TCVN **TIÊU CHUẨN QUỐC GIA**

TCVN 9965:2013
ISO/IEC 27013:2012

CÔNG NGHỆ THÔNG TIN - KỸ THUẬT AN NINH - HƯỚNG DẪN TÍCH HỢP TRIỂN KHAI TCVN ISO/IEC 27001 VÀ ISO/IEC 20000-1

Information technology - Security techniques - Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1

HÀ NỘI - 2013

Mục lục **Trang**

Lời nói đầu

TCVN 9965:2013 do Ban Kỹ thuật tiêu chuẩn quốc gia TCVN/JTC1 "*Công nghệ Thông tin*" biên soạn, Tổng cục Tiêu chuẩn Đo lường Chất lượng đề nghị, Bộ Khoa học và Công nghệ công bố.

TCVN 9965:2013 hoàn toàn tương đương với ISO/IEC 27013:2012.

Lời giới thiệu

Mối quan hệ giữa an ninh thông tin và quản lý dịch vụ rất chặt chẽ mà nhiều tổ chức đã nhận diện các lợi ích của việc đáp ứng đối với cả hai tiêu chuẩn: TCVN ISO/IEC 27001 về an ninh thông tin và ISO/IEC 20000-1 về quản lý dịch vụ. Với một tổ chức, điều này phổ biến để tăng cường cách thức vận hành để phù hợp với các yêu cầu của một Tiêu chuẩn quốc tế và tạo ra các nâng cấp sau này để phù hợp với các yêu cầu của các tiêu chuẩn khác.

Một số lượng các ưu điểm trong việc triển khai một hệ thống quản lý tích hợp được không chỉ được chia thành các dịch vụ được cung cấp mà còn cho việc bảo vệ của các tài sản thông tin. Các lợi ích này có thể được trải nghiệm khi một tiêu chuẩn được triển khai trước các tiêu chuẩn khác, hoặc cả hai tiêu chuẩn đều được triển khai đồng thời. Đặc biệt, việc quản lý và các quy trình tổ chức có thể dẫn đến các lợi ích từ các điểm giống nhau giữa các Tiêu chuẩn quốc tế và các mục tiêu chung giữa chúng.

Các lợi ích chính của một triển khai tích hợp bao gồm:

a) Sự tin tưởng cho các khách hàng bên trong và bên ngoài của tổ chức, của một dịch vụ an ninh và hiệu quả;

b) Giá thành thấp hơn của một chương trình tích hợp của hai dự án, khi việc hướng tới cả quản lý dịch vụ và an ninh thông tin là thành phần của một chiến lược của tổ chức;

c) Một giảm thiểu thời gian triển khai dựa trên việc phát triển tích hợp của các quy trình phổ biến từ cả hai tiêu chuẩn;

d) Việc loại bỏ các trùng lặp không cần thiết;

e) Sự hiểu biết hơn của quản lý dịch vụ và cá nhân an ninh của mỗi quan điểm mỗi bên;

f) Một tổ chức được chứng nhận về TCVN ISO/IEC 27001 có thể dễ dàng đáp ứng các yêu cầu an ninh thông tin của ISO/IEC 20000-1:2011, Điều 6.6 ở cả hai Tiêu chuẩn được bổ sung theo yêu cầu.

Hướng dẫn dựa trên các phiên bản đã công bố của cả hai tiêu chuẩn quốc tế: TCVN ISO/IEC 27001 và ISO/IEC 20000-1:2011.

Tiêu chuẩn này hướng đến việc sử dụng bởi các cá nhân có hiểu biết về cả hai tiêu chuẩn quốc tế, trong một hoặc hai tiêu chuẩn TCVN ISO/IEC 27001 và ISO/IEC 20000-1 hoặc không thuộc tiêu chuẩn nào.

Tiêu chuẩn này mong đợi rằng tất cả người đọc được truy cập để sao chép cả hai tiêu chuẩn quốc tế. Do đó, tiêu chuẩn này không tái sử dụng các phần của tiêu chuẩn khác. Tương tự, tiêu chuẩn này không mô tả tất cả các phần của mỗi tiêu chuẩn quốc tế một cách toàn diện. Các phần đó chỉ ra vấn đề trùng lặp được mô tả chi tiết.

Tiêu chuẩn này không đưa ra hướng dẫn tương tự với các thay đổi luật pháp và quy định bên ngoài sự kiểm soát của tổ chức. Điều đó có thể thay đổi tùy theo quốc gia và tác động của việc hoạch định một hệ thống quản lý của tổ chức.

Công nghệ thông tin - Kỹ thuật an ninh - Hướng dẫn tích hợp triển khai TCVN ISO/IEC 27001 và ISO/IEC 20000-1

Information technology - Security techniques - Guidance on the intergrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1

1 Phạm vi áp dụng

Tiêu chuẩn này cung cấp hướng dẫn tích hợp triển khai TCVN ISO/IEC 27001 ISO/IEC 20000-1 cho các tổ chức có ý định hoặc:

a) Triển khai TCVN ISO/IEC 27001 khi ISO/IEC 20000-1 đã được triển khai, hoặc ngược lại;

b) Triển khai TCVN ISO/IEC 27001 và ISO/IEC 20000-1 cùng nhau;

c) Tích hợp hệ thống quản lý TCVN ISO/IEC 27001 và ISO/IEC 20000-1 hiện có.

Tiêu chuẩn này cũng nêu bật các điểm khác biệt của việc tích hợp triển khai TCVN ISO/IEC 27001 và ISO/IEC 20000-1.

Thực tế, TCVN ISO/IEC 27001 và ISO/IEC 20000-1 cũng có thể tích hợp với các hệ thống quản lý khác như TCVN ISO 9001 và TCVN ISO 14001.

2 Tài liệu viện dẫn

Các tài liệu viện dẫn sau là rất cần thiết cho việc 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 (nếu có).

TCVN ISO/IEC 27001:2009 Công nghệ thông tin - Kỹ thuật an ninh - Hệ thống quản lý an ninh thông tin - Các yêu cầu (*ISO/IEC 27001:2005; Information technology - Security techniques - Information security management systems - Requirements*)

ISO/IEC 20000-1:2011[1] Information technology - Service management - Service management system requirements (*Công nghệ thông tin - Quản lý dịch vụ - Các yêu cầu hệ thống quản lý dịch vụ*)

ISO/IEC 27000:2009 Information technology - Security techniques - Information security management systems - Overview and vocabulary (*Công nghệ thông tin - Kỹ thuật an ninh - Hệ thống quản lý an ninh thông tin - Tổng quan và từ vựng*)

---

[1] Hiện nay, trong hệ thống tiêu chuẩn quốc gia đã có TCVN 8695:2011 Công nghệ thông tin – Quản lý dịch vụ - Phần 1: Các yêu cầu (ISO/IEC 20000-1:2005 Information technology - Service management - Specification)

3 Thuật ngữ, thuật ngữ viết tắt và định nghĩa

Tiêu chuẩn này sử dụng các thuật ngữ và định nghĩa nêu ra trong ISO/IEC 27000:2009 và ISO/IEC 20000-1 và các thuật ngữ, định nghĩa sau:

ISMS - hệ thống quản lý an ninh thông tin (*information security management system*) (từ TCVN ISO/IEC 27001:2005)

SMS - hệ thống quản lý dịch vụ (*service management system*) (từ ISO/IEC 20000-1)

Phụ lục A của tiêu chuẩn này so sánh nội dung giữa TCVN ISO/IEC 27001 và ISO/IEC 20000-1:2011 theo từng Điều.

Phụ lục B của tiêu chuẩn này so sánh thuật ngữ được định nghĩa trong:

- ISO/IEC 27000:2009, Bảng thuật ngữ dùng cho TCVN ISO/IEC 27001;
- Thuật ngữ được dùng trong TCVN ISO/IEC 27001;
- Thuật ngữ được định nghĩa hoặc dùng trong ISO/IEC 20000-1:2011.

4 Tổng quan về TCVN ISO/IEC 27001 và ISO/IEC 20000-1

4.1 Hiểu biết về tiêu chuẩn quốc tế

Một tổ chức nên có sự am hiểu về các đặc trưng, sự giống và khác nhau giữa TCVN ISO/IEC 27001 và ISO/IEC 20000-1 trước khi hoạch định một hệ thống quản lý tích hợp. Điều này giúp tối đa hoá thời gian và nguồn lực sẵn có cho việc triển khai. Các Điều từ 4.2 tới 4.4. của tiêu chuẩn này giới thiệu các khái niệm chính làm nền tảng cho cả hai tiêu chuẩn, nhưng không được dùng thay thế cho việc soát xét chi tiết.

4.2 Khái niệm TCVN ISO/IEC 27001

TCVN ISO/IEC 27001 đưa ra mô hình cho việc thiết lập, thực thi, vận hành, giám sát, xem xét, duy trì và cải tiến một ISMS để bảo vệ tài sản thông tin. Tài sản thông tin bao gồm các thông tin dưới bất kỳ dạng nào, được lưu giữ dưới mọi hình thức, và được dùng cho bất kỳ mục đích nào bởi, hoặc bên trong một tổ chức.

Để phù hợp với TCVN ISO/IEC 27001, tổ chức phải triển khai một ISMS dựa trên quy trình đánh giá rủi ro để nhận diện các rủi ro đối với các tài sản thông tin. Tổ chức phải chọn lựa, thiết lập, giám sát và xem xét một loạt các biện pháp để quản lý các rủi ro như một phần của công việc này. Các biện pháp đó được biết tới như các kiểm soát. Tổ chức phải xác định các mức chấp nhận rủi ro, tính tới các yêu cầu doanh nghiệp và yêu cầu ràng buộc từ bên ngoài. Ví dụ về yêu cầu ràng buộc từ bên ngoài như yêu cầu về pháp lý và quy định hoặc nghĩa vụ hợp đồng.

TCVN ISO/IEC 27001 có thể dùng cho tất cả các tổ chức thuộc mọi loại hình và quy mô.

4.3 Khái niệm ISO/IEC 20000-1

ISO/IEC 20000-1 có thể dùng cho các tổ chức hoặc thành phần của các tổ chức,có sử dụng hoặc cung cấp dịch vụ. Tiêu chuẩn này mang lại lợi ích cho cả khách hàng và bên cung cấp dịch vụ. Tuy nhiên, tất cả các quy trình trong tiêu chuẩn này đều được kiểm soát bởi bên cung cấp dịch vụ, và chỉ bên cung cấp

dịch vụ cần phù hợp với tiêu chuẩn này. Tiêu chuẩn này chủ yếu liên quan tới việc đảm bảo rằng các dịch vụ thỏa mãn các yêu cầu dịch vụ và mang lại lợi ích cho cả khách hàng và bên cung cấp dịch vụ.

Việc quản lý dịch vụ chi phối và kiểm soát các tài nguyên và hoạt động của bên cung cấp dịch vụ trong việc thiết kế, phát triển, chuyển đổi, chuyển giao và cải tiến dịch vụ để thỏa mãn các yêu cầu dịch vụ như đã thỏa thuận với (các) khách hàng.

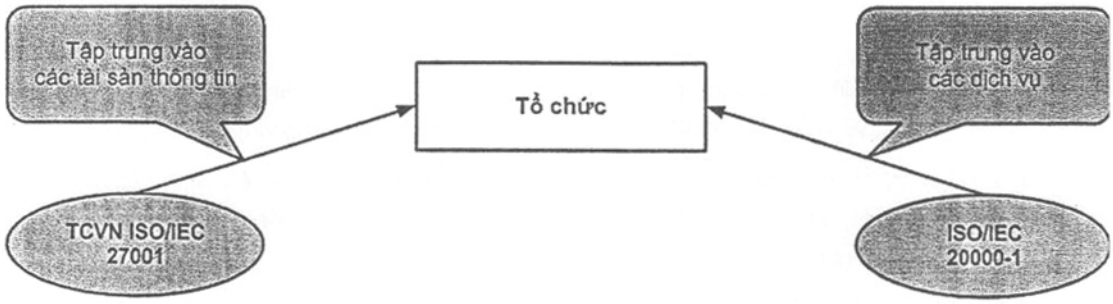
Để thỏa mãn đầy đủ các yêu cầu của tiêu chuẩn này, bên cung cấp dịch vụ nên thực thi một dải các quy trình quản lý dịch vụ cụ thể. Các quy trình này bao gồm quản lý sự cố, quản lý thay đổi và quản lý vấn đề giữa các quản lý khác. Quản lý an ninh thông tin là một trong các quy trình quản lý dịch vụ của ISO/IEC 20000-1.

ISO/IEC 20000-1 có thể được dùng cho tất cả các tổ chức thuộc mọi loại hình và quy mô.

4.4 Điểm giống và khác nhau

Quản lý dịch vụ và quản lý an ninh thông tin thường được xem là không liên kết hay độc lập nhau. Về khía cạnh không liên kết, quản lý dịch vụ thường liên quan đến tính hiệu quả và tính lợi nhuận, trong khi đó, quản lý an ninh thông tin thường không được hiểu là nền tảng cơ sở đối với việc chuyển giao dịch vụ hiệu quả. Kết quả là quản lý dịch vụ thường được thực thi đầu tiên. Tuy nhiên, như chỉ ra ở Hình 1, trong các yêu cầu quản lý dịch vụ theo ISO/IEC 20000-1, cũng bao gồm nhiều mục tiêu và biện pháp kiểm soát theo Phụ lục A trong TCVN ISO/IEC 27001.

Quản lý an ninh thông tin và quản lý dịch vụ rõ ràng đề cập đến các quy trình và hoạt động giống nhau, mặc dù mỗi hệ thống quản lý nêu bật một số chi tiết hơn so với các chi tiết khác. Chi tiết xem phụ lục A . Khi sử dụng cả hai tiêu chuẩn này, nên hiểu rằng chúng có những đặc trưng khác biệt trong nhiều khía cạnh. Ví dụ, phạm vi của chúng khác nhau, xem Điều 5.2 của tiêu chuẩn này. Chúng cũng có những mục đích khác nhau. ISO/IEC 20000-1 được thiết kế để đảm bảo rằng tổ chức cung cấp các dịch vụ hiệu quả, trong khi TCVN ISO/IEC 27001 được thiết kế cho phép tổ chức quản lý rủi ro an ninh thông tin và phòng ngừa các sự cố an ninh.



Đặc thù của TCVN ISO/IEC 27001	Các phần chung (một số phần trùng lặp, một số phần khác biệt)		Đặc thù của ISO/IEC 20000-1
• Phân lớp thông tin • Quản lý tài sản thông tin	• Quản lý năng lực • Quản lý thay đổi • Quản lý cấu hình • Quản lý yêu cầu dịch vụ và sự cố • Quản lý vấn đề • Quản lý triển khai và phát hành	• Quản lý tài nguyên • Đánh giá rủi ro • Vai trò và trách nhiệm • Quản lý an ninh thông tin • Quản lý tính sẵn có và tính liên tục của dịch vụ • Quản lý nhà cung cấp	• Lập ngân sách và tài chính dịch vụ • Quản lý quan hệ doanh nghiệp • Thiết kế và chuyển dịch dịch vụ mới hoặc đã thay đổi • Quản lý mức dịch vụ
Các phần chung (giống nhau giữa các tiêu chuẩn)			
• Cải tiến liên tục • Tuân thủ pháp luật và quy định • Xem xét quản lý		• PDCA • Đào tạo và nhận thức • Quản lý tài liệu	

Hình 1 - So sánh khái niệm giữa TCVN ISO/IEC 27001 và ISO/IEC 20000-1

5 Cách tiếp cận cho việc tích hợp triển khai

5.1 Tổng quan

Việc hoạch định của một tổ chức để triển khai TCVN ISO/IEC 27001 và ISO/IEC 20000-1 có thể rơi vào một trong ba tình huống:

- Có sắp xếp quản lý chuyên trách bao gồm cả quản lý an ninh thông tin và quản lý dịch vụ (các hệ thống quản lý chính thức cũng có thể tồn tại cho các lĩnh vực khác, như quản lý chất lượng);
- Có hệ thống quản lý dựa trên một tiêu chuẩn;
- Có các hệ thống quản lý tách biệt dựa trên hai tiêu chuẩn, nhưng không tích hợp.

Tổ chức hoạch định việc triển khai hệ thống quản lý tích hợp phải cân nhắc ít nhất các điểm sau:

a) (Các) hệ thống quản lý khác đã sử dụng (như hệ thống quản lý chất lượng);

b) Tất cả các dịch vụ, quy trình và các sự phụ thuộc giữa chúng trong hoàn cảnh hệ thống quản lý tích hợp;

c) Các thành phần của mỗi tiêu chuẩn có thể được hợp nhất và cách thức chúng có thể hợp nhất;

d) Các thành phần vẫn còn tách biệt;

e) Tác động của hệ thống quản lý tích hợp đối với các khách hàng, bên cung cấp và các bên khác;

f) Tác động lên công nghệ đang sử dụng;

g) Tác động lên, hoặc gây rủi ro cho các dịch vụ và quản lý dịch vụ;

h) Tác động lên, hoặc gây rủi ro cho việc an ninh thông tin và quản lý an ninh thông tin;

i) Giáo dục và đào tạo trong hệ thống quản lý tích hợp;

j) Các giai đoạn và trình tự của việc tiến hành hoạt động.

5.2 Xem xét về phạm vi áp dụng

Phạm vi mà hai tiêu chuẩn này khác nhau đáng kể trên vấn đề phạm vi áp dụng, cụ thể hơn là tài sản gì, quy trình nào và bộ phận nào của tổ chức nên bao gồm trong hệ thống quản lý.

ISO/IEC 20000-1 đề cập tới các yêu cầu: thiết kế, chuyển dịch, chuyển giao và cải tiến dịch vụ để thỏa mãn các yêu cầu. Điều này được triển khai thông qua một tập các quy trình. Do đó phạm vi của ISO/IEC 20000-1 bao gồm các quy trình quản lý bên trong tổ chức, và các dịch vụ được cung cấp. TCVN ISO/IEC 27001 liên quan đến cách thức quản lý rủi ro an ninh thông tin. Phạm vi của TCVN ISO/IEC 27001 bao quát các thành phần của các hoạt động của chính nó mà tổ chức mong muốn an toàn. Theo đó, phạm vi triển khai của hai tiêu chuẩn được mô tả khác nhau. Do đó có thể triển khai TCVN ISO/IEC 27001 với cùng phạm vi như với ISO/IEC 20000-1, nhưng ISO/IEC 20000-1 không thể được áp dụng cho toàn bộ tổ chức trừ phi tổ chức đó hoàn toàn là bên cung cấp dịch vụ.

