

Thông tin chung của phép đo	
Tên phép đo	**Tần suất soát xét của ban quản lý**
Số hiệu	Tùy theo tổ chức.
Mục đích	Đánh giá cam kết của ban quản lý và các hành động soát xét an toàn thông tin theo các hành động soát xét của ban quản lý
Mục tiêu biện pháp quản lý	A.6.1 [TCVN ISO/IEC 27001:2009]. Nhằm quản lý an toàn thông tin trong tổ chức (đã lập kế hoạch). Nhằm quản lý an toàn thông tin trong tổ chức thông qua các soát xét của ban quản lý thực hiện thường xuyên.
Biện pháp quản lý (1)	A.6.1.1 [TCVN ISO/IEC 27001:2009]. Cam kết của ban quản lý về bảo đảm an toàn thông tin. Ban quản lý phải chủ động hỗ trợ bảo đảm an toàn thông tin trong tổ chức bằng các định hướng rõ ràng, các cam kết có thể thấy được, các nhiệm vụ rõ ràng và nhận thức rõ trách nhiệm về bảo đảm an toàn thông tin (đã triển khai). Tổ chức phải có các cuộc họp hàng tháng về soát xét của ban quản lý để hỗ trợ an toàn thông tin trong tổ chức bằng các định hướng rõ ràng, các cam kết có thể thấy được, các nhiệm vụ rõ ràng và nhận thức rõ trách nhiệm về bảo đảm an toàn thông tin. Soát xét của ban quản lý ISMS cần kết hợp với soát xét của ban quản lý hệ thống quản lý chất lượng QMS (Quality Management System).
Biện pháp quản lý (2)	Tiến trình A.6.1.2 [TCVN ISO/IEC 27001:2009]. Phối hợp bảo đảm an toàn thông tin. Các hoạt động bảo đảm an toàn thông tin cần phải được phối hợp bởi các đại diện của các ban trong tổ chức với vai trò và nhiệm vụ cụ thể. (đã triển khai). Những người nắm giữ vai trò và trách nhiệm có liên quan thuộc các phòng ban chức năng cần phối hợp và tham gia soát xét của ban quản lý.
Đối tượng đo lường và các thuộc tính	
Đối tượng	1. Kế hoạch/ lịch biểu soát xét của ban quản lý an toàn thông tin. 2. Các biên bản cuộc họp soát xét của ban quản lý.
Thuộc tính	1.1. Ngày của các cuộc họp soát xét của ban quản lý được lên kế hoạch. 1.2. Sự có mặt của ban quản lý tham dự các buổi họp soát xét được lên kế hoạch. 2.1. Những ngày họp soát xét của ban quản lý được ghi lại. 2.2. Sự có mặt của ban quản lý được ghi lại đã tham gia các cuộc họp soát xét.
Thông tin đặc tả về số đo cơ bản	
Số đo cơ bản	1.1. Số lượng các cuộc họp soát xét của ban quản lý được lên kế hoạch cho đến nay. 1.2. Số lượng người quản lý, nắm giữ vai trò và trách nhiệm có liên quan được đặt lịch để tham gia các cuộc họp soát xét của ban quản lý.

