TIÊU CHUẨN QUỐC TẾ

ISO 22301

Phiên bản 2
2019-10

An ninh và khả năng phục hồi - Hệ thống quản lý kinh doanh liên tục - Các yêu cầu

CÔNG TY CỔ PHẦN CHỨNG NHẬN & GIÁM ĐỊNH QUỐC TẾ EFC

Tầng 10 - Tòa nhà Pax Sky, số 51 Nguyễn Cư Trinh, Phường Nguyễn Cư Trinh, Quận 1, TP Hồ Chí Minh
Điện thoại: (028) 38 95 96 95 (3 lines) Fax: (028) 38 95 93 94
Website: www.efc.vn Email: info@efcvietnam.com

Lưu ý:
(1) Bản chuyển ngữ ngày được thực hiện bởi Công ty Cổ Phần Chứng Nhận & Giám Định Quốc Tế EFC
(2) Bản chuyển ngữ này được sử dụng cho mục đích đào tạo.

MỤC LỤC

Lời tựa

ISO (Tổ chức Tiêu chuẩn hóa Quốc tế) là một liên đoàn toàn cầu của các tổ chức tiêu chuẩn quốcgia (các tổ chức thành viên của ISO). Công việc chuẩn bị các tiêu chuẩn quốc tế thường được thựchiện thông qua các Ủy ban kỹ thuật của ISO. Mỗi tổ chức thành viên quan tâm đến một chủ đề màỦy ban kỹ thuật đã được thành lập có quyền được đại diện trong ủy ban đó. Các tổ chức quốc tế,chính phủ và phi chính phủ, có liên hệ với ISO, cũng tham gia vào công việc này. ISO hợp tác chặtchẽ với Ủy ban Kỹ thuật Điện Quốc tế (IEC) về tất cả các vấn đề của tiêu chuẩn kỹ thuật điện.

Các thủ tục được sử dụng để phát triển tiêu chuẩn này và những thủ tục nhằm mục đích duy trì tiêuchuẩn này được mô tả trong Hướng dẫn ISO / IEC, Phần 1. Đặc biệt, cần lưu ý các tiêu chí phêduyệt khác nhau cần thiết cho các loại tiêu chuẩn ISO khác nhau. Tiêu chuẩn này được soạn thảotheo các quy tắc biên tập của Chỉ thị ISO / IEC, Phần 2 (xem www.iso.org/directives).

Cần chú ý đến khả năng một số yếu tố của tiêu chuẩn này có thể (may) là đối tượng của quyền sángchế. ISO sẽ không chịu trách nhiệm xác định bất kỳ hoặc tất cả các quyền bằng sáng chế như vậy.

Chi tiết về bất kỳ quyền sáng chế nào được xác định trong quá trình phát triển tiêu chuẩn sẽ có trong Phần giới thiệu và / hoặc trong danh sách ISO các tuyên bố về bằng sáng chế đã nhận được (xem www.iso.org/patents).

Bất kỳ tên thương mại nào được sử dụng trong tiêu chuẩn này là thông tin được cung cấp để thuận tiện cho người dùng và không cấu thành sự chứng thực. Để được giải thích về bản chất tự nguyện của các tiêu chuẩn, ý nghĩa của các thuật ngữ và cách diễn đạt cụ thể của ISO liên quan đến đánh giá sự phù hợp, cũng như thông tin về việc ISO tuân thủ các nguyên tắc của Tổ chức Thương mại Thế giới (WTO) trong Hàng rào Kỹ thuật đối với Thương mại (TBT), hãy xem www.iso.org/iso/foreword.html.