Do vậy một số quy trình, tài sản và vai trò trong tổ chức có thể bị loại bỏ khỏi phạm vi cho một ISMS được phát triển để đáp ứng với TCVN ISO/IEC 27001. Với ISO/IEC 20000-1, những điều này có thể không bị loại bỏ khỏi phạm vi nếu chúng là một phần, hoặc góp phần vào, dịch vụ trong phạm vi của SMS. Phạm vi của ISMS cũng có thể được xác định một cách duy nhất bằng một gianh giới vật lý rõ ràng, như vành đai an ninh.

Trong một số trường hợp, hai tiêu chuẩn này có thể không được thiết lập cho tất cả, hay thậm chí một thành phần nào, trong các hoạt động tổ chức. Ví dụ, nếu tổ chức không thể tuân thủ theo các yêu cầu của ISO/IEC 20000-1 vì nó không quản trị mọi quy trình được vận hành bởi các bên khác.

Tổ chức có thể triển khai SMS và ISMS với một số trùng lặp giữa các phạm vi áp dụng khác nhau. Trong đó, các hoạt động nằm trong phạm vi áp dụng của cả hai tiêu chuẩn này, hệ thống quản lý tích hợp phải tính tới cả hai tiêu chuẩn này, xem phụ lục A của tiêu chuẩn này. Khác biệt phạm vi áp dụng có thể làm nảy sinh một số dịch vụ bao gồm trong SMS nhưng bị loại trừ trong ISMS. Tương tự, SMS có thể loại trừ các quy trình và chức năng của ISMS. Ví dụ, một số tổ chức chọn triển khai một ISMS chỉ với các chức năng truyền thông và vận hành, trong khi các dịch vụ quản lý ứng dụng bao gồm trong SMS. Ngược lại, ISMS có thể được bao gồm tất cả các dịch vụ, trong khi SMS chỉ bao gồm các dịch vụ cho một khách hàng nào đó hoặc một số dịch vụ cho tất cả các khách hàng. Tổ chức phải cân đối các phạm vi của các tiêu chuẩn nhiều nhất có thể để đảm bảo rằng các hệ thống quản lý có thể được tích hợp thành công.

CHÚ THÍCH Hướng dẫn về xác định phạm vi cho ISO/IEC 20000-1 sẵn có trong ISO/IEC 20000-3:2012, Hướng dẫn về xác định phạm vi và tính áp dụng được của ISO/IEC 20000-1.

5.3 Các kịch bản tiền triển khai

5.3.1 Tổng quan

Tổ chức hoạch định một hệ thống quản lý tích hợp có thể ở một trong ba tình huống, như được mô tả trong các Điều từ 5.3.2 tới 5.3.4 của tiêu chuẩn này. Trong tất cả các trường hợp, tổ chức có một số dạng quy trình quản lý, nếu không thì tổ chức không tồn tại. Các điều bên dưới cung cấp các gợi ý cho việc triển khai ở một trong ba trạng thái cũng được mô tả trong Điều 5.1 của tiêu chuẩn này.

5.3.2 Không có tiêu chuẩn nào được sử dụng làm cơ sở cho hệ thống quản lý

Dễ dàng giả định rằng nơi nào không tiêu chuẩn nào được thực hiện thì không có các chính sách, quy trình và thủ tục, và vì thế, tình huống là đơn giản để giải quyết. Không may, đây là một quan niệm sai. Các tổ chức không có hệ thống quản lý dựa trên TCVN ISO/IEC 27001 hoặc ISO/IEC 20000-1 rất có thể đã có dạng nào đó của hệ thống quản lý. Dạng này sau đó được thích nghi để đạt tới việc phù hợp với một hoặc cả hai tiêu chuẩn.

Quyết định liên quan đến thứ tự theo đó hai hệ thống quản lý được thực hiện phải dựa trên các nhu cầu của doanh nghiệp. Các quyết định có thể bị ảnh hưởng bởi liệu khuyến khích là việc vị trí cạnh tranh khi dùng tiêu chuẩn này hay tiêu chuẩn khác, hay nhu cầu để chứng tỏ các yêu cầu của tiêu chuẩn này hay tiêu chuẩn khác cho một khách hàng hiện có hoặc một khách hàng mới.

Quyết định quan trọng khác là liệu việc triển khai hệ thống quản lý dựa trên cả hai tiêu chuẩn từ lúc bắt đầu, hay thiết lập một hệ thống quản lý dựa trên một tiêu chuẩn sau đó mở rộng để bao quát các yêu cầu của các tiêu chuẩn kia, xem Điều 5.3.3 của tiêu chuẩn này. Cả hai tiêu chuẩn có thể được triển khai đồng thời, nếu các hoạt động và nỗ lực triển khai có thể được phối hợp và sự trùng lặp được giảm thiểu. Tuy nhiên, tùy theo bản chất của tổ chức, cần thận trọng để bắt đầu với tiêu chuẩn này và sau đó triển khai tiêu chuẩn kia.

Các cân nhắc này được minh họa trong các kịch bản sau đây.

a) Tổ chức cung cấp dịch vụ bắt đầu với việc triển khai ISO/IEC 20000-1 và sau đó, khai thác từ các bài học rút ra trong việc triển khai đó, mở rộng hệ thống quản lý bao gồm cả TCVN ISO/IEC 27001.

b) Tổ chức sử dụng các bên cung cấp, bao gồm cả các bên khác, để chuyển giao một vài thành phần dịch vụ tập trung trước tiên vào ISO/IEC 20000-1. Điều này cung cấp nhiều yêu cầu hơn cho các bên khác, kể cả việc quản lý bên cung cấp. Điều này cho phép giải quyết các vấn đề về quản lý bên cung cấp và các kiểm soát quy trình. Tổ chức sau đó phải chuyển sang TCVN ISO/IEC 27001.

c) Tổ chức nhỏ tập trung vào một tiêu chuẩn hoặc là TCVN ISO/IEC 27001, hoặc là ISO/IEC 20000-1, tùy theo độ tin cậy vào hệ thống dịch vụ hoặc an ninh thông tin.

d) Tổ chức lớn với việc chuyển giao dịch vụ nội bộ triển khai như một dự án. Nếu việc này là không thể được, phải phân chia việc thực hiện thành hai dự án con song song bên trong một chương trình bao quát toàn bộ công việc. Mỗi dự án con phải quản lý một tiêu chuẩn, và tích hợp các triển khai như một dự án con tiếp theo. Nếu cách tiếp cận này được chọn, Điều quan trọng là cần đảm bảo rằng việc thực hiện là tương thích khi chúng được phát triển. Điều này có thể đưa vào tổng phí phụ và rủi ro thêm cho kết quả nên chỉ được dùng nếu không có phương án khác.

e) Bất kỳ tổ chức nào coi tầm quan trọng của an ninh thông tin là ở mức cao đều phải thực hiện ISMS trước hết mà tuân thủ các yêu cầu của TCVN ISO/IEC 27001. Giai đoạn tiếp theo nên là việc mở

rộng của hệ thống quản lý đó để đáp ứng các yêu cầu của ISO/IEC 20000-1, hỗ trợ an ninh thông tin.

Cuộc họp của nhóm công tác tích hợp trong quá trình triển khai hai tiêu chuẩn giúp đảm đảm bảo việc liên kết hai tiêu chuẩn.

5.3.3 Tồn tại một hệ thống quản lý thỏa mãn đầy đủ yêu cầu của một trong hai tiêu chuẩn

Khi một hệ thống quản lý đã phù hợp với một trong hai tiêu chuẩn rồi, mục đích chính phải là tích hợp với các yêu cầu của tiêu chuẩn kia. Điều này phải được thực hiện mà không gây tổn thất dịch vụ hoặc gây nguy hiểm cho an ninh thông tin của dịch vụ. Tuy nhiên, hệ thống quản lý tồn tại phải được chia nhỏ thành các phần riêng lẻ. Điều này phải được lên kế hoạch kỹ lưỡng từ trước, với tài liệu hiện có được các chuyên gia về tiêu chuẩn hiện có xem xét để xem cái nào cần đưa vào, và được xem xét bởi các chuyên gia trong tiêu chuẩn đã được triển khai.

Tổ chức phải nhận diện thuộc tính của hệ thống quản lý đã được thực hiện, bao gồm ít nhất các phần sau:

a) Phạm vi áp dụng;

b) Cấu trúc tổ chức;

c) Các chính sách;

d) Các hoạt động hoạch định;

e) Thẩm quyền và trách nhiệm;

f) Thực hành;

g) Phương thức quản lý rủi ro;

h) Các quy trình;

i) Các thủ tục;

j) Thuật ngữ và định nghĩa;

k) Tài nguyên.

Các thuộc tính này phải được xem xét để thiết lập cách chúng có thể được áp dụng cho hệ thống quản lý tích hợp. Nếu cách tiếp cận hai-bước được sử dụng, với hệ thống quản lý xem như đang ở bước một, bước hai là hệ thống quản lý kia được triển khai. Phạm vi áp dụng cho mỗi bước phải được định rõ và chấp thuận trước khi bắt đầu triển khai bất kỳ công việc nào.

5.3.4 Tồn tại các hệ thống quản lý riêng rẽ thỏa mãn đầy đủ yêu cầu của từng tiêu chuẩn

Trường hợp cuối cùng có lẽ là phức tạp nhất. Điều này giải thích cho vấn đề về phạm vi, xem Điều 5.2 của tiêu chuẩn này. Điều này có thể khi một tổ chức đã triển khai TCVN ISO/IEC 27001 trong một lĩnh vực của tổ chức, và đã triển khai ISO/IEC 20000-1 cho một lĩnh vực khác. Tổ chức có thể quyết định áp dụng tiêu chuẩn nay hoặc tiêu chuẩn kia trong toàn bộ phạm vi hoạt động rộng hơn. Tại một số thời điểm, các hệ thống quản lý được triển khai cùng các hoạt động. Theo phương án khác, hai tổ chức có thể hoạch định để hợp nhất. Một tổ chức đã chứng tỏ phù hợp với TCVN ISO/IEC 270001, trong khi tổ chức kia đã chứng tỏ phù hợp với ISO/IEC 20000-1.

Việc xem xét thiết lập từ điểm bắt đầu, nhằm đạt tới các điểm sau:

a) Nhận diện và dẫn chứng các phạm vi hiện có và được đề nghị, theo đó từng tiêu chuẩn áp dụng, đặc biệt chú ý tới các điểm khác biệt;

b) So sánh các hệ thống quản lý hiện có và thiết lập nếu có bất kỳ khía cạnh không tương thích lẫn nhau nào;

c) Bắt đầu đưa các bên liên quan trong cả hai hệ thống quản lý tham gia vào với bên kia;

d) Lên kế hoạch cho cách tiếp cận tốt nhất cho một hệ thống quản lý tích hợp:

   1) Bắt đầu với một kế hoạch đề cương rất rộng;

   2) Xem xét Điều này ở các mức khác nhau trong tổ chức để bổ sung các chi tiết;

   3) Cung cấp thông tin phản hồi và các giải pháp gợi ý cho mức thẩm quyền tương ứng để cho phép các quyết định được đưa ra.

Mặc dù có nhiều cách để tích hợp các hệ thống quản lý trong khi vẫn duy trì sự phù hợp, pha lập kế hoạch mở rộng phải được hoàn thành.

6 Xem xét triển khai tích hợp

6.1 Tổng quan

Trong tất cả các trường hợp, mục đích của tổ chức phải là tạo ra một hệ thống quản lý tích hợp có khả năng phù hợp với cả hai tiêu chuẩn. Mục đích này không phải so sánh các tiêu chuẩn hay xác định cái nào tốt nhất hoặc đúng hơn. Khi các quan điểm xung đột, Điều này phải được giải quyết theo cách thỏa mãn các yêu cầu của hai tiêu chuẩn, và đảm bảo rằng tổ chức đạt được cải tiến liên tục của ISMS và SMS. Hệ thống quản lý tích hợp lý tưởng phải dựa trên cách tiếp cận hiệu quả nhất của hai tiêu chuẩn, được áp dụng một cách thích hợp. Điều này cũng được hỗ trợ bằng việc sử dụng các chi tiết bổ sung trong tiêu chuẩn này để hỗ trợ cho tiêu chuẩn kia. Nên chú ý duy trì mọi điều cần thiết cho sự phù hợp với cả hai tiêu chuẩn.

Phải duy trì tính truy xuất nguồn gốc dữ liệu giữa hệ thống quản lý tích hợp và các yêu cầu của từng tiêu chuẩn tách biệt. Để giảm công sức, một tập các tài liệu có thể được tạo ra cho hệ thống quản lý tích hợp. Để hỗ trợ cho điều này, tổ chức có thể tạo ra tài liệu truy xuất như một ma trận truy xuất. Điều này chỉ ra một cách rõ ràng hệ thống quản lý tích hợp tuân thủ các yêu cầu của mỗi tiêu chuẩn. Lợi ích của cách tiếp cận này bao gồm việc cho phép theo dõi hoạt động nào là cần để chứng minh sự phù hợp với mỗi tiêu chuẩn.

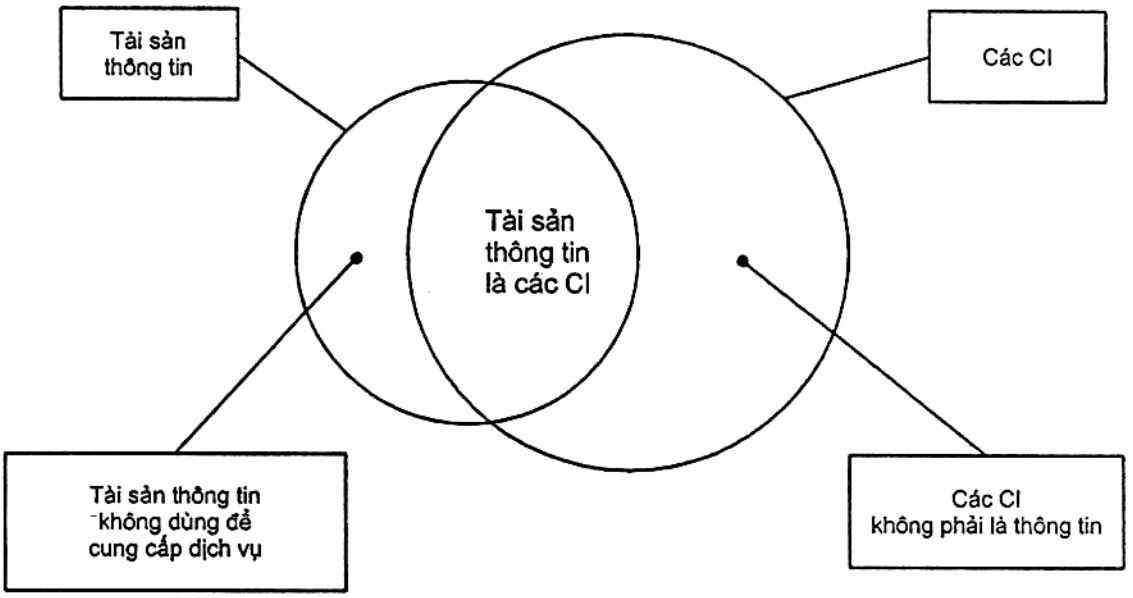
6.2 Các thách thức tiềm ẩn

6.2.1 Việc sử dụng và ý nghĩa của tài sản

Trong ISO/IEC 20000-1, tài sản khác với tài sản thông tin trong TCVN ISO/IEC 27001. Tài sản không phải là thuật ngữ được định nghĩa trong ISO/IEC 20000-1, cho nên nó được dùng theo nghĩa tiếng Anh thông thường về cái gì đó của giá trị. Trong vài điều của ISO/IEC 20000-1:2011 việc sử dụng tài sản được liên kết với các tài sản tài chính, như các cấp phép phần mềm. Trong các điều khác, tài sản được tham chiếu tới như tài sản thông tin. Ngược lại, TCVN ISO/IEC 27001 dựa trên khái niệm của việc bảo vệ thông tin và có một định nghĩa chính thức cho tài sản thông tin. Trong phần còn lại của Điều 6.2 của tiêu chuẩn này, điểm khác biệt và tương đồng của việc sử dụng và ý nghĩa trong hai tiêu chuẩn được thảo luận. Bao gồm các gợi ý về cách tích hợp hai tiêu chuẩn này.

ISO/IEC 20000-1 sử dụng một thuật ngữ được định nghĩa, khoản mục cấu hình (CI), như một phần tử cần được kiểm soát để chuyển giao một hoặc nhiều dịch vụ. Do đó tổ chức phải định nghĩa một CI là gì theo mục đích riêng của nó, có tính tới nhu cầu của nó về tính hiệu quả. "Tài sản thông tin" có thể được bao hàm trong định nghĩa này. Trong ISO/IEC 20000-1, cơ sở dữ liệu quản lí cấu hình (CMDB) là một kho dữ liệu của tất cả các CI và các liên hệ lẫn nhau của chúng. Một số tài sản tổ chức không có ở trong CMDB (như các máy tính để bàn không được dùng để chuyển giao các dịch vụ). Tương tự, một số CI có thể không được coi là tài sản theo ISO/IEC 20000-1 ví dụ: con người. Tài sản trong ISO/IEC 20000-1 thường có giá trị tiền bạc.

Với TCVN ISO/IEC 27001, tài sản thông tin được định nghĩa như tri thức hoặc dữ liệu có giá trị cho tổ chức, bất kể dạng thức, như: giấy, điện tử,.v.v... Như một kết quả, tài sản thông tin có thể là các CI, nhưng các CI là không nhất thiết phải là tài sản thông tin. Ví dụ: một dây cáp dữ liệu có thể là một CI, nhưng thường không phải một tài sản thông tin. Hình 2 cung cấp một minh họa cho mối quan hệ giữa các CI và tài sản thông tin. Với một hệ thống quản lý thông tin tích hợp, một tài sản thông tin trong TCVN ISO/IEC 27001 có thể được dùng bởi, hoặc là một phần của, một dịch vụ trong ISO/IEC 20000-1.