	2.1.1. Số lượng các cuộc họp soát xét của ban quản lý đã tổ chức theo kế hoạch cho đến nay. 2.1.2. Số lượng các cuộc họp soát xét của ban quản lý đã tổ chức đột xuất hoặc không theo kế hoạch cho đến nay. 2.1.3. Số lượng các cuộc họp soát xét của ban quản lý được đặt lịch lại và đã tổ chức cho đến nay. 2.2. Số lượng người quản lý, nắm giữ vai trò và trách nhiệm có liên quan tham dự các cuộc họp soát xét của ban quản lý cho đến nay.
Phương pháp đo	1.1. Đếm số lượng các cuộc họp soát xét của ban quản lý được đặt lịch cho đến nay. 1.2. Với mỗi cuộc họp soát xét của ban quản lý, đếm số lượng người quản lý, nắm giữ vai trò và trách nhiệm có liên quan tham dự; thêm một bản ghi mới với giá trị mặc định về số lượng người tham dự dành cho các cuộc họp đột xuất, không có kế hoạch định trước. 2.1.1. Đếm số lượng các cuộc họp soát xét của ban quản lý đã tổ chức theo kế hoạch cho đến nay. 2.1.2. Đếm số lượng các cuộc họp soát xét của ban quản lý đã tổ chức đột xuất hoặc không theo kế hoạch cho đến nay. 2.1.3. Đếm số lượng các cuộc họp soát xét của ban quản lý được đặt lịch lại và đã tổ chức cho đến nay. 2.2. Đối với tất cả các cuộc họp soát xét của ban quản lý đã được tổ chức, đếm số lượng lãnh đạo của tổ chức tham dự.
Loại phương pháp đo	1.1. Khách quan. 1.2. Khách quan hoặc chủ quan. 2.1.1. Khách quan. 2.1.2. Khách quan. 2.1.3. Khách quan. 2.2. Khách quan.
Thang đo	1.1. Số nguyên từ 0 đến vô cùng. 1.2. Số nguyên từ 0 đến vô cùng. 2.1.1.Số nguyên từ 0 đến vô cùng. 2.1.2. Số nguyên từ 0 đến vô cùng. 2.1.3. Số nguyên từ 0 đến vô cùng. 2.2. Số nguyên từ 0 đến vô cùng.
Loại thang đo	1.1. Theo thứ tự. 1.2. Theo thứ tự. 2.1.1.Theo thứ tự. 2.1.2. Theo thứ tự. 2.1.3. Theo thứ tự. 2.2. Theo thứ tự.
Đơn vị đo	1.1. Cuộc họp. 1.2. Số lượng người. 2.1.1. Cuộc họp. 2.1.2. Cuộc họp. 2.1.3. Cuộc họp. 2.2. Số lượng người.
Thông tin đặc tả về số đo dẫn xuất	
Số đo dẫn xuất	a) Số lượng các cuộc họp soát xét của ban quản lý đã tổ chức cho đến nay. b) Tỷ lệ các lần lãnh đạo tham gia các cuộc họp cho đến nay.
Hàm đo lường	a) Là tổng của [Số lượng các cuộc họp soát xét của ban quản lý được lên kế hoạch cho đến nay] và [Số lượng các cuộc họp soát xét của ban quản lý đột xuất hoặc không theo kế hoạch cho đến nay] và [Số lượng các cuộc họp soát xét của ban quản lý được đặt lịch lại cho đến nay].

	b) Với mỗi cuộc họp soát xét của ban quản lý, là phân số của [Số lượng lãnh đạo của tổ chức tham dự] / [Số lượng lãnh đạo của tổ chức dự kiến tham dự trong danh sách].
Thông tin đặc tả về chỉ báo	
Chỉ báo	a) Các cuộc họp soát xét của ban quản lý đã hoàn thành cho đến nay. b) Tỷ lệ người tham gia trung bình cho đến nay.
Mô hình phân tích	a) Là tỷ số [Số lượng các cuộc họp soát xét của ban quản lý đã triển khai] / [Số lượng các cuộc họp soát xét của ban quản lý được lên kế hoạch]. b) Số lượng trung bình và chênh lệch tiêu chí của tỷ lệ người quản lý tham gia các cuộc họp soát xét của ban quản lý.
Thông tin đặc tả về tiêu chí quyết định	
Tiêu chí quyết định	Kết quả tỷ lệ của chỉ báo a) giữa 0,7 và 1,1 để kết luận đạt được các mục tiêu quản lý và không cần thiết hành động. Nếu không đạt, tỷ lệ này cần đạt trên 0,5 để đáp ứng các yêu cầu tối thiểu. Liên quan đến chỉ báo b), tính toán tỷ lệ tham gia dựa trên chênh lệch tiêu chuẩn để đưa ra tỷ lệ tham gia trung bình thực tế có thể đạt được. Nếu tỷ lệ tham gia có dao động lớn, độ sai lệch trong dự đoán sẽ lớn, cần thiết phải có các kế hoạch dự phòng cho các kết quả xấu nhất có thể xảy ra.
Kết quả phép đo	
Giải thích chỉ báo	Giải thích cho chỉ báo a) như sau: Thỏa mãn: 0,7 ≤ tỷ lệ ≤ 1,1 Chưa thỏa mãn: 0,5 ≤ tỷ lệ < 0,7 hoặc tỷ lệ > 1,1 Tỷ lệ không đạt: 0 ≤ tỷ lệ < 0,5
Định dạng báo cáo đo	Biểu đồ đường mô tả chỉ báo với dữ liệu thu thập được và các đường thể hiện tại các báo cáo đo thường kỳ trước. Số lượng dữ liệu cần thu thập và số báo cáo đo thường kỳ đưa vào để so sánh phụ thuộc và xác định vào từng tổ chức.
Các bên liên quan	
Người yêu cầu đo	Người quản lý chịu trách nhiệm đối với hệ thống ISMS. Người quản lý chất lượng hệ thống.
Người soát xét phép đo	Người có thẩm quyền, quyền truy nhập chương trình đánh giá nội bộ.
Người sở hữu thông tin	Người quản lý chất lượng hệ thống. Kết hợp quản lý hệ thống ISMS và hệ thống quản lý chất lượng QMS.
Bộ phận thu thập thông tin	Quản lý chất lượng. Người quản lý an toàn thông tin.
Bộ phận trao đổi thông tin	Quản lý chất lượng. Người quản lý an toàn thông tin.
Tần suất triển khai	
Tần suất thu thập dữ liệu	Hàng tháng.
Tần suất phân tích dữ liệu	Hàng quý.
Tần suất lập báo cáo các kết quả đo	Hàng quý.
Tần suất sửa đổi phép đo	Soát xét và chỉnh sửa 2 năm/lần.
Tần suất thực hiện phép đo	2 năm/lần.