Tiêu chuẩn này được chuẩn bị bởi Ủy ban kỹ thuật ISO/TC 292, An ninh và khả năng phục hồi. Ấn bản thứ hai này hủy bỏ và thay thế ấn bản đầu tiên (ISO 22301:2012), đã được sửa đổi về mặt kỹ thuật. Những thay đổi chính so với phiên bản trước như sau:

— Các yêu cầu của ISO đối với các tiêu chuẩn hệ thống quản lý, đã phát triển từ năm 2012, đã được áp dụng;

— các yêu cầu đã được làm rõ, không có thêm yêu cầu mới;

— các yêu cầu về tính liên tục của ngành kinh doanh cụ thể hiện nay hầu như hoàn toàn nằm trong

Điều khoản 8;

— Điều khoản 8 đã được cấu trúc lại để cung cấp sự hiểu biết rõ ràng hơn về các yêu cầu chính;

— một số điều khoản về tính liên tục của ngành kinh doanh cụ thể đã được sửa đổi để cải thiện sựrõ ràng và phản ánh tư duy hiện tại.

Mọi phản hồi hoặc câu hỏi về tiêu chuẩn này phải được chuyển đến cơ quan tiêu chuẩn quốc gia của người dùng. Danh sách đầy đủ về các cơ quan này có thể (can) được tìm thấy tại www.iso.org/members.html.

Giới thiệu

0.1 Khái quát

Tiêu chuẩn này quy định cấu trúc và các yêu cầu để thực hiện và duy trì hệ thống quản lý tính liên tục trong kinh doanh (BCMS) nhằm phát triển tính liên tục của hoạt động kinh doanh phù hợp với mức độ và loại tác động mà tổ chức có thể (may) chấp nhận hoặc không thể (may not) chấp nhận sau một sự gián đoạn.

Kết quả của việc duy trì một BCMS được định hình bởi các yêu cầu pháp lý, quy định, tổ chức và ngành của tổ chức, các sản phẩm và dịch vụ được cung cấp, các quá trình được sử dụng, quy mô và cấu trúc của tổ chức cũng như các yêu cầu của các bên liên quan. BCMS nhấn mạnh tầm quan trọng của:

— hiểu nhu cầu của tổ chức và sự cần thiết của việc thiết lập các chính sách và mục tiêu liên tục của doanh nghiệp;

— điều hành và duy trì các quá trình, khả năng và cấu trúc phản ứng để đảm bảo tổ chức sẽ tồn tại sau những gián đoạn;

— giám sát và xem xét việc thực hiện và tính hiệu lực của BCMS;

— cải tiến liên tục dựa trên các đo lường định tính và định lượng.

BCMS, giống như bất kỳ hệ thống quản lý nào khác, bao gồm các thành phần sau:

a) một chính sách;

b) những người có năng lực với trách nhiệm được xác định;

c) các quá trình quản lý liên quan đến:

1) chính sách;

2) hoạch định;

3) thực hiện và điều hành;

4) đánh giá kết quả hoạt động;

5) xem xét của lãnh đạo;

6) cải tiến liên tục;

d) thông tin dạng văn bản hỗ trợ kiểm soát hoạt động và cho phép đánh giá kết quả hoạt động.

0.2 Lợi ích của hệ thống quản lý liên tục trong kinh doanh

Mục đích của BCMS là chuẩn bị, cung cấp và duy trì các biện pháp kiểm soát và khả năng để quản lý khả năng tiếp tục hoạt động chung của một tổ chức trong thời gian gián đoạn. Để đạt được điều

này, tổ chức là:

a) từ góc độ kinh doanh:

1) hỗ trợ các mục tiêu chiến lược của tổ chức;

2) tạo ra lợi thế cạnh tranh;

3) bảo vệ và nâng cao danh tiếng và sự tín nhiệm của tổ chức;

4) đóng góp vào khả năng phục hồi của tổ chức;

b) từ góc độ tài chính:

1) giảm thiểu rủi ro pháp lý và tài chính;

2) giảm chi phí gián tiếp và trực tiếp của sự gián đoạn;

c) từ quan điểm của các bên quan tâm:

1) bảo vệ cuộc sống, tài sản và môi trường;

2) xem xét mong đợi của các bên quan tâm;

3) cung cấp niềm tin vào khả năng thành công của tổ chức;

d) từ góc độ quá trình nội bộ:

1) cải thiện khả năng của tổ chức để duy trì hiệu quả trong thời gian gián đoạn;

2) thể hiện khả năng chủ động kiểm soát rủi ro một cách hiệu quả và có hiệu lực;

3) giải quyết các lỗ hổng trong hoạt động.