Hình 2 - Mối quan hệ giữa các tài sản thông tin trong TCVN ISO/IEC 27001 và các CI trong ISO/IEC 20000-1

Cả hai tiêu chuẩn đều không yêu cầu mọi CI hoặc tài sản thông tin phải được liệt kê riêng rẽ. Chúng có thể được gộp nhóm thành các kiểu, như phần cứng, hoặc tài liệu. Như một phần của quy trình này, các mô tả của chúng phải được làm nhất quán nhất có thể được, đơn giản phù hợp với cả hai tiêu chuẩn. Ví dụ: tại lúc đầu của bất kỳ công việc tích hợp nào, một quyết định phải được đưa ra theo cách tài sản được phân loại và nhận diện. Điều này đảm bảo các tham chiếu rõ ràng có thể thực hiện đối với các tài sản. Nếu thuật ngữ "tài sản thông tin" được sử dụng theo nghĩa TCVN ISO/IEC 27001, các tài sản đặc biệt phải được cho một nhãn bổ sung để đảm bảo rằng trạng thái của chúng được nhận ra như các CI hoặc tài sản tài chính trong ISO/IEC 20000-1, xem Phụ lục B của tiêu chuẩn này.

6.2.2 Thiết kế và chuyển giao dịch vụ

ISO/IEC 20000-1:2011, Điều 5 bao quát các yêu cầu cho việc thiết kế và chuyển giao các dịch vụ thay đổi hoặc mới. Không có Điều tương đương trực tiếp trong TCVN ISO/IEC 27001, mặc dù một số khía cạnh của việc thiết kế, chuyển dịch và chuyển giao dịch vụ được bao quát trong TCVN ISO/IEC 27001, Phụ lục A. Tuy nhiên, một hệ thống quản lý tích hợp phải đảm bảo rằng an ninh thông tin được xem xét chi tiết trong các giai đoạn lập kế hoạch của việc thiết kế và chuyển giao các dịch vụ thay đổi hoặc mới. Các chủ đề nên được xem xét bao gồm một đánh giá về tác động của dịch vụ thay đổi hoặc mới đối với dịch vụ và các kiểm soát an ninh thông tin hiện có, xem ISO/IEC 20000-1:2011, Điều 6.6.2. Điều này cũng nên được thực hiện cho chấp dứt một dịch vụ.

Việc hoạch định cho tất cả các dịch vụ mới hoặc thay đổi nên bao quát cả việc cân nhắc các hệ lụy an ninh thông tin. Điều này phải được thực hiện dù dịch vụ giảm sút trong phạm vi của ISMS.

6.2.3 Đánh giá và quản lý rủi ro

ISO/IEC 20000-1:2011, Điều 4.5.2 và 4.5.3 bao quát các yêu cầu về đánh giá rủi ro, và về cách xử lý các rủi ro liên kết với SMS.

TCVN ISO/IEC 27001:2009, Điều 4.2.1, đưa ra các yêu cầu đối với việc quản lý tất cả các khía cạnh rủi ro liên quan đến an ninh thông tin. Các yêu cầu này không bị giới hạn bởi các rủi ro liên quan đến chính các ISMS và bao quát việc đánh giá và xử lý các rủi ro và các khía cạnh khác của việc quản lý rủi ro an ninh thông tin.

Mặc dù các rủi ro được xem xét trong cả TCVN ISO/IEC 27001 và ISO/IEC 20000-1, bản chất của các rủi ro này là khác nhau. ISO/IEC 20000-1 xem xét các rủi ro cho SMS và các dịch vụ, trong khi TCVN ISO/IEC 27001 xem xét rủi ro an ninh thông tin và cách thức nó ảnh hưởng tới tổ chức. Tiêu chí đánh giá và xử lý các rủi ro có thể khác nhau, tùy thuộc vào liệu các rủi ro liên quan tới việc chuyển giao của một dịch vụ, hoặc đặc biệt với an ninh thông tin. Tuy nhiên, cách thức sử dụng để nhận diện các rủi ro có thể như nhau trong cả hai trường hợp. Một vài rủi ro được xem xét trong ISO/IEC 20000-1 ví dụ: rủi ro của một bên cung cấp không tôn trọng chi phí liên quan đến một SLA, không được coi là rủi ro theo quan điểm của TCVN ISO/IEC 27001. Vậy các rủi ro được nhận diện khi dùng ISO/IEC 20000-1 không thể được giả định là có liên quan đến an ninh thông tin, và ngược lại.

Việc làm chủ sở hữu rủi ro có thể khác biệt giữa hai cách tiếp cận. Ví dụ, trong ISO/IEC 20000-1 tổ chức bên cung cấp dịch vụ hiếm khi sở hữu mọi rủi ro. Khách hàng có thể mong đợi để chấp nhận các rủi ro còn lại như một phần SLA của họ hoặc của bản kế hoạch duy trì tính liên tục dịch vụ. Trong TCVN ISO/IEC 27001, vấn đề chủ sở hữu rủi ro không được thảo luận rõ ràng, nhưng trong thực tế tổ chức được coi như người chủ sở hữu của mọi rủi ro an ninh thông tin.

Hiểu lầm về các tùy chọn quản lý rủi ro nảy sinh do các khác biệt về yêu cầu quản lý rủi ro giữa hai tiêu chuẩn. Khi hoạch định tích hợp triển khai cho cả hai tiêu chuẩn, các tổ chức phải lưu tâm đối với bất kỳ các khác biệt trong tiêu chí rủi ro và tác động mà các khác biệt này có lên xử lý rỉ ro.

Tổ chức phải chấp nhận một trong hai cách tiếp cận được mô tả bên dưới.

a) Dùng một cách tiếp cận chung cho quản lý rủi ro, kể cả đánh giá rủi ro, cho cả hai tiêu chuẩn, tránh trùng lặp. Ví dụ: rủi ro của việc mất tính sẵn có của tài sản thông tin có thể được chia sẻ bởi các

phần khác nhau của hệ thống quản lý tích hợp. Đây là cách tiếp cận hiệu quả nhất để tránh trùng lặp nỗ lực.

b) Dùng các phương thức đánh giá rủi ro tách biệt cho hai tiêu chuẩn. Nếu tùy chọn này được chọn, tổ chức phải sử dụng thuật ngữ làm khác biệt đánh giá rủi ro của SMS và các dịch vụ từ ISMS và đánh giá rủi ro an ninh thông tin.

Khi việc đánh giá rủi ro và quản lý rủi ro là then chốt của tổ chức, việc triển khai TCVN ISO/IEC 27001 nên được ưu tiên để tận dụng các hướng dẫn quản lý rủi ro và đánh giá rủi ro. Dù tùy chọn nào được chọn, tổ chức phải sử dụng thuật ngữ rõ ràng và nhất quán. Điều này có thể yêu cầu việc diễn đạt các yêu cầu từ một hoặc hai tiêu chuẩn một cách khác nhau từ phiên bản đã công bố. Tuy nhiên tổ chức vẫn phải đảm bảo việc truy xuất rõ ràng về các yêu cầu trong cả hai tiêu chuẩn.

6.2.4 Các khác biệt trong các mức chấp nhận rủi ro

Khi một khách hàng giao phó dữ liệu hoặc hệ thống của họ được một bên thứ ba duy trì, có thể có các khác biệt giữa mức chấp nhận rủi ro của khách hàng và của bên thứ ba. Điều này không được rõ ràng trong tiêu chuẩn nào, nhưng tổ chức phải nhận biết về các vấn đề này và đưa ra quyết định rõ ràng liên quan đến các mức rủi ro được kiểm soát bởi các bên khác nhau.

Các vấn đề chính được mô tả dưới đây.

a) Khách hàng có cách nhìn liên quan đến mức an ninh Điều là chấp nhận cho thông tin của nó nằm dưới kiểm soát bởi bên thứ ba. Điều này có thể không tương xứng với mức an ninh mà bên thứ ba coi là đủ.

b) Bên thứ ba cũng có thông tin riêng của họ, như: các bản ghi tài chính. Bên thứ ba có cách nhìn liên quan đến mức an ninh là chấp nhận được cho thông tin này.

c) Khách hàng và bên thứ ba có thể được tham gia vào trong các môi trường pháp luật và các hiệu lực quy định khác nhau, đều thay đổi theo quốc gia hoặc lĩnh vực thị trường. Điều này có thể dẫn đến các quan điểm rủi ro hoặc an ninh thông tin khác nhau.

Các mong đợi và trách nhiệm an ninh thông tin của các khách hàng của tổ chức và các bên thứ ba nên được thảo luận ở cơ hội sớm nhất có thể. Các thảo luận này là quan trọng cho cả hai bên về việc thỏa thuận phạm vi của một dự án thực hiện, và quan trọng tương đương khi thể chế các kiểm soát vận hành các dịch vụ hiện có. Bất kỳ xung đột tiềm ẩn nào cũng phải được nhận diện và quyết định được đưa và được thỏa thuận, một cách lý tưởng là trước khi thực hiện.

6.2.5 Quản lý sự cố và vấn đề

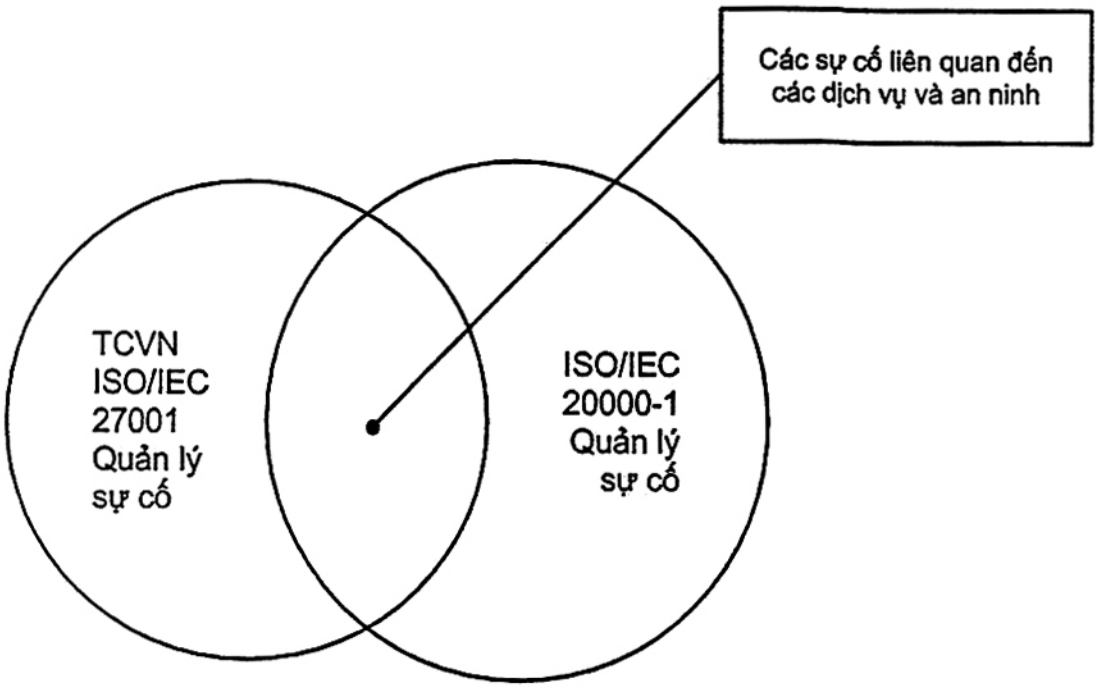
Điểm đầu tiên để thảo luận là vấn đề về thuật ngữ. Trong TCVN ISO/IEC 27001, có một thuật ngữ cho các biến cố không mong đợi đáng quan tâm: sự cố an ninh thông tin. Ngược lại, trong ISO/IEC 20000-1 có một số thuật ngữ đặc biệt liên kết với quản lý sự cố. Ví dụ, sự cố, sự cố an ninh thông tin, vấn đề, lỗi đã biết và sự cố chính, xem phụ lục B của tiêu chuẩn này. Những Điều này có thể là tất cả các sự cố an ninh thông tin theo TCVN ISO/IEC 27001, tùy theo các đặc trưng của nó.

TCVN ISO/IEC 27001 mô tả một quy trình riêng giải quyết tất cả các sự cố an ninh thông tin.

ISO/IEC 20000-1 không chỉ có đa dạng các thuật ngữ, nó cũng có đa dạng các cơ chế quản lý các biến cố như quản lý yêu cầu dịch vụ và sự cố, thủ tục sự cố chính và quản lý vấn đề. Trong ISO/IEC 20000-

1 một biến cố riêng lẻ có thể được quản lý bởi nhiều hơn một trong các quy trình và thủ tục này trong vòng đời của nó. ISO/IEC 20000-1 sử dụng định nghĩa TCVN ISO 9000:2007 (ISO/IEC 9000:2005)) cho thủ tục như "một cách thức đặc biệt để tiến hành một hoạt động hoặc quy trình". Với ISO/IEC 20000-1, quy trình là một mức cao hơn thủ tục, với các thủ tục hỗ trợ cho quy trình.

Hình 3 minh họa mối quan hệ giữa việc quản lý sự cố an ninh thông tin trong TCVN ISO/IEC 27001 và quản lý sự cố trong ISO/IEC 20000-1.



Hình 3 - Mô tả mối quan hệ giữa các tiêu chuẩn quản lý sự cố

Các biến cố mà TCVN ISO/IEC 27001 được phân loại như một sự cố an ninh thông tin, nhưng biến cố đó ISO/IEC 20000-1 không phân loại như một sự cố. Hai ví dụ được cho dưới đây.

a) Một tài liệu mật về việc tiếp thị một sản phẩm được tìm thấy trên bàn sau giờ làm việc, vi phạm chính sách an ninh thông tin. Tài liệu này không liên quan tới việc chuyển giao dịch vụ theo bất kỳ cách nào.

b) Khóa văn phòng của một khách hàng được tìm thấy đã bị phá. Biến cố này có thể được coi là sự cố theo TCVN ISO/IEC 27001. Tuy nhiên điều này không rơi vào phạm vi của ISO/IEC 20000-1 trừ phi nó được giả định truy cập vào thông tin liên quan đến các yêu cầu trong ISO/IEC 20000-1:2011, Điều 6.6.

Một cách tương tự, có các biến cố trong ISO/IEC 20000-1 phân loại như một sự cố, nhưng ở ngoài phạm vi của TCVN ISO/IEC 27001. Ví dụ:

a) Việc bảo trì theo lịch vượt quá giới hạn SLA;

b) Người dùng báo cáo sự cố do hiệu năng dịch vụ chậm.

Điểm trùng lặp giữa các định nghĩa của "sự cố" liên quan tới điều ISO/IEC 20000-1 nói tới là "các sự cố an ninh thông tin", điều này có thể làm nảy sinh mất tính bảo mật, tính toàn vẹn và tính truy cập được liên quan tới dịch vụ.

Để hòa hợp các cách nhìn trên, tổ chức phải quyết định cách xử lý cách quản lý sự cố, nằm trong phạm vi của cả hai hệ thống quản lý.

Quản lý vấn đề được định nghĩa trong ISO/IEC 20000-1 là tiến trình nhận diện căn nguyên của một hoặc nhiều sự cố để giảm thiểu hoặc né tránh tác động của sự cố. Trong ISO/IEC 20000-1, đây là tiến trình đặc biệt tách rời. Trong TCVN ISO/IEC 27001 quản lý vấn đề không được bao quát một cách rõ ràng, mặc dù nó được nói đến trong các yêu cầu về quản lý sự cố an ninh thông tin, xử lý rủi ro và các hoạt động khắc phục.

Trong một hệ thống quản lý tích hợp, quy trình quản lý vấn đề phải được xác định. Nếu một ISMS được triển khai trước SMS, điều này có thể hữu ích cho việc tích hợp các thực hành SMS tốt nhất cho quản lý vấn đề như một phần của ISMS, do ích lợi của nó với tất cả các hệ thống quản lý.

Cả hai tiêu chuẩn đều yêu cầu tổ chức phải phân tích dữ liệu và xu hướng trên sự cố.

Các sự cố có bao hàm rủi ro an ninh thông tin phải được phân loại như các sự cố an ninh thông tin. Điều quan trọng tương đương đối với tính phù hợp với cả hai tiêu chuẩn là ở chỗ quy trình quản lý sự cố phải phản ánh nhu cầu tuân thủ với các yêu cầu bổ sung cho an ninh thông tin trong TCVN ISO/IEC 27001.

Cần lưu ý rằng, kiểm soát trong TCVN ISO/IEC 27001:2011 (ISO/IEC 27001:2009), A.12.2.2 được bao quát việc học hỏi từ các sự cố an ninh và do đó là việc trùng lặp một phần với quản lý vấn đề trong ISO/IEC 20000-1:2011, Điều 8.2. Hơn nữa, việc nhận diện và đánh giá dễ tổn thương được yêu cầu cho đánh giá sự cố an ninh thông tin của TCVN ISO/IEC 27001 nên được coi như một quy trình phân tích dữ liệu mà có thể được sử dụng như làm đầu vào cho quản lý vấn đề.

Vấn đề thứ hai cần mô tả là vấn đề đáp ứng với sự cố. Bất kỳ tổ chức nào cũng phải có mục tiêu phục hồi dịch vụ nhanh chóng sau một sự cố an ninh thông tin đã ảnh hưởng tới dịch vụ. Tuy nhiên, điều này có thể làm giảm các khả năng mà một sự cố an ninh thông tin được điều tra để tìm hiểu nguyên nhân. Cần phải có lưu ý khi tích hợp SMS và ISMS, đảm bảo rằng các yêu cầu cho việc quản lý các sự cố an ninh thông tin được tuân thủ. Ví dụ, các kiểm soát an ninh thông tin có thể bao gồm thu thập, giữ lại và cung cấp bằng chứng cho các mục đích kỷ luật hoặc pháp lý. Hơn nữa, cả hai tiêu chuẩn yêu cầu tuân thủ với các yêu cầu pháp lý và quy định.

Cần phải thừa nhận rằng, trong trường hợp sự cố an ninh thông tin, yêu cầu thu thập bằng chứng có nghĩa là các dịch vụ bị ảnh hưởng không thể được phục hồi trong phạm vi mục tiêu dịch vụ đã thỏa thuận. ISO/IEC 20000-1, yêu cầu bên cung cấp dịch vụ tính tới sự khẩn cấp và tác động của sự cố đó. Điều đó có nghĩa là thời gian bổ sung cần được tới trước khi sự cố an ninh thông tin được giải quyết. Ưu tiên được dành cho giải pháp cần được tính tới tầm quan trọng của việc thu thập bằng chứng an ninh thông tin mà nếu không có thì có thể bị mất bởi việc phục hồi dịch vụ.