B.6 Đo lường bảo vệ chống mã độc

Thông tin chung của phép đo	
Tên phép đo	**Đo lường bảo vệ chống mã độc.**
Số hiệu	Tùy theo tổ chức.
Mục đích	Đánh giá hiệu lực của hệ thống bảo vệ đối với các phần mềm tấn công độc có chứa mã độc.
Mục tiêu biện pháp quản lý	Biện pháp quản lý A.10.4 [TCVN ISO/IEC 27001:2009] Nhằm bảo vệ tính toàn vẹn của phần mềm và thông tin. (đã lập kế hoạch) Nhằm bảo vệ tính toàn vẹn của phần mềm và thông tin đối với các

	phần mềm độc.
Biện pháp quản lý (1)	Biện pháp quản lý A.10.4.1 [TCVN ISO/IEC 27001:2009]. Quản lý chống lại mã độc. Các biện pháp quản lý trong việc phát hiện, ngăn chặn và phục hồi nhằm chống lại các đoạn mã độc và các thủ tục tuyên truyền nâng cao nhận thức của người sử dụng phải được triển khai.
Đối tượng đo lường và các thuộc tính	
Đối tượng	1. Các báo cáo sự cố gặp phải. 2. Các file log của phần mềm chống mã độc.
Thuộc tính	Sự cố gây ra bởi phần mềm có chứa mã độc.
Thông tin đặc tả về số đo cơ bản	
Số đo cơ bản	1. Số lượng sự cố gây ra bởi phần mềm có chứa mã độc. 2. Tổng số tấn công đã bị chặn gây ra bởi phần mềm có chứa mã độc.
Phương pháp đo	1. Đếm số lượng. 2. Đếm số lượng.
Loại phương pháp đo	1. Khách quan. 2. Khách quan.
Thang đo	1. Số nguyên từ 0 đến vô cùng. 2. Số nguyên từ 0 đến vô cùng.
Loại thang đo	1. Theo thứ tự. 2. Theo thứ tự.
Đơn vị đo	1. Sự cố an toàn 2. Bản ghi/records.
Thông tin đặc tả về số đo dẫn xuất	
Số đo dẫn xuất	Khả năng bảo vệ của phần mềm chống mã độc.
Hàm đo lường	Số lượng sự cố mất an toàn thông tin gây ra bởi phần mềm có chứa mã độc / Số lần phát hiện và ngăn chặn tấn công của mã độc.
Thông tin đặc tả về chỉ báo	
Chỉ báo	Xu hướng phát hiện các tấn công không được ngăn chặn theo các báo cáo đo thường kỳ trước.
Mô hình phân tích	So sánh tỷ lệ với các tỷ lệ trong các báo cáo đo thường kỳ trước.
Thông tin đặc tả về tiêu chí quyết định	
Tiêu chí quyết định	Đường biểu thị nên nằm dưới một số cụ thể (ngưỡng). Kết quả của xu hướng nên theo chiều hướng giảm hoặc là đường không đổi.
Kết quả phép đo	
Giải thích chỉ báo	Đường biểu thị có xu hướng tăng cho thấy các nguy cơ xấu, xu hướng giảm cho thấy các cải tiến. Khi có xu hướng tăng lên đáng kể, cần thiết điều tra nguyên nhân và có các biện pháp đối phó.
Định dạng báo cáo đo	Đường biểu thị xu hướng mô tả tỷ lệ phát hiện phần mềm có chứa mã độc, ngăn chặn tỷ lệ tăng so với các đường biểu thị trong các báo cáo đo thường kỳ trước.
Các bên liên quan	
Người yêu cầu đo	Người quản lý an toàn thông tin.
Người soát xét phép đo	Người quản lý an toàn thông tin.
Người sở hữu thông tin	Người quản trị hệ thống.
Bộ phận thu thập thông tin	Người quản lý an toàn thông tin. Người quản trị hệ thống. Người quản trị mạng.
Bộ phận trao đổi thông tin	Ban điều phối dịch vụ.
Tần suất triển khai	
Tần suất thu thập dữ liệu	Hàng ngày.
Tần suất phân tích dữ liệu	Hàng tháng.
Tần suất lập báo cáo các kết quả đo	Hàng tháng.
Tần suất sửa đổi phép đo	Soát xét hàng năm.
Tần suất thực hiện phép đo	Hàng năm.