0.3 Chu kỳ Lập kế hoạch - Thực hiện - Kiểm tra – Hành động (PDCA)

Tiêu chuẩn này áp dụng chu trình Lập kế hoạch (thiết lập), Thực hiện (thực hiện và điều hành),

Kiểm tra (giám sát và xem xét) và Hành động (duy trì và cải tiến) (PDCA) để thực hiện, duy trì và liên tục nâng cao hiệu lực của BCMS của một tổ chức.

Điều này đảm bảo mức độ nhất quán với các tiêu chuẩn hệ thống quản lý khác, chẳng hạn như ISO 9001, ISO 14001, ISO / IEC 20000-1, ISO / IEC 27001 và ISO 28000, do đó hỗ trợ việc thực hiện và điều hành nhất quán và tích hợp với các hệ thống quản lý liên quan.

Phù hợp với chu trình PDCA, từ Điều khoản 4 đến Điều khoản 10 bao gồm các thành phần sau.

— Điều khoản 4 giới thiệu các yêu cầu cần thiết để thiết lập bối cảnh của BCMS áp dụng cho tổ chức, cũng như nhu cầu, yêu cầu và phạm vi.

— Điều khoản 5 tóm tắt các yêu cầu cụ thể đối với vai trò của lãnh đạo cao nhất trong BCMS và cách lãnh đạo trình bày các kỳ vọng của mình với tổ chức thông qua một tuyên bố chính sách.

— Điều khoản 6 mô tả các yêu cầu đối với việc thiết lập các mục tiêu chiến lược và các nguyên tắc hướng dẫn cho toàn bộ BCMS.

— Điều khoản 7 hỗ trợ các hoạt động BCMS liên quan đến việc thiết lập năng lực và trao đổi thông tin trên cơ sở định kỳ / khi cần thiết với các bên quan tâm, đồng thời lập hồ sơ, kiểm soát, duy trì và lưu giữ thông tin dạng văn bản được yêu cầu.

— Điều khoản 8 xác định các nhu cầu liên tục của doanh nghiệp, xác định cách giải quyết và phát triển các thủ tục để quản lý tổ chức trong thời gian gián đoạn.

— Điều khoản 9 tóm tắt các yêu cầu cần thiết để đo lường hoạt động liên tục của hoạt động kinh doanh, sự phù hợp của BCMS với tiêu chuẩn này và để tiến hành xem xét của ban lãnh đạo.

— Điều khoản 10 xác định và hành động đối với sự không phù hợp của BCMS và cải tiến liên tục thông qua hành động khắc phục.

0.4 Nội dung của tiêu chuẩn này

Tiêu chuẩn này tuân thủ các yêu cầu của ISO đối với các tiêu chuẩn hệ thống quản lý. Các yêu cầu này bao gồm cấu trúc bậc cao, văn bản cốt lõi giống hệt nhau và các thuật ngữ chung với các định nghĩa cốt lõi, được thiết kế để mang lại lợi ích cho người dùng triển khai nhiều tiêu chuẩn hệ thống quản lý ISO.

Tiêu chuẩn này không bao gồm các yêu cầu cụ thể đối với các hệ thống quản lý khác, mặc dù các yếu tố của nó có thể (can) được điều chỉnh hoặc tích hợp với các yêu cầu của các hệ thống quản lý khác.