Trong một số trường hợp, sự cố an ninh thông tin là sự cố chính, dựa trên định nghĩa sự cố chính được thỏa thuận với khách hàng theo ISO/IEC 20000-1:2011, Điều 8.1. Theo các yêu cầu báo cáo dịch vụ trong ISO/IEC 20000-1:2011, Điều 6.2 và các yêu cầu quản lý sự cố chính trong ISO/IEC 20000-

1:2011, Điều 8.1, việc cấp quản lý cao nhất được thông báo về sự cố chính. Điều này bao gồm cả sự cố là sự cố an ninh thông tin. Điều này cũng đảm bảo một cá nhân chịu trách nhiệm, được đào tạo bài bản được bổ nhiệm để quản lý sự cố an ninh thông tin. Bên trong hệ thống quản lý tích hợp, biến cố này phải được quản lý như sự cố chính.

Sự cố chính không nên được công bố một cách thường xuyên để cho phép việc trì hoãn việc giải quyết tới khi thu thập được bằng chứng trong trường hợp sự cố an ninh thông tin. Ví dụ, nếu một website xử lý thanh toán của khách hàng được phát hiện đã bị phá hoại, thời gian thu thập bằng chứng và phục hồi dịch vụ phải được bao quát thích hợp trong các yêu cầu dịch vụ, danh mục dịch vụ và trong thỏa thuận mức dịch vụ (các SLA).

Định nghĩa ISO/IEC 20000-1 về an ninh thông tin sử dụng từ "tính truy cập" và định nghĩa TCVN ISO/IEC 27001 sử dụng từ "tính sẵn có". Khác biệt này là vì từ "tính sẵn có" được định nghĩa khác trong hai tiêu chuẩn, như được mô tả trong phụ lục B.

6.2.6 Quản lý thay đổi

ISO/IEC 27001:2009, A.10.1.2 và A.12.5.1 mô tả quản lý thay đổi. Cả A.10.1.2 và A.12.5.1 cho phép tổ chức pháp triển các thủ tục đáp ứng các nhu cầu đặc biệt của nó.

ISO/IEC 20000-1:2011, Điều 9.2, Quản lý thay đổi, bao quát các yêu cầu liên quan tới rủi ro. Các yêu cầu được bổ sung bởi Điều 6.6.3, Các sự cố và thay đổi an ninh thông tin. Điều 6.6.3 bao quát các yêu cầu cho đánh giá tác động của các thay đổi được yêu cầu, để xem xét tác động của chúng dựa trên các kiểm soát an ninh thông tin hiện có.

Để đảm bảo rằng các yêu cầu quản lý thay đổi được hoàn thành, các danh sách kiểm tra cho đánh giá tác động hoặc xem xét sau khi triển khai phải được phát triển như một phần của hệ thống quản lý tích hợp dựa trên ISO/IEC 20000-1. Điều này phải đảm bảo rằng mọi kiểu rủi ro an ninh thông tin đều được xem xét như một phần của quy trình quản lý thay đổi.

6.3 Các lợi ích tiềm năng

6.3.1 Sử dụng quy trình: Hoạch định-Thực hiện-Kiểm tra-Hành động

Cả TCVN ISO/IEC 27001 và ISO/IEC 20000-1 đều tham chiếu rõ ràng tới quy trình: Hoạch định-Thực hiện-Kiểm tra-Hành động (PDCA). Điều này có thể là thuận tiện, vì tổ chức có thể tuân theo cùng nguyên lý du cho bất kỳ tiêu chuẩn nào được thực hiện trước.

PDCA là cơ sở cho việc cải tiến liên tục trong cả hai tiêu chuẩn, nên việc cải tiến liên tục phải là sự hội tụ các hoạt động khi thực hiện một hoặc cả hai chuẩn này. Cần phải được lưu ý là các quy trình PDCA có thể vận hành ở các thang thời gian khác nhau, nhưng nếu ở mọi khả năng tổ chức nên sử dụng một quy trình tích hợp riêng để cung cấp cho cùng việc xem xét hoặc thời gian kiểm toán nội bộ.

6.3.2 Quản lý mức dịch vụ và báo cáo

Báo cáo dịch vụ được bao quát một cơ sở các hoạt động rộng hơn nhiều so với được yêu cầu cho quản lý mức dịch vụ. Tuy nhiên, báo cáo dịch vụ có thể hỗ trợ cho quản lý an ninh thông tin bằng cách có các mục đích dịch vụ dành cho các sự cố an ninh thông tin mà được đo đạc, được lấy xu hướng và được dùng trong báo cáo dịch vụ.

ISO/IEC 20000-1:2011, Điều 6.2 phần b, nói rằng quy trình báo cáo dịch vụ phải bao quát các thông tin liên quan về các biến cố lớn như các sự cố chính và việc không tuân thủ. Đầu ra từ quy trình báo cáo dịch vụ ISO/IEC 20000-1 có thể là một ưu thế chính để duy trì và cải tiến an ninh thông tin.

Khi thực hiện TCVN ISO/IEC 27001, các chi tiết kiểm soát an ninh thông tin được xác định, và tính hiệu quả của những kiểm soát này phải được đo, xem ISO/IEC 27001:2009, Điều 4.2.3 Giám sát và xem xét ISMS. Điều này cũng cung cấp một cơ hội cho việc tích hợp với quy trình báo cáo dịch vụ của ISO/IEC 20000-1:2011, Điều 6.2, để cho thông tin liên quan và kịp thời có thể được dùng để duy trì hoặc cải tiến an ninh thông tin. Khách hàng có thể có hiểu biết tốt hơn về hiện năng thực của dịch vụ và SMS, bao gồm các quy trình quản lý dịch vụ, liệu các mức tuân thủ kiểm soát an ninh thông tin liên quan và thống kê sự cố được tổ hợp trong các báo cáo.

Cả hai báo cáo của TCVN ISO/IEC 27001 và ISO/IEC 20000-1, dù cho việc sử dụng nội bộ hoặc cho khách hàng, phải được thiết kế với những lưu ý trên.

6.3.3 Cam kết của cấp quản lý

TCVN ISO/IEC 27001 mô tả an ninh thông tin trong quan hệ với các những bên có liên quan. Các bên có liên quan được nói là các bên có quyền lợi được đầu tư trong tổ chức nơi ISMS được thực hiện. Các bên này có thể bao gồm cán bộ, các cổ đông, các khách hàng và thậm chí có cả cơ quan quản lý hoặc công chúng. ISO/IEC 20000-1 đề cập đến các khách hàng và các bên có quan tâm. Các bên có quan tâm là cá nhân hoặc nhóm có lợi ích đặc biệt trong việc thực hiện hay thành công của một hoặc nhiều hoạt động của bên cung cấp dịch vụ. Các bên có quan tâm do đó là tương tự như "các bên có liên quan", dùng trong ISO/IEC 27001:2009.

Cam kết của quản lý cấp cao nhất được yêu cầu để tạo ra tính hiệu quả của SMS. Điều này bao gồm việc đảm bảo rằng các mối quan hệ với khách hàng và các bên có quan tâm khác là thành công. Hiểu theo cách thông thường, cam kết của cấp quản lý được nói trong TCVN ISO/IEC 27001 hỗ trợ cho cách tiếp cận tập trung vào khách hàng có trong ISO/IEC 20000-1.

ISO/IEC 20000-1:2011 bao quát các yêu cầu đặc biệt cho cam kết quản lý và trách nhiệm quản lý, Ví dụ như: các yêu cầu trong Điều 4.4.4 và 4.1.4. Ngược lại, ISO/IEC 27001:2009 có ít chuyên môn về vai trò nào phải chịu trách nhiệm và đảm nhiệm cho ISMS, Ví dụ các yêu cầu trong Điều 5.1 và 5.2.2. Hệ thống quản lý tích hợp phải tận dụng ưu thế của bản chất đặc biệt của ISO/IEC 20000-1 và việc sử dụng các yêu cầu của nó để đảm bảo rằng các trách nhiệm an ninh thông tin rộng hơn được thực hiện một cách nghiêm túc như trách nhiệm quản lý dịch vụ.

ISO/IEC 20000-1 nói rằng, khi trình bày việc quản lý các cải tiến, tổ chức phải phân công trách nhiệm cho việc quản lý quy trình cải tiến cho một vai trò đặc biệt. Ngược lại, ISO/IEC 27001:2009, Điều 4.2.4 và 8.1 nói tới tổ chức giải quyết nhiệm vụ này, trong khi Điều 5.1 bao quát các yêu cầu rằng tổ chức thiết lập ra các vai trò và trách nhiệm cho an ninh thông tin. Yêu cầu của ISO/IEC 20000-1 cho việc phân công rõ ràng trách nhiệm quản lý các cải tiến phải được sử dụng để đảm bảo rằng việc quản lý các cải tiến an ninh thông tin cũng được phân công cho một vai trò đặc biệt.

6.3.4 Quản lý năng lực

Quản lý năng lực trong ISO/IEC 20000-1:2011, Điều 6.5 bao quát một miền rộng hơn của các khái niệm năng lực trong TCVN ISO/IEC 27001, nên một số yêu cầu của ISO/IEC 20000-1 có thể được

dùng để hỗ trợ việc triển khai TCVN ISO/IEC 27001. Ví dụ, quản lý năng lực được mô tả trong ISO/IEC 20000-1 áp dụng cho cả năng lực kỹ thuật và năng lực tài nguyên con người. Hơn nữa, ISO/IEC 27001:2009, Điều 5.2, Quản lý tài nguyên, có thể liên quan tới quản lý năng lực, vì năng lực là việc truy cập vào các nguồn tài nguyên đủ để đối phó với hoàn cảnh có thể dự đoán một cách hợp lý.

Trong ISO/IEC 27001:2009, Điều 3.2, tính sẵn có được định nghĩa ngụ ý cả tính truy cập và tính dùng được. Quản lý năng lực trong ISO/IEC 20000-1:2011, Điều 6.5, hỗ trợ cả hai khía cạnh này của tính sẵn có. Ví dụ, nếu năng lực không đủ, một dịch vụ hoặc thành phần dịch vụ có thể là không được truy cập được, kiểu như không thể lưu được tệp bởi vì có quá ít năng lực lưu trữ. Một cách khác, một dịch vụ hoặc thành phần dịch vụ có thể quá chậm làm cho nó không được sử dụng, ví dụ thời gian đáp ứng, bởi vì năng lực mạng quá nhỏ.

Tổ chức nên nhận biết về sự khác biệt này khi có các yêu cầu tham chiếu chéo giữa hai tiêu chuẩn. Tổ chức phải tính tới nhu cầu cấu thành tham chiếu chéo trong ISO/IEC 20000-1:2011, Điều 4.3 và 6.5 và các điều liên quan trong TCVN ISO/IEC 27001, xem Phụ lục A của tiêu chuẩn này. Ví dụ, yêu cầu đưa vào tác động tiềm ẩn của các thay đổi theo luật định, quy định, hợp đồng hoặc thay đổi của tổ chức trong bản kế hoạch năng lực, được yêu cầu bởi ISO/IEC 20000-1:2011, Điều 6.5 phải được tham chiếu chéo với ISO/IEC 27001:2009, Điều A.10.1.

6.3.5 Quản lý sự cố bên thứ ba

Trong TCVN ISO/IEC 27001, bên thứ ba như khách hàng, bên cung cấp và nhóm nội bộ độc lập ở bên ngoài phạm vi áp dụng của ISMS và được xem như nguồn rủi ro tiềm ẩn. Phụ lục B của tiêu chuẩn này bao quát một so sánh về các thuật ngữ, TCVN ISO/IEC 27001 mô tả các kiểm soát phải được dùng để quản lý an ninh các bên thứ ba này trong A.6.2.1 và A.6.2.3

Ngược lại, trong ISO/IEC 20000-1, các bên khác là thực thể không dưới quyền kiểm soát trực tiếp của bên cung cấp dịch vụ nhưng là các bên đóng góp cho dịch vụ trong phạm vi của SMS. Các bên khác là các bên cung cấp, các nhóm nội bộ hoặc khách hàng (khi hoạt động như bên cung cấp). Các bên khác có thể đóng góp cho phần chính của dịch vụ, xem ISO/IEC 20000-1:2011 Điều 4.2, Quản trị các quy trình được vận hành bởi các bên khác. ISO/IEC 20000-1:2011, Điều 6.6, mô tả các yêu cầu của việc quản lý an ninh thông tin. Điều này bao gồm việc quản lý rủi ro liên quan kết với bên cung cấp dịch vụ, mà có thể ảnh hưởng trực tiếp tới an ninh thông tinh của tổ chức khách hàng, ISO/IEC 20000-1:2011, Điều 8.1 cũng nói tới sự cố và quy trình yêu cầu dịch vụ cho việc quản lý các sự cố an ninh thông tin, và việc đánh giá tất cả các thay đổi để xem xét tác động của các kiểm soát an ninh thông tin.

Khi thiết kế một hệ thống quản lý tích hợp, hai cân nhắc chính ảnh hưởng mối quan hệ doanh nghiệp và các quy trình quản lý bên cung cấp đối với việc quản lý các rủi ro của bên thứ ba. Hai cân nhắc này được mô tả dưới đây.

a) Các nghĩa vụ an ninh thông tin hợp đồng phải là một đầu vào cho quy trình đánh giá rủi ro. Quy trình này phải đóng góp cho việc hoàn thành các yêu cầu của ISO/IEC 20000-1 cho bên cung cấp dịch vụ để đáp ứng các nhu cầu doanh nghiệp.

b) An ninh thông tin phải được được bao quát khi đối phó với các bên thứ ba khác, bao gồm các khách hàng đóng vai trò như bên cung cấp. Điều này phải được cân nhắc khi một dịch vụ thay đổi hoặc mới được thiết kế và danh mục dịch vụ và các SLA được thảo luận.

Các khái niệm khác được bao quát trong ISO/IEC 2000-1:2011, Điều 7.1, như các kiểm định hiệu năng, các thay đổi dịch vụ, quản lý sự hài lòng của khách hàng và giải quyết khiếu nại, có thể được áp dụng cho một hệ thống quản lý tích hợp để làm mạnh cho nó như một tổng thể.

Tóm lại, một hệ thống quản lý tích hợp phải tuân theo cách tiếp cận của TCVN ISO/IEC 27001 để quản lý các mối quan hệ với các bên cung cấp, nhưng cũng phải tuân thủ các yêu cầu trong ISO/IEC 20000-1:2011, Điều 6.6.2. Các kiểm soát an ninh thông tin liên quan tới rủi ro bên cung cấp. Tài sản của tổ chức trong phạm vi của ISMS có một số hoặc tất cả tài sản này được kiểm soát bởi bên khác, tổ chức phải thỏa thuận các hợp đồng phù hợp, các SLA và các thỏa thuận hướng dẫn khác. Cách tiếp cận này phải đảm bảo rằng bên thứ ba hoặc bên khác áp dụng các kiểm soát thích hợp.

6.3.6 Quản lý tính sẵn có và tính liên tục

ISO/IEC 2000-1:2011, Điều 6.3, Quản lý tính sẵn có và tính liên tục của dịch vụ, bao quát rõ ràng một phần các lĩnh vực liên quan của mối quan tâm về an ninh thông tin. Các hoạt động về tính sẵn có và tính liên tục trong một hệ thống quản lý hiện có phải được xem xét để thấy được liệu chúng có thể được mở rộng hữu dụng để bao trùm việc quản lý tính toàn vẹn và tính bảo mật, và do đó quản lý an ninh thông tin cho bất kỳ dịch vụ nào. Ở đây, chi tiết có thể được rút ra từ ISO/IEC 20000-1 và các quy tắc chung từ ISO/IEC 27001:2009, Điều A.14.

6.3.7 Quản lý bên cung cấp

ISO/IEC 27001:2009 bao quát việc quản lý bên cung cấp trong nhiều điều khác nhau, ví dụ: A.6.2.1, A.6.2.3, A.10.2, A.8 cho tài nguyên con người bao quát các nhà thầu. ISO/IEC 20000-1:2011, Điều 4.2 bao quát yêu cầu cho việc quản trị các quy trình được vận hành bởi các bên khác và Điều 7.2 bao quát các yêu cầu cho quản lý bên cung cấp. Quản lý bên cung cấp theo cả hai chuẩn có thể được tổ hợp một cách hiệu quả.

Điều 6.3.5 của tiêu chuẩn này bao gồm các thông tin bổ sung về quản lý các rủi ro liên kết với các bên cung cấp. Ví dụ, đánh giá rủi ro của ISO/IEC 20000-1 có thể được mở rộng, sử dụng các khái niệm TCVN ISO/IEC 27001, để cân nhắc liệu an ninh tổ chức có phá hoại bởi việc bổ sung hoặc gỡ bỏ của một bên cung cấp, hoặc bởi một thay đổi đặc thù cho dịch vụ mà một bên cung cấp đóng góp cho.

Điều này phải được cân nhắc cho dù tổ chức quyết định thực hiện chỉ một tiêu chuẩn.

6.3.8 Quản lý cấu hình

Kho tài sản trong TCVN ISO/IEC 27001 là kho chứa bất kỳ cái gì có giá trị (tiền tệ hoặc các thứ khác) cho một tổ chức và là phạm vi áp dụng của ISMS, tức là: thông tin, cơ sở dữ liệu hay các quy trình.

Khái niệm cơ sở dữ liệu quản lý cấu hình (CMDB) trong ISO/IEC 20000-1 là tương tự với việc kiểm kê tài sản trong TCVN ISO/IEC 27001, nhưng phạm vi áp dụng và quan điểm khác nhau. Việc triển khai phạm vi áp dụng được thảo luận trong ISO/IEC 20000-1:2011, Điều 4.5.1

Các yêu cầu trong ISO/IEC 20000-1:2011, Điều 9.1 có thể được dùng trong việc tạo ra và quản lý một ISMS. Theo quan điểm của TCVN ISO/IEC 27001, tổ chức phải quản lý an ninh của CMDB, cho nó (CMDB) cần được đối xử như một tài sản thông tin.