B.7 Đo lường biện pháp quản lý truy nhập vật lý

Thông tin chung của phép đo	
Tên phép đo	**Đo lường biện pháp quản lý truy nhập vào/ra**
Số hiệu	Tùy theo tổ chức.
Mục đích	Cho biết sự tồn tại, mức độ và chất lượng của hệ thống quản lý truy nhập.
Mục tiêu biện pháp quản lý	Biện pháp quản lý A.9.1 [TCVN ISO/IEC 27001:2009]. Các khu vực an toàn. Nhằm ngăn chặn sự truy cập vật lý trái phép, làm hư hại và cản trở thông tin và tài sản của tổ chức.
Biện pháp quản lý (1)	Biện pháp quản lý A.9.1.2 [TCVN ISO/IEC 27001:2009]. Quản lý cổng truy cập vật lý. Các khu vực bảo mật cần được bảo vệ bằng các biện pháp biện pháp quản lý truy cập thích hợp nhằm đảm bảo chỉ những người có quyền mới được phép truy cập.
Đối tượng đo lường và các thuộc tính	
Đối tượng	Các khu vực an toàn.
Thuộc tính	Báo cáo quản lý danh tính cá nhân.
Thông tin đặc tả về số đo cơ bản	
Số đo cơ bản	Quản lý truy nhập vật lý bằng thẻ truy nhập.
Phương pháp đo	Phương pháp đo tương đối trong đó mỗi nhóm nhỏ là một phần của nhóm phía trên. Quản lý các loại hệ thống truy nhập và kiểm tra các khía cạnh sau: - Sử dụng hệ thống thẻ. - Sử dụng mã PIN (Personal Identify Number - Mã định danh cá nhân). - Chức năng truy nhập từ các lần trước (theo file log). - Xác thực sinh trắc học.
Loại phương pháp đo	Chủ quan.
Thang đo	Có 6 mức từ 0 – 5: 0: Không có hệ thống biện pháp quản lý truy nhập. 1. Hệ thống biện pháp quản lý truy nhập sử dụng mã PIN. 2. Hệ thống biện pháp quản lý truy nhập sử dụng thẻ. 3. Sử dụng mã PIN và mã thẻ. 4. 3 + chức năng ghi nhớ truy cập các lần trước. 5. 4 + mã PIN, có thêm xác thực sinh trắc học (vân tay, nhận dạng giọng nói, quét võng mạc...).
Loại thang đo	Theo thứ tự.
Đơn vị đo	Không có.
Thông tin đặc tả về số đo dẫn xuất	
Số đo dẫn xuất	Không có.
Hàm đo lường	Không có.
Thông tin đặc tả về chỉ báo	
Chỉ báo	Thanh tiến trình. Màu đỏ: 0 đến 0,8; Màu xanh: giữa 0,8 và 1.
Mô hình phân tích	Các phân tích đánh giá.
Thông tin đặc tả về tiêu chí quyết định	
Tiêu chí quyết định	Giá trị 3 trở lên: thỏa mãn.
Kết quả phép đo	
Giải thích chỉ báo	Dưới giá trị 3: chưa thỏa mãn, cần có các nỗ lực hành động dựa trên mức độ của lỗ hổng an toàn thông tin. Giá trị 3 trở lên: thỏa mãn, mỗi lớp có thể cho biết các vấn đề liên quan đến đánh giá.
Định dạng báo cáo đo	Đồ thị.
Các bên liên quan	