Tiêu chuẩn này bao gồm các yêu cầu mà một tổ chức có thể (can) sử dụng để thực hiện BCMS và đểđánh giá sự phù hợp. Một tổ chức muốn chứng minh sự phù hợp với tiêu chuẩn này có thể (can) làm như vậy bằng cách:

— tự xác định, tự công bố; hoặc

— tìm kiếm sự xác nhận về sự phù hợp của tổ chức bởi các bên có lợi ích trong tổ chức, chẳng hạn như khách hàng; hoặc

— tìm kiếm xác nhận về bản xác định của mình bởi một bên bên ngoài tổ chức; hoặc

— tìm kiếm chứng nhận / đăng ký BCMS của mình bởi một tổ chức bên ngoài.

Các Điều khoản từ 1 đến 3 trong tiêu chuẩn này đưa ra phạm vi, các tài liệu viện dẫn và các thuật ngữ và định nghĩa áp dụng cho việc sử dụng tiêu chuẩn này. Các Điều khoản từ 4 đến 10 bao gồm các yêu cầu được sử dụng để đánh giá sự phù hợp với tiêu chuẩn này.

Trong tiêu chuẩn này, các từ sau được sử dụng:

a) “phải” (shall) chỉ ra một yêu cầu;

b) “nên” (should) chỉ ra một khuyến nghị;

c) “có thể” (may) chỉ ra một sự cho phép;

d) “có thể” (can) chỉ ra một khả năng hoặc một khả năng.

Thông tin được đánh dấu là “CHÚ THÍCH” là để hướng dẫn cách hiểu hoặc làm rõ yêu cầu liên quan. “Chú thích” được sử dụng trong Điều khoản 3 cung cấp thông tin bổ sung bổ sung cho dữ liệu thuật ngữ và có thể (can) chứa các điều khoản liên quan đến việc sử dụng một thuật ngữ.

An ninh và khả năng phục hồi - Hệ thống quản lý- Kinh doanh liên tục –
Các yêu cầu

1 Phạm vi

Tiêu chuẩn này quy định các yêu cầu để thực hiện, duy trì và cải tiến hệ thống quản lý nhằm bảo vệ, giảm thiểu khả năng xảy ra, chuẩn bị, ứng phó và phục hồi sau những gián đoạn khi chúng phát sinh.

Các yêu cầu quy định trong tiêu chuẩn này là chung và nhằm áp dụng cho tất cả các tổ chức hoặc các bộ phận của tổ chức đó, bất kể loại hình, quy mô và tính chất của tổ chức. Mức độ áp dụng các yêu cầu này tùy thuộc vào môi trường hoạt động và mức độ phức tạp của tổ chức.

Tiêu chuẩn này có thể áp dụng cho tất cả các loại hình và quy mô của các tổ chức:

a) thực hiện, duy trì và cải tiến BCMS;

b) tìm cách đảm bảo sự phù hợp với chính sách kinh doanh liên tục đã tuyên bố;

c) cần có khả năng tiếp tục cung cấp các sản phẩm và dịch vụ với năng suất xác định trước có thể chấp nhận được trong thời gian gián đoạn;

d) tìm cách nâng cao khả năng phục hồi thông qua việc áp dụng hiệu quả BCMS. Tiêu chuẩn này có thể (can) được sử dụng để đánh giá khả năng của một tổ chức trong việc đáp ứng các nhu cầu và nghĩa vụ liên tục kinh doanh của chính tổ chức đó.

2 Tiêu chuẩn viện dẫn

Các tiêu chuẩn sau đây được đề cập theo cách mà một số hoặc tất cả nội dung của chúng tạo thành các yêu cầu của tiêu chuẩn này. Đối với tiêu chuẩn ghi năm chỉ bản được nêu áp dụng. Đối với các tiêu chuẩn viện dẫn không ghi ngày tháng, phiên bản mới nhất của tiêu chuẩn viện dẫn (bao gồm mọi sửa đổi) sẽ được áp dụng. ISO 22300, An ninh và khả năng phục hồi - Từ vựng

3 Thuật ngữ và định nghĩa

Theo mục đích của tiêu chuẩn này, các thuật ngữ và định nghĩa được đưa ra trong ISO 22300 và những thuật ngữ sau đây được áp dụng.