ISO/IEC 20000-1:2011, Điều 9.1 cũng yêu cầu CMDB được an toàn để bảo vệ tính chính xác của dữ liệu được lưu trữ. Điều này bao quát yêu cầu về duy trì các dịch vụ và tính toàn vẹn của thành phần

dịch vụ. Tuy nhiên, ISO/IEC 20000-1 không đưa ra sự phân biệt giữa các mức khá nhau của tính toàn vẹn. TCVN ISO/IEC 27001 có thể bổ sung giá trị ở đây, vì nó yêu cầu các rủi ro cho hệ thống, dịch vụ và các thành phần dịch vụ được đánh giá, và các mức chấp nhận được về rủi ro được xác định. Vấn đề chính là liệu mức rủi ro có thể bị thay đổi bởi một thay đổi hay không, và nếu có, liệu thay đổi đó có làm gia tăng rủi ro tới một mức không thể chấp nhận được hay không.

Các yêu cầu về tuyến cơ sở cấu hình và các bản sao chính trong ISO/IEC 20000-1 thực tế là các kiểm soát, theo quan điểm của TCVN ISO/IEC 27001. Các yêu cầu này phải được cân nhắc khi tích hợp các cách tiếp cận quản lý rủi ro. Một số trong chúng ảnh hưởng tới các quyết định về việc liệu có thực hiện các kiểm sát nào đó hay không.

6.3.9 Quản lý triển khai và phát hành

Việc phù hợp với các yêu cầu về quản lý triển khai và phát hành trong ISO/IEC 20000-1:2011, Điều 9.3 không đảm bảo phù hợp với các yêu cầu trong TCVN ISO/IEC 27001 để phát hành. Các vấn đề an ninh có thể được đưa ra ngẫu nhiên trong phần này nếu các yêu cầu của TCVN ISO/IEC 27001 không được tuân theo. Các ví dụ bao gồm:

a) Các thay đổi có thể được tạo ra cho việc vận hành (các) hệ thống tồn tại, đều đưa vào các hư hỏng thông tin nếu việc quản lý triển khai và phát hành không tính tới khả năng của hoạt động nguy hại;

b) Quản lý thử nghiệm và các môi trường tồn tại thường được thực hiện bởi các nhóm khác nhau, do đó quy trình phát hành phải đảm bảo rằng vai trò sản xuất đúng nhận dữ liệu từ nhóm kiểm thử, để tránh các rủi ro cố cho dữ liệu mật.

Điều này là đặc biệt quan trọng trong các phát hành khẩn cấp. Trong các tình huống này, quy trình triển khai và phát hành khác có thể biến động được sử dụng do các ràng buộc về thời gian và/hoặc tài nguyên. Rủi ro của việc phá hoại an ninh thông tin do đó được gia tăng. Các rủi ro an ninh thông tin bao giờ cũng phải được quản lý đúng bằng cách tuân theo các quy trình an ninh thông tin đã được chấp nhận, bất kể quy trình triển khai và phát hành nào được sử dụng.

Quản lý triển khai và phát hành có thể được cải tiến qua việc chọn lựa các kiểm soát trong ISO/IEC 27000:2005, A.1.1.4 Phân tách các tiện nghi phát triển, kiểm thử và các vận hành; và A.1.3.2 Chấp nhận hệ thống.

6.3.10 Lập ngân sách và tài chính

Các yêu cầu lập ngân sách và tài chính trong ISO/IEC 20000-1:2011, Điều 6.4 không thể được ánh xạ trực tiếp theo bất kỳ yêu cầu nào của TCVN ISO/IEC 27001. Trong TCVN ISO/IEC 27001, yêu cầu cho việc cung cấp tài nguyên và đầu ra của xem xét quản lý (yêu cầu một quyết định được đưa ra cho các nhu cầu tài nguyên) có thể có ích lợi từ việc xem xét nguồn lực tài chính và quy trình lập ngân sách được xác định.

Phụ lục A

(tham khảo)

Tương ứng giữa TCVN ISO/IEC 27001:2011 và ISO/IEC 20000-1:2011

A.1 Tổng quát

Phụ lục A cung cấp so sánh nội dung theo các điều giữa ISO/IEC 27001:2009 và ISO/IEC 20000-1:2011.

Các điều có sự trùng lặp hầu hết các yêu cầu và chi tiết giữa TCVN ISO/IEC 27001 và ISO/IEC 20000-1 được làm nổi bật bởi màu xám nhạt.

Các điều có sự trùng lặp hầu hết các yêu cầu và chi tiết giữa TCVN ISO/IEC 27001, Phụ lục A và ISO/IEC 20000-1 được làm nổi bật bởi màu xám đậm.

Các lĩnh vực không được đánh dấu là những lĩnh vực không có sự trùng lặp đáng kể.

Bảng A.1 - Tương ứng giữa ISO/IEC 27001:2009 và ISO/IEC 20000-1:2011

TCVN ISO/IEC 27001:2009	ISO/IEC 20000-1:2011
Giới thiệu	Giới thiệu
Tổng quát	Không tương đương trực tiếp
Cách tiếp cận quy trình	Không tương đương trực tiếp
Tương thích với các hệ thống quản lý khác	Không tương đương trực tiếp
1 Phạm vi	1 Phạm vi
1.1 Tổng quát	1.1 Tổng quát
1.2 Ứng dụng	1.2 Ứng dụng
2 Tài liệu viện dẫn	2 Tài liệu viện dẫn
3 Thuật ngữ và định nghĩa	3 Thuật ngữ và định nghĩa
4 Hệ thống quản lý an ninh thông tin	4 Các yêu cầu chung hệ thống quản lý dịch vụ
4.1 Các yêu cầu chung	Không tương đương trực tiếp
4.2 Xây dựng và quản lý ISMS	4.5 Xây dựng và cải tiến SMS
Không tương đương trực tiếp	4.5.1 Xác định phạm vi
Không tương đương trực tiếp	4.5.2 Hoạch định SMS (Hoạch định)

TCVN ISO/IEC 27001:2009	ISO/IEC 20000-1:2011
4.2.2 Thiết lập và vận hành ISMS	4.5.3 Thiết lập và vận hành SMS (Thực hiện)
4.2.3 Giám sát và xem xét ISMS	4.5.4 Giám sát và xem xét SMS (Kiểm tra)
4.2.4 Bảo trì và cải tiến ISMS	4.5.5 Bảo trì và cải tiến SMS (Hành động)
4.3 Các yêu cầu tài liệu	4.3 Quản lý tài liệu
4.3.1 Tổng quát	4.3.1 Thực hiện và bảo trì tài liệu
4.3.2 Kiểm soát tài liệu	4.3.2 Kiểm soát tài liệu
4.3.3 Kiểm soát bản ghi	4.3.4 Kiểm soát bản ghi
5 Trách nhiệm của cấp quản lý	4.1 Trách nhiệm của cấp quản lý
5.1 Cam kết của cấp quản lý	4.1.1 Cam kết của cấp quản lý
Không tương đương trực tiếp	4.1.2 Chính sách quản lý dịch vụ
Không tương đương trực tiếp	4.1.3 Thẩm quyền, trách nhiệm và trao đổi
Không tương đương trực tiếp	4.1.4 Đại diện quản lý
Không tương đương trực tiếp	4.2 Quản trị quy trình được vận hành bởi các bên khác
5.2 Quản lý tài nguyên	4.4 Quản lý tài nguyên
5.2.1 Cung cấp tài nguyên	4.4.1 Cung cấp tài nguyên
5.2.2 Đào tạo, nhận biết và năng lực	4.4.2 Tài nguyên con người
6 Kiểm tra ISMS nội bộ	4.5.2 Kiểm tra nội bộ
7 Xem xét quản lý ISMS	4.5.4.3 Xem xét của cấp quản lý
7.1 Tổng quát	4.5.4.3 Xem xét của cấp quản lý
7.2 Xem xét đầu vào	4.5.4.3 Xem xét của cấp quản lý
7.3 Xem xét đầu ra	4.5.4.3 Xem xét của cấp quản lý
8 Cải tiến ISMS	4.5.5 Bảo trì và cải tiến SMS (Hành động)
8.1 Cải tiến liên tục	4.5.5.1 Tổng quát
	4.5.5.2 Quản lý cải tiến

TCVN ISO/IEC 27001:2009	ISO/IEC 20000-1:2011
8.2 Hành động khắc phục	4.5.5.1 Tổng quát
	4.5.5.2 Quản lý cải tiến
	8 Quy trình giải quyết
8.3 Hành động phòng ngừa	4.5.5.1 Tổng quát
	4.5.5.2 Quản lý cải tiến
	8 Quy trình giải quyết
Không tương đương trực tiếp	5 Thiết kế và chuyển dịch các dịch vụ thay đổi hoặc mới
Không tương đương trực tiếp	5.1 Tổng quát
Không tương đương trực tiếp	5.3 Thiết kế và phát triển dịch vụ thay đổi hoặc mới
Không tương đương trực tiếp	5.4 Chuyển dịch các dịch vụ mới hoặc thay đổi
Không tương đương trực tiếp	6 Quy trình chuyển giao dịch vụ
A.10.2.1 Chuyển giao dịch vụ	6.1 Quản lý mức dịch vụ
A.10.2.2 Giám sát và xem xét dịch vụ bên thứ ba	6.2 Báo cáo dịch vụ
Không tương đương trực tiếp	6.3 Quản lý tính sẵn có và tính liên tục dịch vụ
Không tương đương trực tiếp	6.4 Lập ngân sách và tài chính cho dịch vụ
A.10.2.3 Quản lý thay đổi dịch vụ bên thứ ba	5.2 Lập kế hoạch cho các dịch vụ mới hoặc thay đổi
A.10.3.1 Quản lý năng lực	6.5 Quản lý năng lực
TCVN ISO/IEC 27001	6.6 Quản lý an ninh thông tin
Không tương đương trực tiếp	7 Quy trình quan hệ
Không tương đương trực tiếp	7.1 Quản lý quan hệ doanh nghiệp
Không tương đương trực tiếp	7.2 Quản lý bên cung cấp
A.13 Quản lý sự cố an ninh thông tin	8.1 Quản lý yêu cầu dịch vụ và sự cố
Không tương đương trực tiếp	8.2 Quản lý vấn đề
Không tương đương trực tiếp	9 Quy trình kiểm soát

TCVN ISO/IEC 27001:2009	ISO/IEC 20000-1:2011
Không tương đương trực tiếp (chỉ một phần trong vài kiểm soát)	9.1 Quản lý cấu hình
A.12.5.1 Quy trình kiểm soát thay đổi	9.2 Quản lý thay đổi
Không tương đương trực tiếp	9.3 Quản lý triển khai và phát hành
Phụ lục A Các mục đích kiểm soát và các kiểm soát	(một phần được bao quát ở trên, xem phân tích chi tiết)
Phụ lục B Các nguyên lý OECD và tiêu chuẩn này	Không tương đương trực tiếp
Phụ lục C Tương ứng giữa TCVN ISO 9001:2000 (ISO 9001:2000), TCVN ISO 14001:2005 (ISO 14001:2004) và tiêu chuẩn này	Không tương đương trực tiếp

Phụ lục B

(tham khảo)

So sánh thuật ngữ ISO/IEC 27000:2009 và ISO/IEC 20000-1:2011

Trong bảng B.1 của tiêu chuẩn đề cập mà không có năm xuất bản của "Ghi chú sử dụng thuật ngữ trong cả hai tiêu chuẩn" theo mục đích tối giản. Bảng B.1 cung cấp một so sánh thuật ngữ được định nghĩa trong ISO/IEC 27000:2009, là Thuật ngữ cho ISO/IEC 27001:2009, các thuật ngữ được sử dụng trong TCVN ISO/IEC 27001, và các thuật ngữ được định nghĩa hoặc được sử dụng trong ISO/IEC 20000-1:2011. Các lĩnh vực mà các thuật ngữ được định nghĩa khác nhau giữa ISO/IEC 27000 và ISO/IEC 20000-1 được thể hiện bởi màu xám nhạt.

Bảng B.1 - So sánh thuật ngữ

Thuật ngữ	ISO/IEC 27000:2009	ISO/IEC 20000-1:2011	Ghi chú sử dụng thuật ngữ trong cả hai tiêu chuẩn
Biện pháp truy cập	2.1 Đảm bảo rằng truy cập tới các tài sản (2.3) được chứng nhận và giới hạn dựa trên các yêu cầu an ninh và kinh doanh.	Không được định nghĩa.	Không tương ứng trực tiếp.
Trách nhiệm giải trình	2.2 Trách nhiệm của một thực thể cho các quyết định và hành động của chính nó.	Không được định nghĩa.	Từ "trách nhiệm giải trình" được dùng trong ISO/IEC 20000-1 theo nghĩa tiếng Anh thông thường là trách nhiệm, được yêu cầu để giải thích hoặc bảo vệ các hành động của ai đó hoặc tiến hành, khuyến nghị và giả định trách nhiệm. Từ "trách nhiệm giải trình" là quan trọng với các yêu cầu trong ISO/IEC 20000-1, Điều 4.2, vi dụ "bởi ...a) mô tả tài chính cho các quy trình và thẩm quyền để yêu cầu việc tham gia các quy trình.

Thuật ngữ	ISO/IEC 27000:2009	ISO/IEC 20000-1:2011	Ghi chú sử dụng thuật ngữ trong cả hai tiêu chuẩn
Tài sản	2.3 Bất kỳ thứ gì có giá trị cho tổ chức CHÚ Ý Có nhiều loại tài sản, bao gồm: a) Thông tin (2.18); b) Phần mềm, ví dụ: một chương trình máy tính; c) Phần cứng vật lý, ví dụ: máy tính; d) Dịch vụ; e) Con người, và các đặc tính của họ, kỹ năng và kinh nghiệm; và f) Tài sản vô hình, ví dụ: danh tiếng và hình ảnh.	Không được định nghĩa.	Từ "tài sản" được dùng trong ISO/IEC 20000-1 theo nghĩa tiếng Anh thông thường là bất kỳ điều gì có giá trị hoặc hiệu dụng, như kỹ năng, chất lượng, con người,... Từ "tài sản" được dùng hạn chế trong ISO/IEC 20000-1, Điều 4.1.4: "[Đại diện quản lý] có thẩm quyền và trách nhiệm mà bao gồm: d) đảm bảo rằng các tài sản, bao gồm chứng nhận, được dùng cho các dịch vụ phân phối và được quản lý dựa trên các yêu cầu luật định và quy định và các nghĩa vụ hợp đồng. Điều 6.4: "Điều này phải là các chính sách và các thủ tục hướng dẫn cho: a) lập kế hoạch ngân sách và tài chính cho các thành phần dịch vụ bao gồm ít nhất: 1) các tài sản - bao gồm các chứng chỉ - sử dụng cung cấp các dịch vụ." Điều 6.6.2: "Bên cung cấp dịch vụ phải thực hiện và vận hành các kiểm soát an ninh kỹ thuật và quản trị, vật lý thay vì: a) Duy trì tính bảo mật, toàn vẹn và khả năng truy cập của các tài sản thông tin." Điều 9.1: "Điều này phải là một giao diện định nghĩa giữa quy trình quản lý cấu hình và quy trình quản lý tài sản tài chính. CHÚ THÍCH Phạm vi của quy trình quản lý cấu hình độc nhất việc quản lý tài sản tài chính."
Tấn công	2.4 Có xu hướng bị phá hoại, nổ, thay đổi, tắt, lấy cắp hoặc gia tăng truy cập bất hợp pháp tới hoặc tạo ra việc sử dụng bất hợp pháp của một tài sản.	Không được định nghĩa.	Không tương ứng trực tiếp.

Thuật ngữ	ISO/IEC 27000:2009	ISO/IEC 20000-1:2011	Ghi chú sử dụng thuật ngữ trong cả hai tiêu chuẩn
Thẩm quyền	2.5 Cung cấp đảm bảo rằng một đặc điểm công bố của một thực thể là hợp thức.	Không được định nghĩa.	Không trực tiếp liên quan tới thuật ngữ liên quan an ninh thông tin này, "thẩm quyền", mà được dùng trong TCVN ISO/IEC 27001 trong kỹ thuật. "Thẩm quyền" không giống "xác thực" trong các hành động của vòng đời hệ thống quản lý.
Tính xác thực	2.6 Quyền hạn mà một thực thể được gán.	3.11 CHÚ THÍCH 1 Bổ sung, các thuộc tính khác như: tính xác thực, trách nhiệm, chống chối bỏ và độ tin cậy có thể tham gia.	Tham chiếu trong ISO/IEC 20000-1 nhưng không được sử dụng thêm.
Tính khả dụng	2.7 Quyền hạn được truy cập và sử dụng dựa theo yêu cầu của một thực thể hợp pháp.	3.1 Khả năng của một dịch vụ hoặc thành phần dịch vụ thực hiện chức năng yêu cầu theo một khoản thỏa thuận hoặc qua một khoảng thời gian thỏa thuận. CHÚ THÍCH Tính sẵn sàng được được nhấn mạng như một tỉ lệ hoặc phần trăm thời gian mà dịch vụ hoặc thành phần dịch vụ sẵn sàng thực tế cho việc sử dụng bởi khách hàng cho thời gian thỏa thuận rằng dịch vụ phải là sẵn có. CHÚ THÍCH 1 Bổ sung các đặc tính khác như: tính xác thực, trách nhiệm, chống chối bỏ và độ tin cậy có thể tham gia. CHÚ THÍCH 2 Thuật ngữ "tính sẵn có" được được dùng trong định nghĩa này bởi nó là một thuật ngữ định nghĩa trong phần này của ISO/IEC 20000 mà không tương ứng với định nghĩa này.	Xem "an ninh thông tin". Tính sẵn có thường đề cập như trung tâm của quản lý dịch vụ và đóng vai trò như một vai trò nổi bật trong ISO/IEC 20000-1 theo khía cạnh của việc truy cập chất lượng dịch vụ cung cấp. Xem ISO/IEC 20000-1, Điều 6.3. Điểm khác biệt giữa hai định nghĩa là không lớn, nhưng bởi tầm quan trọng đặt trong "tính sẵn có" của quản lý dịch vụ, khác biệt này là đáng chú ý. Một hệ quả trực tiếp của sự khác biệt giữa hai ý nghĩa của tính sẵn có là định nghĩa anh ninh thông tin TCVN ISO/IEC 27001 đã đáp ứng cho ISO/IEC 20000-1bằng cách sử dụng tính truy cập thay vì tính sẵn có.