Người yêu cầu đo	Ban quản lý.
Người soát xét phép đo	Kiểm toán nội bộ/ kiểm toán bên ngoài.
Người sở hữu thông tin	Người quản lý hạ tầng thông tin.
Bộ phận thu thập thông tin	Đánh giá viên nội bộ/ đánh giá viên bên ngoài.
Bộ phận trao đổi thông tin	Đánh giá viên nội bộ và Người quản lý an toàn thông tin.
Tần suất triển khai	
Tần suất thu thập dữ liệu	Hàng năm.
Tần suất phân tích dữ liệu	Hàng năm.
Tần suất lập báo cáo các kết quả đo	Hàng năm.
Tần suất sửa đổi phép đo	12 tháng.
Tần suất thực hiện phép đo	Mỗi 12 tháng.

B.8 Đo lường soát xét các file log

Thông tin chung của phép đo	
Tên phép đo	**Đo lường soát xét các file log**
Số hiệu	Tùy theo tổ chức.
Mục đích	Đánh giá tình trạng tuân thủ việc thường xuyên soát xét các file log hệ thống thiết yếu.
Mục tiêu biện pháp quản lý	Biện pháp quản lý A.10.10 [TCVN ISO/IEC 27001:2009] Giám sát. Nhằm phát hiện các hoạt động xử lý thông tin trái phép (đã lập kế hoạch) Nhằm phát hiện các hoạt động xử lý thông tin trái phép của các hệ thống thiết yếu từ các file log hệ thống
Biện pháp quản lý (1)	Biện pháp quản lý A.10.10.2 [TCVN ISO/IEC 27001:2009] Giám sát việc sử dụng hệ thống. Các thủ tục giám sát việc sử dụng các phương tiện xử lý thông tin cần được thiết lập và kết quả giám sát cần phải được xem xét thường xuyên.
Đối tượng đo lường và các thuộc tính	
Đối tượng	Hệ thống.
Thuộc tính	Từng file log.
Thông tin đặc tả về số đo cơ bản (1)	
Số đo cơ bản	Số lượng file log.
Phương pháp đo	Tính tổng số các file log được liệt kê trong danh sách các file log soát xét.
Loại phương pháp đo	Khách quan.
Thang đo	Số nguyên từ 0 đến vô cùng.
Loại thang đo	Theo thứ tự.
Đơn vị đo	File log.
Thông tin đặc tả về số đo cơ bản (2)	
Số đo cơ bản	Số lượng các file log đã soát xét.
Phương pháp đo	Tính tổng số các file log trên toàn bộ hệ thống thuộc phạm vi hệ thống ISMS.
Loại phương pháp đo	Khách quan.
Thang đo	Số lượng.
Loại thang đo	Theo tỷ lệ.
Đơn vị đo	File log.
Thông tin đặc tả về số đo cơ bản (3)	
Số đo cơ bản	Số của các hệ thống trong phạm vi hệ thống ISMS.
Phương pháp đo	Số định danh của các file log đã soát xét.
Loại phương pháp đo	Khách quan.
Thang đo	Số lượng.

Loại thang đo	Theo tỷ lệ.
Đơn vị đo	File log.
Thông tin đặc tả về số đo dẫn xuất	
Số đo dẫn xuất	Tỷ lệ phần trăm các file log đánh giá đã soát xét trong mỗi khoảng thời gian.
Hàm đo lường	(Số file log đã soát xét trong một thời gian cụ thể) / (tổng số file log) * 100.
Thông tin đặc tả về chỉ báo	
Chỉ báo	Đồ thị đường của xu hướng qua các khoảng thời gian theo tỷ lệ soát xét các file log kiểm tra.
Mô hình phân tích	Xu hướng mong muốn là tăng tới 100%.
Thông tin đặc tả về tiêu chí quyết định	
Tiêu chí quyết định	Khi kết quả dưới 20%, cần thiết kiểm tra nguyên nhân gây ra hiệu suất kém.
Kết quả phép đo	
Giải thích chỉ báo	Giá trị thấp hơn giá trị xác định của tổ chức: không đạt yêu cầu. Cần thiết có hành động quản lý dựa trên lỗ hổng an toàn thông tin. Giá trị trên giá trị xác định của tổ chức có thể chỉ báo việc đầu tư quá mức ngoại trừ việc những cơ chế quản lý truy nhập này là cần thiết cho mỗi đánh giá rủi ro.
Định dạng báo cáo đo	Đồ thị đường mô tả xu hướng, với tóm tắt các kết quả và đề xuất các hành động quản lý.
Các bên liên quan	
Người yêu cầu đo	Người quản lý chịu trách nhiệm đối với hệ thống ISMS. Người quản lý an toàn thông tin.
Người soát xét phép đo	Người quản lý an toàn thông tin
Người sở hữu thông tin	Người quản lý an toàn thông tin
Bộ phận thu thập thông tin	Nhân viên an toàn thông tin.
Bộ phận trao đổi thông tin	Nhân viên an toàn thông tin.
Tần suất triển khai	
Tần suất thu thập dữ liệu	Hàng tháng.
Tần suất phân tích dữ liệu	Hàng tháng.
Tần suất lập báo cáo các kết quả đo	Hàng quý.
Tần suất sửa đổi phép đo	Soát xét và sửa đổi 2 năm/lần.
Tần suất thực hiện phép đo	2 năm/lần.