ISO và IEC duy trì cơ sở dữ liệu thuật ngữ để sử dụng trong tiêu chuẩn hóa tại các địa chỉ sau:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

CHÚ THÍCH: Các thuật ngữ và định nghĩa được đưa ra dưới đây thay thế các thuật ngữ và định nghĩa được nêu trong ISO 22300: 2018.

3.1 hoạt động tập hợp một hoặc nhiều nhiệm vụ với đầu ra xác định
[NGUỒN: ISO 22300: 2018, 3.1, được sửa đổi - Định nghĩa đã được thay thế và ví dụ đã bị xóa.]

3.2 đánh giá (audit) quá trình có hệ thống, độc lập và được lập thành văn bản (3.26) để thu thập bằng chứng đánh giá và đánh giá nó một cách khách quan nhằm xác định mức độ đáp ứng các chuẩn mực đánh giá

CHÚ THÍCH 1: Cuộc đánh giá có thể (can) là cuộc đánh giá nội bộ (bên thứ nhất) hoặc cuộc đánh giá bên ngoài (bên thứ hai hoặc bên thứ ba) và nó có thể (can) là cuộc đánh giá kết hợp (kết hợp hai hoặc nhiều lĩnh vực).

CHÚ THÍCH 2: Đánh giá nội bộ được tiến hành bởi chính tổ chức (3.21) hoặc bởi một bên bên ngoài thay mặt tổ chức.

CHÚ THÍCH 3: “Bằng chứng đánh giá” và “chuẩn mực đánh giá” được định nghĩa trong ISO 19011.

CHÚ THÍCH 4: Các yếu tố cơ bản của cuộc đánh giá bao gồm việc xác định sự phù hợp (3.7) của một đối tượng theo một thủ tục được thực hiện bởi nhân viên không chịu trách nhiệm về đối tượng được đánh giá.

CHÚ THÍCH 5: Đánh giá nội bộ có thể (can) nhằm mục đích xem xét của ban giám đốc và các mục đích nội bộ khác và có thể (can) tạo cơ sở cho tuyên bố về sự phù hợp của một tổ chức. Tính độc lập có thể (can) được chứng minh bằng sự tự do khỏi trách nhiệm đối với hoạt động (3.1) được đánh giá. Đánh giá bên ngoài bao gồm đánh giá của bên thứ hai và thứ ba. Đánh giá của bên thứ hai được thực hiện bởi các bên có lợi ích trong tổ chức, chẳng hạn như khách hàng hoặc bởi những người khác thay mặt họ. Đánh giá của bên thứ ba được thựchiện bởi các tổ chức đánh giá độc lập, bên ngoài, chẳng hạn như các tổ chức cung cấp chứng nhận / đăng ký sự phù hợp hoặc các cơ quan chính phủ.

CHÚ THÍCH 6: Điều này tạo thành một trong những thuật ngữ chung và định nghĩa cốt lõi của cấu trúc bậc cao đối với các tiêu chuẩn hệ thống quản lý ISO. Định nghĩa ban đầu đã được sửa đổi bằng cách thêm Chú thích 4 và 5 vào.

3.3 kinh doanh liên tục khả năng của một tổ chức (3.21) để tiếp tục cung cấp các sản phẩm và dịch vụ (3.27) trong các khung thời gian có thể chấp nhận được với khả năng được xác định trước trong thời gian gián đoạn (3.10) [NGUỒN: ISO 22300: 2018, 3.24, được sửa đổi - Định nghĩa đã được thay thế.]