Thuật ngữ	ISO/IEC 27000:2009	ISO/IEC 20000-1:2011	Ghi chú sử dụng thuật ngữ trong cả hai tiêu chuẩn
		CHÚ THÍCH 3 Đáp ứng từ ISO/IEC 27000:2009.	
Kinh doanh liên tục	2.8 Các quy trình (2.31) và/hoặc các thủ tục (2.30) để đảm bảo các vận hành kinh doanh liên tục.	Không được định nghĩa.	Dịch vụ liên tục được sử dụng trong ISO/IEC 20000-1 như là một tập con của kinh doanh liên tục. Xem "dịch vụ liên tục".
Tính bảo mật	2.9 Đặc tính mà thông tin không tạo ra tính sẵn sàng hoặc bị tiết cho cho các cá nhân thực thể và quy trình bất hợp pháp (2.3.).	Không được định nghĩa.	Không tương ứng trực tiếp.
Đường căn bản cấu hình	Không được định nghĩa.	3.2 Thông tin cấu hình thường được định ở một thời gian đặc trưng trong suốt cuộc đời một dịch vụ hoặc thành phần dịch vụ. CHÚ THÍCH 1 Các đường cơ bản cấu hình, bổ sung thêm các thay đổi từ các đường cơ bản, là thông tin cấu hình hiện tại. CHÚ THÍCH 2 Đáp ứng từ ISO/IEC/IEEE 24765:2010.	Thuật ngữ được dùng một lần trong ISO.IEC 2000-1. Điều 9, như: "...Một đường cơ sở cấu hình của các CI bị ảnh hưởng phải được thực hiện trước khi triển khai một phát hành trong môi trường sống".
Khoản mục cấu hình (CI)	Không được định nghĩa.	3.3 Thành phần mà các nhu cầu được kiểm soát thay vì phân chia một hoặc nhiều dịch vụ.	Các CI nổi bật trong ISO/IEC 20000-1 và được xem xét như một thành phần của dịch vụ. Các CI có thể là một hoặc một phần của một thành phần dịch vụ. Một tài sản thông tin có thể là một CI. Xem TCVN ISO/IEC 27001, Định nghĩa 3.27 Thành phần dịch vụ.

Thuật ngữ	ISO/IEC 27000:2009	ISO/IEC 20000-1:2011	Ghi chú sử dụng thuật ngữ trong cả hai tiêu chuẩn
Cơ sở dữ liệu quản lý cấu hình (CMDB)	Không được định nghĩa.	3.4 Kho dữ liệu dùng để ghi các thuộc tính của các CI, và mối quan hệ giữa các CI, thông qua vòng đời của chính chúng.	Dựa trên các tiếp cận được đáp ứng với tổ chức, một CMDB có thể được dùng để giữ các kho tài sản. Xem TCVN ISO/IEC 27001, phụ lục A, Điều A.7.1.1.
Nâng cấp liên tục	Không được định nghĩa.	3.5 Hoạt động định kỳ nhằm tăng cường khả năng đáp ứng đầy đủ các yêu cầu dịch vụ. CHÚ THÍCH Đáp ứng theo TCVN ISO 9000:2007 (ISO/IEC 9000:2005))	ISO/IEC 20000-1, Điều 4.1.2, yêu cầu một chính sách cho việc nâng cấp liên tục, như một phần của chính sách quản lý dịch vụ. Chu trình PDCA, bao gồm việc giới thiệu TCVN ISO/IEC 27001, là rất giống với TCVN ISO 9001 (ISO 9001:2008) và ISO/IEC 20000-1 (tham khảo TCVN ISO/IEC 27001, Điều 4.2.4 và ISO/IEC 20000-1, Điều 4.5.5.).
Kiểm soát	2.10 Nghĩa là việc quản lý rủi ro (2.34), bao gồm các chính sách (2.28), thủ tục (2.30), hướng dẫn (2.16), thực hành hoặc cấu trúc tổ chức, mà có thể quản trị, kỹ thuật, quản lý hoặc hợp pháp tự nhiên ISO 31000:2009. 2.26 Kiểm soát Đo đạc và điều chỉnh rủi ro (2.1) CHÚ THÍCH 1 Các kiểm soát bao gồm bất kỳ quy trình, chính sách, thiết bị, thực hành hoặc các hành động khác mà điều chỉnh rủi ro.	Không được định nghĩa.	Từ "kiểm soát" được dùng trong ISO/IEC 20000-1 theo cả danh từ và động từ, nhưng không được định nghĩa như thuật ngữ đặc biệt, mà ý nghĩa tiếng Anh thông thường áp dụng. Danh từ: thẩm quyền hoặc nghĩa vụ, quyền lực để ảnh hưởng hoặc hướng dẫn, điều khiển, một ý nghĩa của việc giới hạn (các kiểm soát) một thiết bị để vận hành, điều chỉnh hoặc kiểm tra (một máy móc, hệ thống,...) Động từ: (được điều khiển, điều khiển) để có hoặc thực hành quyền lực thông qua ai đó hoặc cái gì, để điều chỉnh, giới hạn, vận hành, hoặc kiểm tra (một máy móc, hệ thống) Tất cả nhưng việc sử dụng 2 nghĩa của từ "kiểm soát" là một danh từ trong ISO/IEC 20000-1, điều 6.6, Quản lý an ninh thông tin. Cách sử dụng khác trong Điều 4.3.2 và 4.4.3 mà không thay đổi từ TCVN ISO 9001 (ISO/IEC 9001:2008)).

Thuật ngữ	ISO/IEC 27000:2009	ISO/IEC 20000-1:2011	Ghi chú sử dụng thuật ngữ trong cả hai tiêu chuẩn
	CHÚ THÍCH 2 Các kiểm soát có thể không thường xuyên phát huy hoặc thừa nhận việc thay đổi hiệu quả (ISO Guide 73:2009, định nghĩa 3.8.1.1)		Kiểm soát được dùng như một động từ trong nhiều vị trí, thường là "điều khiển của quy trình XXX" hoặc "X phải được điều khiển bởi Y".
Mục tiêu kiểm soát	2.11 Trạng thái mô tả những cái gì phải đạt được như một kết quả của việc thực hiện các kiểm soát (2.10).	Không được định nghĩa.	Danh từ "mục tiêu" được dùng trong ISO/IEC 20000-1 trong thì tiếng Anh đơn: một điều nhằm mục đích hoặc mong muốn cho, một mục tiêu. Có một liên kết dễ tổn thương giữa việc sử dụng "mục tiêu kiểm soát" trong TCVN ISO/IEC 27001 và việc sử dụng trong ISO/IEC 20000-1, Điều 4 của các cụm từ như "các mục tiêu quản lý dịch vụ" hoặc Điều 6.6, "các mục tiêu quản lý an ninh thông tin".
Hành động khắc phục	2.12 hành động để loại bỏ nguyên nhân của một sự phát hiện không phù hợp hoặc tình huống không mong muốn khác. [TCVN ISO 9000:2007 (ISO/IEC 9000:2005)]	3.6 hành động để loại bỏ nguyên nhân hoặc giảm khả năng tái phát của một sự phát hiện không phù hợp hoặc tình huống không mong đợi khác. CHÚ THÍCH Đáp ứng theo TCVN ISO 9000:2007 (ISO/IEC 9000:2005)).	Thuật ngữ tương tự được dùng cho cả hai tiêu chuẩn, nhưng có nhiều khác biệt về nghĩa. Nó không phải lúc nào cũng có thể hoặc mong muốn để loại bỏ nguyên nhân, thay vào đó nó có thể được tốt hơn hoặc nhiều hơn chi phí hiệu quả để tránh tái phát. Xem hành động phòng ngừa trong ISO/IEC 20000-1, định nghĩa 3.18.
Khách hàng	Không được định nghĩa.	3.7 Tổ chức hoặc một phần của tổ chức mà nhận một hoặc nhiều dịch vụ. CHÚ THÍCH 1 Một khách hành có thể ở bên trong hoặc bên ngoài tổ chức bên cung cấp dịch vụ.	Trong ISO/IEC 20000-1, khách hàng có thể đóng vai trò bổ sung như bên cung cấp.

Thuật ngữ	ISO/IEC 27000:2009	ISO/IEC 20000-1:2011	Ghi chú sử dụng thuật ngữ trong cả hai tiêu chuẩn
		CHÚ THÍCH 2 Đáp ứng theo TCVN ISO 9000:2007 (ISO/IEC 9000:2005)).	
Văn bản	Không được định nghĩa.	3.8 Thông tin và phương tiện hỗ trợ [TCVN ISO 9000:2007 (ISO/IEC 9000:2005)]. VÍ DỤ Các chính sách, kế hoạch, mô tả quy trình, thủ tục, thỏa thuận mức dịch vụ, hợp đồng và bản ghi. CHÚ THÍCH 1 Văn bản có thể ở bất kỳ dạng thức hoặc loại phương tiện nào. CHÚ THÍCH 2 Trong ISO/IEC 20000, các văn bản ngoại trừ các bản ghi, phải nêu rõ mục đích cần đạt được.	Không tương ứng trực tiếp.
Tính hiệu quả	2.13 Mở rộng các hoạt động lập kế hoạch được nhận ra và các kết quả kế hoạch đã đạt được [TCVN ISO 9000:2007 (ISO/IEC 9000:2005)].	3.9 Mở rộng các hoạt động lập kế hoạch được nhận ra và các kết quả kế hoạch đã đạt được [TCVN ISO 9000:2007 (ISO/IEC 9000:2005)].	Giống nhau.
Hiệu quả	2.14 Mối quan hệ giữa các kết quả đã đạt được và cách thức sử dụng tốt các tài nguyên.	Không được định nghĩa.	Từ này được dùng trong thì tiếng Anh thường, và chỉ một lần, trong việc giới thiệu ISO/IEC 20000-1. Không có bất kỳ yêu cầu nào liên quan đến hiệu quả.

Thuật ngữ	ISO/IEC 27000:2009	ISO/IEC 20000-1:2011	Ghi chú sử dụng thuật ngữ trong cả hai tiêu chuẩn
Sự kiện	2.15 Sự xuất hiện của một tập cụ thể các tình huống [ISO/IEC Guide 73:20002].	Không được định nghĩa.	Từ "sự kiện" được dùng trong ISO/IEC 20000-1 theo nghĩa tiếng Anh thông thường là một cái gì đó đã hoặc đang xảy ra. Ví dụ, xem ISO/IEC 20000-1, Điều 6.2: "các sự kiện quan trọng" hoặc Điều 6.3.2, các kế hoạch sẵn có và liên tục của dịch vụ: "trong sự kiện của việc mất mát lớn dịch vụ". Việc sử dụng tương đương trong TCVN ISO/IEC 27001, để so sánh rộng rãi. Xem "sự kiện an ninh thông tin".
Hướng dẫn	2.16 Yêu cầu về điều mong đợi được thực hiện để đạt được một mục tiêu.	Không được định nghĩa.	Xem các phần khác của ISO/IEC 20000. Trong khi ISO/IEC 20000-1 bao gồm các yêu cầu viện dẫn, tất cả các phần khác của ISO/IEC 20000 là các tiêu chuẩn quốc gia hoặc báo cáo kỹ thuật tham khảo.
Tác động	2.17 Thay đổi bất lợi đối với mức mục tiêu kinh doanh đã đạt được.	Không được định nghĩa.	Sử dụng từ "tác động" trong cả hai tiêu chuẩn là tương đối giống nhau. "Tác động" được dùng 26 lần trong ISO/IEC 20000-1. Trong thời tiếng Anh thông thường của: "tác động", danh từ: một hiệu ứng hoặc áp lực mạnh mẽ. Nó sử dụng "tác động" ít cụ thể hơn trong ISO/IEC 20000-1 về cách thức "tác động" được dùng trong TCVN ISO/IEC 27001. Hầu hết cách sử dụng trong ISO/IEC 20000-1 là liên kết với các rủi ro hoặc các hoàn cảnh thực tế tiêu cực như định nghĩa 3.15, Lỗi đã biết và trong Điều 5: "Bên cung cấp dịch vụ phải sử dụng quy trình này cho tất cả các dịch vụ và các thay đổi các dịch vụ có tiềm năng có tác động lớn về các dịch vụ hoặc khách hàng" hoặc Điều 6.3.2: "Bên cung cấp dịch vụ phải đánh giá tác động của các yêu cầu thay đổi của (các) kế hoạch dịch vụ liên tục và (các) kế hoạch sẵn có".

Thuật ngữ	ISO/IEC 27000:2009	ISO/IEC 20000-1:2011	Ghi chú sử dụng thuật ngữ trong cả hai tiêu chuẩn
Sự cố	Xem "sự cố an ninh thông tin"	3.10 Việc gián đoạn không kế hoạch một dịch vụ, một giảm thiểu về chất lượng một dịch vụ hoặc một sự kiện mà chưa tác động dịch vụ tới khách hàng.	Có một điểm khác biệt chủ yếu giữa việc sử dụng "sự cố" trong bộ tiêu chuẩn TCVN ISO/IEC 27001 và trong ISO/IEC 20000-1. Từ "sự cố" được dùng trong TCVN ISO/IEC 27001 theo nghĩa "điều gì đó đã sai với an ninh của môi trường phạm vi". Trong ISO/IEC 20000-1 từ "sự cố" có một ý nghĩa được xác định và cụ thể hơn trong TCVN ISO/IEC 27001. Trong ISO/IEC 20000-1 "sự cố" là một trong một loạt các điều khoản liên quan và không chỉ liên quan tới các sự cố an ninh thông tin. Các thuật ngữ khác là: 3.19 Vấn đề Nguyên nhân gốc rễ của một hoặc nhiều sự cố. Nguyên nhân gốc rễ không chỉ được biết tới ở thời điểm một bản ghi vấn đề được tạo ra và quy trình quản lý vấn đề là chịu trách nhiệm cho các điều tra sau này. 3.15 Lỗi đã biết Vấn đề mà có một nguyên nhân gốc rễ được định danh hoặc một phương pháp nhằm giảm thiểu hoặc loại bỏ tác động của nó trên một dịch vụ bằng cách làm việc quanh nó. Sự cố lớn (không phải là một thuật ngữ định nghĩa) hoặc một sự cố (hoặc vấn đề) đã được coi là chủng loại cao nhất của tác động. Mỗi "sự cố", "vấn đề", và "sự cố lớn" được quản lý khác nhau và là chủ đề cho các yêu cầu khác nhau. "Lỗi đã biết" là một vấn đề khi nguyên nhân cơ bản được hiểu và được quản lý bởi quy trình quản lý vấn đề, mà bao gồm các yêu cầu áp dụng một lần một vấn đề đã trở thành một lỗi đã biết.

Thuật ngữ	ISO/IEC 27000:2009	ISO/IEC 20000-1:2011	Ghi chú sử dụng thuật ngữ trong cả hai tiêu chuẩn
			"Sự cố lớn" được quản lý bởi quy trình quản lý yêu cầu dịch vụ, với một yêu cầu mà có một thủ tục đặc biệt cho việc quản lý "các sự cố lớn". Xem "sự cố an ninh thông tin"
Tài sản thông tin	2.18 Kiến thức hoặc dữ liệu mà có giá trị cho tổ chức.	Không được định nghĩa.	Thuật ngữ này không phải là một thuật ngữ định nghĩa nhưng được dùng trong ISO/IEC 20000-1, như Điều 6.6.2: "Bên cung cấp dịch vụ phải thực hiện và vận hành các kiểm soát an ninh vật lý, hành chính và kỹ thuật để: a) Duy trì sự bảo mật, tính toàn vẹn và khả năng truy cập các tài sản thông tin." Xem "tài sản".
An ninh thông tin	2.19 Sự duy trì của tính bảo mật (2.13), tính toàn vẹn (2.36) và tính sẵn sàng (2.10) của thông tin. CHÚ THÍCH Bổ sung, các đặc tính khác như tính xác thực (2.9), trách nhiệm (2.2), chống chối bỏ (2.49) và độ tin cậy (2.56) cũng có thể tham gia.	3.11 Sự duy trì tính bảo mật, tính toàn vẹn và khả năng truy cập của thông tin. CHÚ THÍCH 1 Bổ sung, các đặc tính khác như tính xác thực, trách nhiệm, chống chối bỏ và độ tin cậy có thể tham gia. CHÚ THÍCH 2 Thuật ngữ "tính sẵn có" không được dùng trong định nghĩa này bởi nó là một thuật ngữ định nghĩa trong phần này của tiêu chuẩn ISO/IEC 20000 mà không phù hợp với định nghĩa này. CHÚ THÍCH 3 Đáp ứng từ ISO/IEC 27000:2009.	Trong ISO/IEC 20000-1, từ "tính sẵn có" không thể được dùng trong địnhnghĩa an ninh thông tin trong Điều 3.11, bởi tính sẵn có là một thuật ngữ định nghĩa với một ý nghĩa khác (xem "tính sẵn có") Định nghĩa cho an ninh thông tin do đó được đáp ứng cho việc sử dụng thuật ngữ "khả năng truy cập" thay thế. Khả năng truy cập được thực hiện từ định nghĩa ISO/IEC 27000 của tính sẵn có "đặc tính được truy cập và sử dụng dựa trên đòi hỏi của một thực thể hợp pháp".