B.9 Đo lường quản lý bảo trì ISMS thường xuyên

Thông tin chung của phép đo	
Tên phép đo	**Đo lường quản lý bảo trì ISMS thường xuyên**
Số hiệu	Tùy theo tổ chức.
Mục đích	Đánh giá tính kịp thời trong các hoạt động bảo trì trong lịch trình.
Mục tiêu biện pháp quản lý	Biện pháp quản lý A.9.2 [TCVN ISO/IEC 27001:2009] Đảm bảo an toàn trang thiết bị. Nhằm ngăn ngừa sự mất mát, hư hại đánh cắp hoặc gây hại tài sản và sự gián đoạn hoạt động của tổ chức. (đã lập kế hoạch) Nhằm ngăn ngừa sự mất mát, hư hại đánh cắp hoặc gây hại tài sản và sự gián đoạn hoạt động của tổ chức thông qua bảo trì hệ thống thường xuyên.
Biện pháp quản lý (1)	Biện pháp quản lý A.9.2.4 [TCVN ISO/IEC 27001:2009] Duy trì thiết bị. Các thiết bị cần được duy trì một cách thích hợp nhằm đảm bảo luôn sẵn sàng và toàn vẹn.
Đối tượng đo lường và các thuộc tính	
Đối tượng	1. Bản kế hoạch/ lịch biểu dự kiến bảo trì hệ thống.

	2. Các bản ghi bảo trì hệ thống.
Thuộc tính	1. Ngày kế hoạch/ dự kiến bảo trì hệ thống. 2. Ngày hoàn thành bảo trì hệ thống.
Thông tin đặc tả về số đo cơ bản	
Số đo cơ bản	1. Ngày dự kiến bảo trì hệ thống. 2. Ngày hoàn thành bảo trì hệ thống. 3. Số lần bảo trì hệ thống đã lên kế hoạch. 4. Số lần bảo trì hệ thống đã thực hiện.
Phương pháp đo	1. Trích ngày dự kiến bảo trì hệ thống trong kế hoạch. 2. Trích ngày hoàn thành bảo trì hệ thống từ bản ghi. 3. Đếm số lần bảo trì hệ thống đã lên kế hoạch trong bản kế hoạch bảo trì hệ thống. 4. Đếm số lượng bản ghi bảo trì hệ thống.
Loại phương pháp đo	Khách quan.
Thang đo	1. Thời gian. 2. Thời gian. 3. Số nguyên từ 0 đến vô cùng. 4. Số nguyên từ 0 đến vô cùng.
Loại thang đo	1. Danh sách. 2. Danh sách. 3. Theo thứ tự. 4. Theo thứ tự.
Đơn vị đo	1. Khoảng thời gian. 2. Khoảng thời gian. 3. Sự kiện bảo trì. 4. Sự kiện bảo trì.
Thông tin đặc tả về số đo dẫn xuất	
Số đo dẫn xuất	Mức độ trễ đối với mỗi sự kiện bảo trì hoàn thành.
Hàm đo lường	Với mỗi sự kiện bảo trì hoàn thành: là hiệu [Ngày bảo trì theo dự kiến] - [Ngày bảo trì thực tế].
Thông tin đặc tả về chỉ báo	
Chỉ báo	1. Mức độ trễ bảo trì trung bình. 2. Tỷ lệ các sự kiện bảo trì hoàn thành. 3. Xu hướng của mức độ trễ bảo trì trung bình. 4. Xu hướng của tỷ lệ các sự kiện bảo trì hoàn thành.
Mô hình phân tích	1. Là tỷ số [tổng của (Mức độ trễ đối với mỗi sự kiện bảo trì hoàn thành)] / [Số lượng sự kiện bảo trì đã hoàn thành]. 2. Là tỷ số [Số lượng sự kiện bảo trì đã hoàn thành] / [Số lượng sự kiện bảo trì đã lên kế hoạch]. 3. So sánh chỉ báo 1 với các báo cáo đo tần suất trước. 4. So sánh chỉ báo 2 với các báo cáo đo tần suất trước.
Thông tin đặc tả về tiêu chí quyết định	
Tiêu chí quyết định	1. Tùy theo tổ chức, ví dụ: nếu mức độ trễ trung bình thường quá 3 ngày, cần thiết kiểm tra nguyên nhân. 2. Tỷ lệ các sự kiện bảo trì hoàn thành cần lớn hơn 0,9. 3. Xu hướng cần ổn định hoặc gần với 0. 4. Xu hướng cần ổn định hoặc có chiều hướng đi lên.
Kết quả phép đo	
Giải thích chỉ báo	Các chỉ số giúp đánh giá chất lượng tiến trình bảo trì hệ thống thiết bị.
Định dạng báo cáo đo	Biểu đồ dạng đường
Các bên liên quan	
Người yêu cầu đo	Người quản lý chịu trách nhiệm đối với hệ thống ISMS. Người quản lý an toàn thông tin.
Người soát xét phép đo	Người quản lý an toàn thông tin.
Người sở hữu thông tin	Người quản trị hệ thống.
Bộ phận thu thập thông tin	Nhân viên an toàn thông tin.