3.4 kế hoạch kinh doanh liên tục thông tin dạng văn bản (3.11) hướng dẫn tổ chức (3.21) ứng phó với sự gián đoạn (3.10) và tiếp tục, khôi phục và khôi phục việc cung cấp sản phẩm và dịch vụ (3.27) phù hợp với mục tiêu liên tục kinh doanh (3.3) (3.20)

[NGUỒN: ISO 22300: 2018, 3.27, được sửa đổi - Định nghĩa đã được thay thế và Chú thích 1 đã bị xóa.]

3.5 Phân tích tác động kinh doanh quá trình (3.26) phân tích tác động (3.13) theo thời gian gián đoạn (3.10) đối với tổ chức (3.21)

CHÚ THÍCH 1: Kết quả là một tuyên bố và lý giải cho các yêu cầu về tính liên tục của hoạt động kinh doanh (3.3) (3.28). [NGUỒN: ISO 22300: 2018, 3.29, được sửa đổi - Định nghĩa đã được thay thế và Chú thích 1 đã được bổ sung.]

3.6 năng lực khả năng áp dụng kiến thức và kỹ năng để đạt được kết quả dự định

CHÚ THÍCH 1: Điều này tạo thành một trong những thuật ngữ chung và định nghĩa cốt lõi của cấu trúc bậc cao đối với các tiêu chuẩn hệ thống quản lý ISO.

3.7 sự phù hợp đáp ứng đầy đủ một yêu cầu (3,28)

CHÚ THÍCH 1: Điều này tạo thành một trong những thuật ngữ chung và định nghĩa cốt lõi của cấu trúc bậc cao đối với các tiêu chuẩn hệ thống quản lý ISO.

3.8 cải tiến liên tục hoạt động (3.1) lặp đi lặp lại để nâng cao kết quả hoạt động (3.23)

CHÚ THÍCH 1: Điều này tạo thành một trong những thuật ngữ chung và định nghĩa cốt lõi của cấu trúc bậc cao đối với các tiêu chuẩn hệ thống quản lý ISO.

3.9 hành động khắc phục hành động để loại bỏ (các) nguyên nhân của sự không phù hợp (3.19) và ngăn ngừa tái diễn

CHÚ THÍCH 1: Điều này tạo thành một trong những thuật ngữ chung và định nghĩa cốt lõi của cấu trúc bậc cao đối với các tiêu chuẩn hệ thống quản lý ISO.

3.10 gián đoạn sự cố (3.14), dù có thể dự đoán hay không lường trước được, gây ra sự sai lệch tiêu cực ngoài kế hoạch so với việc cung cấp sản phẩm và dịch vụ dự kiến (3.27) theo các mục tiêu (3.21) của tổ chức (3.20) [NGUỒN: ISO 22300: 2018, 3.70, được sửa đổi - Định nghĩa đã được thay thế.]

3.11 thông tin dạng văn bản thông tin cần thiết phải được kiểm soát và duy trì bởi một tổ chức (3.21) và phương tiện chứa thông tin đó

CHÚ THÍCH 1: Thông tin dạng văn bản có thể (can) ở bất kỳ định dạng và phương tiện nào, và từ bất kỳ nguồn nào.

CHÚ THÍCH 2: Thông tin dạng văn bản có thể (can) tham chiếu đến:

— hệ thống quản lý (3.16), bao gồm các quá trình liên quan (3.26);

— thông tin được tạo ra để tổ chức hoạt động (tài liệu);

— bằng chứng về kết quả đạt được (hồ sơ).

CHÚ THÍCH 3: Đây là một trong những thuật ngữ chung và định nghĩa cốt lõi của cấu trúc bậc cao đối với các tiêu chuẩn hệ thống quản lý ISO.

3.12 hiệu lực mức độ thực hiện các hoạt động theo kế hoạch (3.1) và đạt được các kết quả theo kế hoạch

CHÚ THÍCH 1: Điều này tạo thành một trong những thuật ngữ chung và định nghĩa cốt lõi của cấu trúc bậc cao đối với các tiêu chuẩn hệ thống quản lý ISO.