Thuật ngữ	ISO/IEC 27000:2009	ISO/IEC 20000-1:2011	Ghi chú sử dụng thuật ngữ trong cả hai tiêu chuẩn
Sự kiện an ninh thông tin	2.20 Sự xuất hiện định danh của một hệ thống, dịch vụ hoặc trạng thái mạng chỉ ra một nhánh tiềm năng của an ninh thông tin (2.19) chính sách (2.28) và lỗi kiểm soát (2.10), hoặc một trạng thái không biết trước đó mà có thể liên quan đến an ninh.	Không được định nghĩa.	Các sự kiện an ninh thông tin chỉ được dùng trong ISO/IEC 20000-1 như một phần của định nghĩa 3.12: sự cố an ninh thông tin. Thêm vào đó, sự kiện 2.15 (không phải sự kiện an ninh thông tin) cũng được dùng trong: a) Định nghĩa rủi ro - xem 3.25 mà bao gồm GHI CHÚ 3 và 4 liên quan các sự kiện, b) Định nghĩa "sự liên tục của dịch vụ" (3.28), c) ISO/IEC 20000-1, Điều 6.2: báo cáo dịch vụ, d) ISO/IEC 20000-1, Điều 6.3.2: sự liên tục của dịch vụ" và các kế hoạch sẵn có". Xem "sự kiện": một hoặc nhiều sự kiện có thể tạo các phần của một sự cố an ninh.
Sự cố an ninh thông tin	2.21 Một hoặc chuỗi các sự kiện an ninh thông tin không mong đợi hoặc không mong muốn (2.20) mà có một khả năng đáng kể ảnh hưởng đến lựa chọn kinh doanh và đe dọa (2.19).	3.12 Một hoặc chuỗi các sự kiện an ninh thông tin không mong đợi hoặc không mong muốn mà có một khả năng đáng kể ảnh hưởng đến lựa chọn kinh doanh và đe dọa. [ISO/IEC 27000:2009].	ISO/IEC 20000-1 định nghĩa 3.12 bao gồm thuật ngữ sự cố an ninh thông tin của ISO/IEC 27000. ISO/IEC 20000-1, Điều 6.6.3 bao gồm một yêu cầu: các sự cố an ninh thông tin phải được quản lý sử dụng các thủ tục quản lý sự cố, với một mức ưu tiên thích hợp cho các rủi ro an ninh thông tin. Nó không phục vụ cho "thứ đã đi sai với dịch vụ" khi mà nguyên nhân là một vấn đề, như nguyên nhân gốc rễ của một hoặc nhiều sự cố, khi nguyên nhân gốc rễ không thường được biết đến tai thời điểm một bản ghi vấn đề được tạo ra và quy trình quản lý vấn đề là chịu trách nhiệm cho các điều tra sau này. Nó được quản lý bởi quy trình quản lý vấn đề, không phải việc quản lý sự cố và quy trình yêu cầu dịch vụ.

Thuật ngữ	ISO/IEC 27000:2009	ISO/IEC 20000-1:2011	Ghi chú sử dụng thuật ngữ trong cả hai tiêu chuẩn
			Các sự cố [an ninh thông tin] chính được quản lý bởi quy trình yêu cầu dịch vụ và sự cố liên quan. Sự khác biệt trong cách thuật ngữ được sử dụng trong cả hai tiêu chuẩn là phức tạp hơn sự kiện an ninh hoặc sự cố là một tập phụ hoặc loại đặc biệt của sự cố [quản lý dịch vụ]. Xem Điều 6.2.5 của tiêu chuẩn này.
Quản lý sự cố an ninh thông tin	2.22 Các quy trình (2.31) để phát hiện, báo cáo, truy cập, chịu trách nhiệm, quyết định, và học hỏi từ các sự cố an ninh thông tin (2.21).	Không được định nghĩa.	Xem: "Sự cố". "Sự cố an ninh thông tin". "Lỗi đã biết". "Vấn đề".
Hệ thống quản lý an ninh thông tin (ISMS)	2.23 Phần của hệ thống quản lý tổng quan (2.26), dựa trên một hướng tiếp cận rủi ro kinh doanh để thiết lập, thực hiện, vận hành, giám sát, đánh giá, bảo trì và nâng cấp an ninh thông tin (2.19).	Không được định nghĩa.	Xem "hệ thống quản lý dịch vụ" và "hệ thống quản lý".
Rủi ro an ninh thông tin	2.24 Tiềm năng mà một đe dọa (2.45) phát tán một lỗ hổng (2.46) của một tài sản (2.3) hoặc nhóm tài sản và do đó gây ra nguy hại cho tổ chức.	Không được định nghĩa.	Xem "rủi ro". Rủi ro an ninh thông tin không được định nghĩa nhưng được sử dụng trong các phần quản lý an ninh thông tin của ISO/IEC 20000-1, Điều 6.6.1.
Tính toàn vẹn	2.25 Đặc tính bảo vệ độ chính xác và sự đầy đủ của các tài sản (2.3).	Không được định nghĩa.	Từ "tính toàn vẹn" được sử dụng trong ISO/IEC 20000-1 theo nghĩa tiếng Anh thông thường; chất lượng hoặc trạng thái của toàn bộ và không bị hư hỏng. (ví dụ: xem ISO/IEC 20000-1, Điều 6.6.2: "bên cung cấp dịch vụ phải thực hiện và vận hành các kiểm soát an ninh thông tin kỹ

Thuật ngữ	ISO/IEC 27000:2009	ISO/IEC 20000-1:2011	Ghi chú sử dụng thuật ngữ trong cả hai tiêu chuẩn
			thuật, hành chính và vật lý để: a) duy trì tính bảo mật, tính toàn vẹn và khả năng truy cập các tài sản thông tin." ISO/IEC 20000-1, Điều 9.1 bao gồm các yêu cầu: "Chúng phải là một thủ tục tài liệu cho việc ghi, kiểm soát và theo dõi các piên bản của các CI. Mức độ kiểm soát phải duy trì tính toàn vẹn của các dịch vụ và các thành phần dịch vụ yêu cầu dịch có tính đến các yêu cầu dịch vụ và rủi ro liên quan tới các CI." "Các thay đổi với các CI phải được truy xuất và kiểm tra để đảm bảo tính toàn vẹn của các CI và dữ liệu trong CMDB." ISO/IEC 20000-1, Điều 9.3 bao gồm các yêu cầu: "Bản phát hành phải được thực thi trong môi trường sống để tính toàn vẹn của phần cứng, phần mềm và các thành phần dịch vụ khác được duy trì trong suốt sự thực thi của bản phát hành."
Bên liên quan	Không được định nghĩa.	3.13 Cá nhân hoặc nhóm có một sư quan tâm đặc biệt về hiệu năng hoặc thành công của (các) hành động bên cung cấp dịch vụ. VÍ DỤ Các khách hàng , chủ, quản lý, người trong tổ chức của bên cung cấp dịch vụ, bên cung cấp, nhân viên ngân hàng, ủy ban hoặc đối tác. CHÚ THÍCH 1 Một nhóm có thể bao gồm một tổ chức, một phần của nó, hoặc nhiều hơn một tổ chức. CHÚ THÍCH 2 Đáp ứng theo TCVN ISO 9000:2007 (ISO/IEC 9000:2005))	Xem "bên cung cấp dịch vụ".

Thuật ngữ	ISO/IEC 27000:2009	ISO/IEC 20000-1:2011	Ghi chú sử dụng thuật ngữ trong cả hai tiêu chuẩn
Nhóm nội bộ	Không được định nghĩa.	3.14 Phần của bên cung cấp dịch vụ của tổ chức mà tham gia vào một thỏa thuận văn bản với bên cung cấp để đóng góp cho việc thiết kế, chuyển đổi, phân phát và nâng cấp một hoặc nhiều dịch vụ. CHÚ THÍCH Nhóm nội bộ là bên ngoài phạm vi vủa bên cung cấp dịch vụ của SMS.	Xem "bên cung cấp dịch vụ".
Lỗi đã biết	Không được định nghĩa.	3.15 Vấn đề mà có một nguyễn nhân gốc rễ được định danh hoặc một phương pháp giảm thiểu hoặc loại bỏ tác động của nó trên một dịch vụ bằng cách làm việc với nó.	Xem "sự cố" và "vấn đề".
Hệ thống quản lý	2.26 Nền tảng của các chính sách (2.28), thủ tục (2.30), hướng dẫn (2.16) và các tài nguyên liên quan để đạt được các mục tiêu của tổ chức.	Hệ thống quản lý được định nghĩa trong CHÚ THÍCH 1 của định nghĩa hệ thống quản lý dịch vụ. CHÚ THÍCH 1 Một hệ thống quản lý là một tập của các phần tử tương tác hoặc có có liên kết để thiết lập chính sách và các mục tiêu và để đạt được các mục tiêu đó.	Được sử dụng trong ISO/IEC 20000-1 để đề cập tới "các hệ thống quản lý khác", ISO/IEC 20000-1 được đề cập tới như một "hệ thống quản lý dịch vụ".

Thuật ngữ	ISO/IEC 27000:2009	ISO/IEC 20000-1:2011	Ghi chú sử dụng thuật ngữ trong cả hai tiêu chuẩn
Chống chối bỏ	2.27 Khả năng chứng minh sự xuất hiện của một biến cố đã được công bố (2.15) hoặc hành động và các thực thể gốc để giải quyết trang cãi về sự xuất hiện hay không xuất hiện của biến cố này (2.15) hay hành động và sự tham gia của các thực thể trong biến cố này (2.15).	Không được định nghĩa hoặc sử dụng.	Không tương ứng trực tiếp.
Tổ chức	Không được định nghĩa.	3.17 Nhóm người hoặc cơ sở với một sự sắp xếp trách nhiệm, thẩm quyền và mối quan hệ. VÍ DỤ Đoàn thể, tập đoàn, thương hội, công ty, tổ chức từ thiện, hiệp hội, hoanh nghiệp tư nhân hoặc các thành phần kết hợp đó với nhau. CHÚ THÍCH 1 Nói chung, việc sắp xếp là có trật tự. CHÚ THÍCH 2 Một tổ chức có thể là công cộng hoặc tư nhân.	ISO/IEC 20000-1 sử dụng thuật ngữ "bên cung cấp dịch vụ" và "tổ chức" cho các thực thể khác nhau, nên sự khác biệt là chủ yếu cho bất kỳ các giải thích nào đối với hệ thống quản lý kết hợp. Xem "bên cung cấp dịch vụ".
Chính sách	2.28 Mục đích và định hướng tổng thể được thể hiện chính thức bằng việc quản lý.	Không được định nghĩa.	Từ "chính sách" được dùng trong ISO/IEC 20000-1 theo nghĩa tiếng Anh thông thường là: (chính sách - số nhiều) một kế hoạch hành động, thường dựa trên các quy tắc thực tế, được quyết định bởi một bộ phận hoặc cá nhân một quy tắc hoặc tập các quy tắc cho các quyết định cơ bản, một chuỗi hành động phải tuân theo.

Thuật ngữ	ISO/IEC 27000:2009	ISO/IEC 20000-1:2011	Ghi chú sử dụng thuật ngữ trong cả hai tiêu chuẩn
			Các chính sách được sử dụng trong ISO/IEC 20000-1 cho các hướng tổ chức. Một vài được yêu cầu bởi ISO/IEC 20000-1, bao gồm một chính sách quản lý dịch vụ. Việc sử dụng phần lớn là giống nhau trên cả hai tiêu chuẩn.
Hành động phòng ngừa	2.29 Hành động để loại bỏ nguyên nhân của một sự không phù hợp tiềm ẩn hoặc tình huống tiềm ẩn không mong đợi khác [TCVN ISO 9000:2007 (ISO/IEC 9000:2005)]	3.18 Hành động để tránh hoặc loại bỏ nguyên nhân hoặc giảm khả năng xuất hiện của sự không phù hợp tiềm ẩn hoặc tình huống không mong đợi khác. CHÚ THÍCH Đáp ứng trong TCVN ISO 9000:2007 (ISO/IEC 9000:2005)	Các định nghĩa nghĩa khác, trong đó định nghĩa của ISO/IEC 20000-1 đã được mở rộng bao gồm hành động phòng ngừa mà không được loại bỏ nguyên nhân, nhưng việc xung quanh nó một cách nào đó để tránh bị tác động; và hành động phòng ngừa không loại bỏ nguyên nhân, nhưng việc xung quanh nó một cách nào đó để tránh bị tác động. Thuật ngữ tương tự được sử dụng trong cả hai tiêu chuẩn, nhưng chúng khác biệt về ý nghĩa. Nó không phải là luôn luôn có thể hoặc mong muốn để có hành động phòng ngừa trong quản lý dịch vụ. Thay vào đó, nó có thể tốt hơn/ hiệu quả hơn để tránh dư thừa. Hơn nữa, với ISO/IEC 20000-1, định nghĩa TCVN ISO 9000 (ISO 9000:2005) được đáp ứng để cho phép khả năng này. Các liên kết cho hoạt động chính sách trong ISO/IEC 20000-1, định nghĩa 3.6 và ISO/IEC 27000 định nghĩa 2.12
Vấn đề	Không được định nghĩa.	3.19 Nguyên nhân gốc rễ của một hoặc nhiều sự cố. CHÚ THÍCH Nguyên nhân gốc rễ không thường được biết đến ở thời điểm một bản ghi vấn đề được tạo ra và quy trình quản lý vấn đề là chịu trách nhiệm cho việc điều tra sau này.	Xem "sự cố" và "lỗi đã biết".

Thuật ngữ	ISO/IEC 27000:2009	ISO/IEC 20000-1:2011	Ghi chú sử dụng thuật ngữ trong cả hai tiêu chuẩn
Thủ tục	2.30 Cách thức được quy định để thực hiện một hoạt động hoặc một quy trình. [TCVN ISO 9000:2007 (ISO/IEC 9000:2005)]	3.20 Cách thức đặc trưng để thực hiện một hoạt động hoặc một quy trình [TCVN ISO 9000:2007 (ISO/IEC 9000:2005)]. CHÚ THÍCH Các thủ tục có thể được ghi lại hoặc không.	Cả hai định nghĩa đều dựa trên TCVN ISO 9000 (ISO 9000:2005). Chúng đa phần giống nhau. Chỉ trong phần CHÚ THÍCH là khác biệt, như: thủ tục có thể không được ghi lại, nhưng các tham chiếu của ISO/IEC 20000-1 để thủ tục hóa được tất cả "thủ tục văn bản". Các thủ tục đó là một phần của kế hoạch được ghi lại như một phần của kế hoạch.
Quy trình	2.31 Tập các hoạt động tương tác hoặc liên kết với nhau, chuyển đổi các đầu vào thành các đầu ra. [TCVN ISO 9000:2007 (ISO/IEC 9000:2005)]	3.31 Tập các hoạt động tương tác hoặc liên kết với nhau, chuyển đổi các đầu vào thành các đầu ra. [TCVN ISO 9000:2007 (ISO/IEC 9000:2005)]	Cả hai đều dựa trên TCVN ISO 9000:2007 (ISO/IEC 9000:2005).
Bản ghi	2.32 Tài liệu nêu rõ kết quả đạt được hoặc cung cấp bằng chứng về các hoạt động đã thực hiện. [TCVN ISO 9000:2007 (ISO/IEC 9000:2005)]	3.22 Tài liệu nêu rõ kết quả đạt được hoặc cung cấp bằng chứng về các hoạt động đã thực hiện. [TCVN ISO 9000:2007 (ISO/IEC 9000:2005)] VÍ DỤ Các báo cáo kiểm toán, các báo cáo sự cố, các báo cáo đào tạo hoặc các biên bản họp.	Cả hai đều dựa trên TCVN ISO 9000:2007 (ISO/IEC 9000:2005).
Bản phát hành	Không được định nghĩa hoặc sử dụng.	3.23 Tập hợp của một hoặc nhiều CI thay đổi hoặc mới được thiết lập trong một trường thực như một hệ quả của một hoặc nhiều thay đổi.	Không tương ứng trực tiếp.

Thuật ngữ	ISO/IEC 27000:2009	ISO/IEC 20000-1:2011	Ghi chú sử dụng thuật ngữ trong cả hai tiêu chuẩn
Sự tin cậy	2.33 Tính chất của hành vi và các kết quả có khả năng phù hợp.	Được đề cập trong an ninh thông tin 3.11. CHÚ THÍCH 1 Thêm vào đó, các tính chất khác như tính xác thực, trách nhiệm, chống thoái thác và độ tin cậy cũng có thể tham gia.	Từ ""sự tin cậy" được sử dụng trong ISO/IEC 20000-1 theo nghĩa tiếng Anh thông thường: sự đáng tin. ISO/IEC 20000-1, Điều 8.1: "CMDB phải quản lý để đảm bảo độ tin cậy và chính xác của chính nó, bao gồm việc kiểm soát của truy cập cập nhật".
Đề nghị thay đổi	Không được định nghĩa hoặc sử dụng.	3.24 Đề nghị một thay đổi được tạo ra cho một dịch vụ, thành phần dịch vụ hoặc hệ thống quản lý dịch vụ. CHÚ THÍCH Một thay đổi cho một dịch vụ bao gồm việc cung cấp một dịch vụ mới hoặc gỡ bỏ một dịch vụ mà không còn được yêu cầu nữa.	TCVN ISO/IEC 27001, phụ lục A đề cập tới "quản lý thay đổi" như một kiểm soát trong A.0.1.2. Nhiều kiểm soát trong TCVN ISO/IEC 27001 đề cập tới việc quản lý và kiểm soát các thay đổi. Ví dụ: A.8.3, A.10.1, A.10.2.3, A.12.5.1.
Rủi ro	2.34 Sự kết hợp của các khả năng của một sự kiện (2.15) và hệ quả của nó [ISO/IEC Guider 73 20002]	3.25 Hiệu quả các mục tiêu không thực tế và chắc chắn. CHÚ THÍCH 1 Một hiệu quả là một độ lệch so với dự kiến - tích cực và/hoặc tiêu cực. CHÚ THÍCH 2 Các mục tiêu có thể các có khía cạnh khác nhau (như tài chính, sức khỏe và sự an toàn và các mục đích môi trường) và có thể áp dụng ở các mức khác nhau (như: chiến lược, toàn tổ chức, dự án, sản phẩm và quy trình).	Việc sử dụng rõ ràng giới hạn của "rủi ro" trong ISO/IEC 20000, mặc dù nhiều khía cạnh chủ động của việc quản lý dịch vụ là nhằm mục đích giảm thiểu các rủi ro. Nó phải được chú thích rằng khái niệm "rủi ro" đáp ứng trong TCVN ISO/IEC 27001 được sửa đổi tương tự trong ISO/IEC 20000-1, dựa trên ISO 31000. Xem "lỗ hổng kỹ thuật".