Bộ phận trao đổi thông tin	Nhân viên an toàn thông tin.
Tần suất triển khai	
Tần suất thu thập dữ liệu	Hàng năm.
Tần suất phân tích dữ liệu	Hàng năm.
Tần suất lập báo cáo các kết quả đo	Hàng năm.
Tần suất sửa đổi phép đo	Hàng năm.
Tần suất thực hiện phép đo	Hàng năm.

B.10 An toàn trong các thỏa thuận với bên thứ ba

Thông tin chung của phép đo	
Tên phép đo	**An toàn trong các thỏa thuận với bên thứ ba**
Số hiệu	Tùy theo tổ chức.
Mục đích	
Mục tiêu biện pháp quản lý	Biện pháp quản lý A.6.2 [TCVN ISO/IEC 27001:2009] Các bên tham gia bên ngoài. Nhằm duy trì an toàn đối với thông tin và các phương tiện xử lý thông tin của tổ chức được truy cập, xử lý, truyền thông, hoặc quản lý bởi các bên tham gia bên ngoài tổ chức.
Biện pháp quản lý (1)	Biện pháp quản lý A.6.2.3 [TCVN ISO/IEC 27001:2009] Giải quyết an toàn trong các thỏa thuận với bên thứ ba. Các thỏa thuận với bên thứ ba liên quan đến truy cập, xử lý, truyền thông hoặc quản lý thông tin hay phương tiện xử lý thông tin của tổ chức hoặc các sản phẩm dịch vụ phụ trợ của các phương tiện xử lý thông tin phải bao hàm tất cả các yêu cầu an toàn liên quan.
Đối tượng đo lường và các thuộc tính	
Đối tượng	Các thỏa thuận an toàn thông tin với bên thứ ba.
Thuộc tính	Các điều khoản bảo mật hoặc các yêu cầu trong các thỏa thuận an toàn thông tin với bên thứ ba.
Thông tin đặc tả về số đo cơ bản (1)	
Số đo cơ bản	Số lượng các thỏa thuận với bên thứ ba.
Phương pháp đo	Soát xét, đếm số lượng các thỏa thuận với bên thứ ba.
Loại phương pháp đo	Khách quan.
Thang đo	Số nguyên từ 0 đến vô cùng.
Loại thang đo	Theo thứ tự.
Đơn vị đo	Thỏa thuận với bên thứ ba.
Thông tin đặc tả về số đo cơ bản (2)	
Số đo cơ bản	Một số chuẩn các yêu cầu về an toàn thông tin với bên thứ ba.
Phương pháp đo	Xác định số lượng các yêu cầu về an toàn thông tin phải được chỉ ra trong mỗi thỏa thuận với đối tác (căn cứ vào chính sách an toàn thông tin của tổ chức).
Loại phương pháp đo	Khách quan.
Thang đo	Số nguyên từ 0 đến vô cùng.
Loại thang đo	Theo thứ tự.
Đơn vị đo	Số yêu cầu.
Thông tin đặc tả về số đo cơ bản (3)	
Số đo cơ bản	Số lượng các yêu cầu về an toàn thông tin được đề cập đến trong mỗi thỏa thuận với bên thứ ba.
Phương pháp đo	Soát xét, đếm số lượng các yêu cầu về an toàn thông tin được đề cập đến trong mỗi thỏa thuận với bên thứ ba.
Loại phương pháp đo	Khách quan.
Thang đo	Số nguyên từ 0 đến vô cùng.
Loại thang đo	Theo thứ tự.
Đơn vị đo	Số yêu cầu.