Thuật ngữ	ISO/IEC 27000:2009	ISO/IEC 20000-1:2011	Ghi chú sử dụng thuật ngữ trong cả hai tiêu chuẩn
		CHÚ THÍCH 3 Rủi ro thường được đặc trưng bởi tham chiếu tới các sự kiện và hậu quả tiềm ẩn, hoặc một kết hợp của chúng CHÚ THÍCH 4 Rủi ro thường được diễn tả trong thuật ngữ kết hợp của một sự kết hợp hậu quả của một sự kiện (bao gồm các thay đổi trong nhiều tình huống) và khả năng tương ứng với sự xuất hiện [ISO 31000:2009]	
Chấp nhận rủi ro	2.35 Quyết định chấp nhận một rủi ro (2.34). [ISO/IEC Guide 73:2002]	Không được định nghĩa.	Cụm từ "sự chấp nhận rủi ro" không được định nghĩa hoặc sử dụng trong ISO/IEC 20000-1. Tuy nhiên, trong ISO/IEC 20000-1 các yêu cầu để định nghĩa lĩnh vực chấp nhận rủi ro trong kế hoạch quản lý dịch vụ, Điều 4.5.2 và trong quy trình quản lý an ninh thông tin, Điều 6.6.1, Các khái niệm tương đồng trong Điều 5.4, trong các yêu cầu sử dụng lĩnh vực chấp nhận.
Phân tích rủi ro	2.36 Sử dụng có hệ thống thông tin để định danh các nguồn và để đánh giá rủi ro (2.34). [ISO/IEC Guide 73:2002] CHÚ THÍCH Phân tích rủi ro cung cấp một cơ sở cho việc đánh giá rủi ro (2.41), xử lý rủi ro (2.43) và chấp nhận rủi ro (2.35).	Không được định nghĩa.	Xem "đánh giá rủi ro". Việc quan tâm đặc biệt phải được áp dụng, phân tích rủi ro được định ngĩa không giống "chấp nhận rủi ro", xem ISO/IEC 27005 để tham chiếu.
Đánh giá rủi ro	2.37 Quy trình tổng thể (2.31) của việc phân tích rủi ro (2.36) và đánh giá rủi ro (2.41).	Không được định nghĩa.	Các tham chiếu trong ISO/IEC 20000-1 cho việc đánh giá rủi ro liên quan tới các dịch vụ. Ví dụ: Điều 4.5.3 (Thiết lập và vận hành SMSM (Thực hiện) bao gồm "... d) định danh, đánh giá và quản lý các rủi ro cho các dịch vụ".

Thuật ngữ	ISO/IEC 27000:2009	ISO/IEC 20000-1:2011	Ghi chú sử dụng thuật ngữ trong cả hai tiêu chuẩn
	[ISO/IEC Guide 73:20002]		Điều 5.2 (Lập kế hoạch cho các dịch vụ thay đổi hoặc mới) bao gồm "... f) định danh, đánh giá và quản lý rủi ro." Điều 6.6.1: "d) đảm bảo rằng các đánh giá rủi ro thông tin được tiến hành trong khoảng thời gian kế hoạch".
Kết nối rủi ro	2.38 Việc trao đổi hoặc chia sẻ thông tin về rủi ro (2.34) giữa người quyết định và các bên khác. [ISO/IEC Guide 73:2002]	Không được định nghĩa.	Không được sử dụng trong ISO/IEC 20000-1 trong bất kỳ cách thức liên quan đến rủi ro nào.
Tiêu chí rủi ro	2.39 Các thuật ngữ cho việc tham chiếu bởi tầm quan trọng của rủi ro (2.34) được đánh giá. [ISO/EIC Guide 73 2002]	Không được định nghĩa.	Được sử dụng trng ISO/EIC 20000-1 ở cách thức tương tự trong việc sử dụng TCVN ISO/IEC 27001, ví dụ: ISO/IEC 20000-1, Điều 4.5.2 "Kế hoạch quản lý dịch vụ phải bao gồm một tham chiếu cho ... j) sự tiếp cận để được thực hiện cho việc quản lý các rủi ro và tiêu chí chấp nhận các rủi ro". Khái niệm tương tự cho cả hai tiêu chuẩn, nhưng có ý nghĩa lớn hơn đối với TCVN ISO/IEC 27001 hơn là ISO/IEC 20000.
Đánh giá rủi ro	2.40 Hoạt động để gán các giá trị cho khả năng và các hậu qủa của một rủi ro. [ISO/IEC Guide 73 2002]	Không được định nghĩa.	Xem "đánh giá rủi ro".
Đánh giá rủi ro	2.41 Quy trình (2.31) so sánh đánh giá rủi ro (2.34) chống lại tiêu chí rủi ro sẵn có (2.39) để xác định ý nghĩa của rủi ro (2.34). [ISO/IEC Guide 73;2002]	Không được định nghĩa.	Xem "đánh giá rủi ro".

Thuật ngữ	ISO/IEC 27000:2009	ISO/IEC 20000-1:2011	Ghi chú sử dụng thuật ngữ trong cả hai tiêu chuẩn
Quản lý rủi ro	2.42 Các hoạt động phối hợp để định hướng và kiểm soát một tổ chức liên quan đến rủi ro (2.34). [ISO/IEC Guide 73:2002] CHÚ THÍCH Quản lý rủi ro chủ yếu bao gồm việc đánh giá rủi ro (2.37), xử lý rủi ro (2.43), chấp nhận rủi ro (2.35), kết nối rủi ro (2.38), giám sát rủi ro và đáng giá rủi ro.	Không được định nghĩa.	Chủ yếu cùng nghĩa trong cả hai tiêu chuẩn.
Xử lý rủi ro	2.43 Quy trình (2.31) lựa chọn và thiết lập tính toán thay đổi rủi ro (2.34). [ISO/IEC Guide 73:2002]	Không được định nghĩa.	Thuật ngữ "xử lý rủi ro" không được sử dụng trong ISO/IEC 20000-1, nó được bao trùm trong thuật ngữ quản lý rủi ro (xem ví dụ trong "đánh giá rủi ro").
Dịch vụ	Không được định nghĩa.	3.26 Cách thức phân phối giá trị cho khách hàng bằng cách tạo điều kiện cho các kết quả mà khách hành muốn đạt được. CHÚ THÍCH 1 Dịch vụ nhìn chung là vô hình. CHÚ THÍCH 2 Một dịch vụ có thể được phân phối cho bên cung cấp dịch vụ bởi mọt bên cung cấp, một nhóm nội bộ hoặc một khách hàng đúng vai trò như một bên cung cấp.	Không tương ứng trực tiếp.

Thuật ngữ	ISO/IEC 27000:2009	ISO/IEC 20000-1:2011	Ghi chú sử dụng thuật ngữ trong cả hai tiêu chuẩn
Thành phần dịch vụ	Không được định nghĩa.	3.27 Đơn vị đơn lẻ của một dịch vụ mà khi kết hợp với các đơn vị khác phân phối một dịch vụ hoàn chỉnh. VÍ DỤ Phần cứng, phần mềm, các công cụ, ứng dụng, văn bản, thông tin, quy trình hoặc các dịch vụ hỗ trợ. CHÚ THÍCH Một thành phần dịch vụ có thể bao gồm một hoặc nhiều CI.	Không tương ứng trực tiếp.
Dịch vụ liên tục	Không được định nghĩa	3.28 Khả năng quản lý các rủi ro và sự kiện mà có các tác động nghiêm trọng trên một hoặc nhiều dịch vụ thay vì phân phối liên tục các dịch vụ ở các mức thỏa thuận.	Xem "lỗ hổng kỹ thuật" và "các rủi ro". Xem "kinh doanh liên tục". Dịch vụ liên tục được xem như là một tập phụ của kinh doanh liên tục.
Thỏa thuận mức dịch vụ (SLA)	Không được định nghĩa.	3.29 Thỏa thuận bằng văn bản giữa bên cung cấp dịch vụ và khách hàng mà định danh các dịch vụ và các đối tượng dịch vụ. CHÚ THÍCH 1 Một thỏa thuận mức dịch vụ có thể được thực hiện giữa bên cung cấp dịch vụ và một bên cung cấp, một nhóm nội bộ hoặc một khách hàng đóng vai trò như một bên cung cấp. CHÚ THÍCH 2 Một thỏa thuận mức dịch vụ có thể bao gồm trong một hợp đồng hoặc loại khác của tài liệu thỏa thuận.	Thuật ngữ này không được sử dụng trong TCVN ISO/IEC 27001. Tuy nhiên, định nghĩa được chấp nhận khi đề cập đến mục đích kiểm soát A.10.2 khi các khía cạnh an ninh của việc phân phối và duy trì dịch vụ của một bên thứ ba liên quan, như kiểm soát A.10.2.1 (các mức thỏa thuận dịch vụ liên tục).

Thuật ngữ	ISO/IEC 27000:2009	ISO/IEC 20000-1:2011	Ghi chú sử dụng thuật ngữ trong cả hai tiêu chuẩn
Quản lý dịch vụ	Không được định nghĩa.	3.30 Tập các khả năng và quy trình để định hướng và kiểm soát các hoạt động và tài nguyên của bên cung cấp dịch vụ đối với việc thiết kế, chuyển giao, phân phối và nâng cấp các dịch vụ để đáp ứng đầy đủ các yêu cầu dịch vụ.	Mục đích kiểm soát A.10.2 của TCVN ISO/IEC 27001, liên quan đến thuật ngữ này.
Hệ thống quản lý dịch vụ (SMS)	Không được định nghĩa.	3.31 Hệ thống quản lý định hướng và kiểm soát các hành động quản lý dịch vụ của bên cung cấp dịch vụ. CHÚ THÍCH 1 Một hệ thống quản lý là một tập của các thành phần liên tác hoặc liên hợp để thực hiện chính sách hoặc các mục tiêu để đạt được các mục tiêu đó. CHÚ THÍCH 2 SMS bao gồm tất cả các chính sách quản lý dịch vụ, mục tiêu, kế hoạch, quy trình, văn bản và các tài nguyên yêu cầu cho việc thiết kế, chuyển giao, phân phối và nâng cấp các dịch vụ và đáp ứng đầy đủ các yêu cầu trong phần này của ISO/IEC 20000. CHÚ THÍCH 3 Được đáp ứng từ định nghĩa "hệ thống quản lý chất lượng" trong TCVN ISO 9000:2007 (ISO/IEC 9000:2005).	Xem "hệ thống quản lý an ninh thông tin" (ISMS).
Nhà cung cấp dịch vụ	Không được định nghĩa.	3.32 Tổ chức hay một phần của một tổ chức mà quản lý và phân phối một hoặc nhiều dịch vụ cho khách hàng.	Bên cung cấp dịch vụ trong ISO/IEC 20000-1, định nghĩa 3.32 là tổ chức mà nhằm đáp ứng đầy đủ các yêu cầu trong ISO/IEC 20000-1. Thuật ngữ được sử dụng bởi nó đưa ra một điểm khác biệt

Thuật ngữ	ISO/IEC 27000:2009	ISO/IEC 20000-1:2011	Ghi chú sử dụng thuật ngữ trong cả hai tiêu chuẩn
		CHÚ THÍCH Một khách hàng có thể là nội bộ hoặc ngoại bộ đối với tổ chức của bên cung cấp dịch vụ.	giữa bên cung cấp dịch vụ và các nhóm khác, là các khách hàng, các bên khác (các bên cung cấp, các nhóm nội bộ, khách hàng, đóng vai trò như các bên cung cấp), các tổ chức ngoại bộ, các bên quan tâm hoặc các bên cung cấp sản phẩm hoặc dịch vụ hỗ trợ vận hành SMS. Một bên cung cấp dịch vụ có thể là mọt phần của một tổ chức lớn hơn hoặc toàn bộ một tổ chức.
Yêu cầu dịch vụ	Không được định nghĩa.	3.33 Yêu cầu thông tin, lời khuyên, truy cập từ một dịch vụ hoặc một thay đổi tiền-chấp nhận.	Không tương ứng trực tiếp.
Yêu cầu dịch vụ	Không được định nghĩa.	3.34 Các nhu cầu của khách hàng và người sử dụng dịch vụ, bao gồm các yêu cầu mức dịch vụ, và các nhu cầu của bên cung cấp dịch vụ.	Yêu cầu dịch vụ được định nghĩa trong ISO/IEC 20000-1, định nghĩa 3.34. Trong TCVN ISO/IEC 27001, "yêu cầu" được dùng ở nghĩa tiếng Anh thông thường của: một nhu cầu, một vài thứ mà được yêu cầu, cần thiết, được yêu cầu. Nó không được dùng trong ISO/IEC 20000 như "các yêu cầu dịch vụ", mặc dù có một vài sử dụng của "các yêu cầu an ninh", yêu cầu pháp lý hoặc quy định.
Bên cung cấp	Không được định nghĩa.	3.35 Tổ chức hoặc một phần của một tổ chức mà là bên ngoài đối với tổ chức của bên cung cấp dịch vụ và tham gia trong một hợp đồng với bên cung cấp dịch vụ để góp phần vào việc thiết kế, chuyển giao, phân phối và nâng cấp một hoặc nhiều dịch vụ hoặc các quy trình.	ISO/IEC 20000-1 bao gồm các tham chiếu và các yêu cầu cho việc quản lý của: a) Các bên cung cấp, b) Các bên cung cấp chính (quản lý các bên cung cấp hợp đồng phụ), c) Các khách hàng (đóng vai trò như các bên cung cấp).

Thuật ngữ	ISO/IEC 27000:2009	ISO/IEC 20000-1:2011	Ghi chú sử dụng thuật ngữ trong cả hai tiêu chuẩn
		CHÚ THÍCH Các bên cung cấp bao gồm các bên cung cấp dẫn đầu nhưng không gồm các nhà thầu phụ của họ.	Tất cả các đóng góp cho tổng thể dịch vụ và được quản lý bởi bên cung cấp dịch vụ: Quản lý dịch vụ bao gồm các bên cung cấp/bên cung cấp chính (và thông qua các bên cung cấp chính, bên cung cấp hợp đồng phụ). Quản lý mức dịch vụ bao trùm việc quản lý các các nhóm nội bộ và các khách hành, đóng vai trò như các bên cung cấp. TCVN ISO/IEC 27001 sử dụng thuật ngữ "bên cung cấp" chỉ một lần.
Báo cáo áp dụng	2.44 Báo cáo tài liệu mô tả các mục tiêu kiểm soát (2.11) và các kiểm soát (2.10) mà liên quan và được chấp nhận cho ISMS của tổ chức (2.33).	Không được định nghĩa hoặc được sử dụng.	ISO/IEC 20000-1, Điều 1.2 Ứng dụng không giống báo cáo áp dụng trong TCVN ISO/IEC 27001.
Đe dọa	2.45 Nguyên nhân tiềm ẩn của một rắc rối không mong đợi, dẫn đến việc nguy hại một hệ thống hoặc tổ chức.	Không được định nghĩa.	Trong ISO/IEC 20000-1, thuật ngữ "đe dọa" được sử dụng một lần, trong định nghĩa 3.12: "Sự cố an ninh thông tin: đơn lẻ hoặc một chuỗi của các sự kiện an ninh thông tin không mong muốn hoặc mong đợi mà có một khả năng quan trọng hoặc ảnh hưởng đến vận hành kinh doanh và đe dọa an ninh thông tin".
Chuyển đổi	Không được định nghĩa.	3.37 Các hành động liên quan trong việc di chuyển một dịch vụ thay đổi hoặc mới tới hoặc từ môi trường sống.	Một liên kết tồn tại trong việc chuyển đổi, được sử dụng trong ISO/IEC 20000-1, Điều 5 và cách thức trong một vài thay đổi được kiểm soát dựa trên TCVN ISO/IEC 27001. Các quy trình kiểm soát, được miêu tả trong ISO/IEC 20000-1, Điều 5 và 9, cũng được liên kết chặt chẽ trong định nghĩa này TCVN ISO/IEC 27001 quản lý việc quản lý thay đổi trong các điều sau: A.10.1.2 Quản lý thay đổi các thủ tục vận hành và trách nhiệm. A.10.2.3 Quản lý các thay đổi các dịch vụ bên thứ ba.

Thuật ngữ	ISO/IEC 27000:2009	ISO/IEC 20000-1:2011	Ghi chú sử dụng thuật ngữ trong cả hai tiêu chuẩn
Lỗ hổng an ninh	2.46 Điểm yếu của một tài sản (2.3) hoặc kiểm soát (2.10) mà có thể bị khai thác bởi một đe dọa (2.45).	Không được định nghĩa hoặc được sử dụng.	Không tương ứng trực tiếp.

Thư mục tài liệu tham khảo

[1] ISO 9000 *Quality management systesm – Fundamentals and vocabulary*

[2] ISO 9004 *Quality management systems – Guidelines for performance improvements*

[3] ISO/IEC TS 15504-8 *Information tecnology – Service management - Part 8: Process assessment mode for service management* (đang phát triển)

[4] TCVN ISO 19011:2003 *Hệ thống quản lý chất lượng - Hướng dẫn đánh giá hệ thống quản lý chất lượng, môi trường* (ISO 19011 *Quality management systems – Guidelines for quality and/or environmental management systems auditing*)

[5] TCVN 8695-2:2011 *Công nghệ thông tin - Quản lý dịch vụ - Phần 2: Quy tắc thực hàng* (ISO/IEC 20000-2 *Information tecnology – Service management – Part 2: Guidance on the application of service management systems*)

[6] ISO/IEC 20000-3 *Information tecnology – Service management – Part 3: Guidance on the application of scope definition and applicability for ISO/IEC 20000-1*

[7] ISO/IEC 20000-4 *Information tecnology – Service management – Part 4: Process referance model for service management*

[8] ISO/IEC 20000-5 *Information tecnology – Service management – Part 5: Exemplar implementation plan for ISO/IEC 20000-1*

[9] ISO/IEC TR 90006[2] *Information tecnology - Guidelines for the application of ISO 9001:2008 to IT service management and it intergration with ISO/IEC 20000-1:2011*

[10] TCVN ISO/IEC 27002 Công nghệ thông tin - Các kỹ thuật an toàn - Quy tắc thực hành quản lý an toàn thông tin (ISO/IEC 27002 *Information technology – Security techniques – Information security management systems - Code of practice for information security control*) (đang soát xét)

[11] ISO/IEC 27003 *Information technology – Security techniques – Information security management systems - Information security management system implementation guidance*

[12] ISO/IEC 27004 *Information technology – Security techniques – Information security management systems - Information security management system measurements*

[13] ISO/IEC 27005 *Information technology – Security techniques – Information security management systems - Information security risk management*

[14] ISO/IEC 27006 *Information technology – Security techniques – Information security management systems - Requirements for bodies providing audiit and certification of information security management systems*

[15] ISO/IEC 27007 *Information technology – Security techniques – Information security management*

[2] Đã được xuất bản.

systems - Guidelines for information security management system auditing

[16] ISO/IEC TR 27008 *Information technology – Security techniques – Information security management systems - Guidelines for auditors on information security controls*

[17] ISO/IEC 27010 *Information technology – Security techniques – Information security management systems - Information security management system for inter-sector and inter-organizational communications*

[18] ISO/IEC 27014 *Information technology – Security techniques – Information security management systems - Governance of information security*

[19] ISO/IEC 31000 *Risk management - Principles and Guidelines on Implementation*