Thông tin đặc tả về số đo dẫn xuất	
Số đo dẫn xuất	Tỷ lệ phần trăm trung bình các yêu cầu hợp lý về an toàn thông tin được đề cập đến trong thỏa thuận với bên thứ ba.
Hàm đo lường	Tổng của (với mỗi thỏa thuận (Số các yêu cầu cần thiết - số lượng các yêu cầu đề cập đến)) / Số lượng các thỏa thuận.
Thông tin đặc tả về chỉ báo	
Chỉ báo	1. Tỷ lệ trung bình về sai khác giữa số các yêu cầu hợp lý và số yêu cầu đề cập đến. 2. Xu hướng của tỷ lệ.
Mô hình phân tích	1. Tổng của (với mỗi thỏa thuận ([Tổng số các yêu cầu an toàn đề cập đến] - [Số chuẩn các yêu cầu an toàn]) / [Số lượng các thỏa thuận của bên thứ ba]. 2. So sánh chỉ báo 1) với báo cáo đo trước đó.
Thông tin đặc tả về tiêu chí quyết định	
Tiêu chí quyết định	1. Chỉ báo 1) nên lớn hơn 0,9. 2. Chỉ báo 2) nên có xu hướng ổn định hoặc đi lên.
Kết quả phép đo	
Giải thích chỉ báo	Chỉ báo này cung cấp cái nhìn sâu vào khả năng chuyển giao chức năng triển khai cho bên thứ ba để giải quyết các yêu cầu an toàn.
Định dạng báo cáo đo	Biểu đồ đường mô tả xu hướng so với các báo cáo đo thường kỳ trước, có thể đưa ra được tổng kết ngắn gọn và các hành động quản lý.
Các bên liên quan	
Người yêu cầu đo	Người quản lý chịu trách nhiệm đối với hệ thống ISMS. Người quản lý an toàn thông tin.
Người soát xét phép đo	Người quản lý an toàn thông tin.
Người sở hữu thông tin	Phòng quản trị hợp đồng.
Bộ phận thu thập thông tin	Nhân viên toàn thông tin.
Bộ phận trao đổi thông tin	Nhân viên an toàn thông tin.
Tần suất triển khai	
Tần suất thu thập dữ liệu	Hàng tháng.
Tần suất phân tích dữ liệu	Hàng quý.
Tần suất lập báo cáo các kết quả đo	Hàng quý.
Tần suất sửa đổi phép đo	2 năm/lần.
Tần suất thực hiện phép đo	Áp dụng trong 2 năm.

Thư mục tài liệu tham khảo

[1] ISO 9000:2005, Quality management systems — Fundamentals and vocabulary;

[2] ISO/IEC 27002:2005, Information technology — Security techniques — Code of practice for information security management;

[3] ISO/IEC 15504-3:2004, Information technology — Process assessment — Part 3: Guidance on performing an assessment;

[4] ISO/IEC 15939:2007, Systems and software engineering — Measurement process

[5] ISO/IEC 27005:2008, Information technology — Security techniques — Information security risk management;

[6] ISO/TR 10017:2003, Guidance on statistical techniques for ISO 9001:2000;

[7] ISO Guide 99:2007, International vocabulary of metrology — Basic and general concepts and associated terms (VIM);

[8] NIST Special Publication 800-55, Revision 1, Performance Measurement Guide for Information Security, July 2008;

[9] ISO/IEC TR 18044:2004, Information technology — Security techniques — Information security incident management;

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