3.13 tác động kết quả của sự gián đoạn (3.10) ảnh hưởng đến các mục tiêu (3.20)

[NGUỒN: ISO 22300: 2018, 3.107, được sửa đổi - Định nghĩa đã được thay thế.]

3.14 sự cố sự kiện có thể (can) xảy ra hoặc có thể dẫn đến sự gián đoạn (3.10), mất mát, khẩn cấp hoặc khủng hoảng

[NGUỒN: ISO 22300: 2018, 3.111, được sửa đổi - Định nghĩa đã được thay thế.]

3.15 bên quan tâm (thuật ngữ được ưu tiên) bên liên quan (thuật ngữ được thừa nhận) cá nhân hoặc tổ chức (3.21) có thể ảnh hưởng, bị ảnh hưởng bởi hoặc có nhận thức là bản thân họ bị ảnh hưởng bởi một quyết định hoặc hoạt động (3.1)

VÍ DỤ: Khách hàng, chủ sở hữu, nhân sự, nhà cung cấp, chủ ngân hàng, cơ quan quản lý, công đoàn, đối tác hoặc xã hội có thể bao gồm các đối thủ cạnh tranh hoặc các nhóm áp lực chống đối.

CHÚ THÍCH 1: Người ra quyết định có thể là một bên quan tâm.

CHÚ THÍCH 2: Các cộng đồng bị ảnh hưởng và người dân địa phương được coi là các bên quan tâm.

CHÚ THÍCH 3: Đây là một trong những thuật ngữ chung và định nghĩa cốt lõi của cấu trúc bậc cao đối với các tiêu chuẩn hệ thống quản lý ISO. Định nghĩa ban đầu đã được sửa đổi bằng cách thêm một ví dụ và Chú thích và 2.

3.16 hệ thống quản lý

Tập hợp các yếu tố có liên quan hoặc tương tác với nhau của một tổ chức (3.21) để thiết lập các chính sách (3.24) và các mục tiêu (3.20) và các quá trình (3.26) để đạt được các mục tiêu đó

CHÚ THÍCH 1: Hệ thống quản lý có thể (can) giải quyết một lĩnh vực duy nhất hoặc một số lĩnh vực.

CHÚ THÍCH 2: Các yếu tố của hệ thống bao gồm cấu trúc, vai trò và trách nhiệm, kế hoạch và hoạt động của tổ chức.

CHÚ THÍCH 3: Phạm vi của hệ thống quản lý có thể bao gồm toàn bộ tổ chức, các chức năng cụ thể và được xác định của tổ chức, các bộ phận cụ thể và được xác định của tổ chức, hoặc một hoặc nhiều chức năng trong một nhóm tổ chức.

CHÚ THÍCH 4: Đây là một trong những thuật ngữ chung và định nghĩa cốt lõi của cấu trúc bậc cao đối với các tiêu chuẩn hệ thống quản lý ISO.

3.17 đo lường quy trình (3.26) để xác định giá trị

CHÚ THÍCH 1: Điều này tạo thành một trong những thuật ngữ chung và định nghĩa cốt lõi của cấu trúc bậc cao đối với các tiêu chuẩn hệ thống quản lý ISO.

3.18 theo dõi xác định trạng thái của một hệ thống, một quá trình (3.26) hoặc một hoạt động (3.1)

CHÚ THÍCH 1: Để xác định tình trạng, có thể (can)cần phải kiểm tra, giám sát hoặc quan sát nghiêm túc.

CHÚ THÍCH 2: Đây là một trong những thuật ngữ chung và định nghĩa cốt lõi của cấu trúc bậc cao đối với các tiêu chuẩn hệ thống quản lý ISO.

3.19 sự không phù hợp không đáp ứng đầy đủ yêu cầu (3.28)

CHÚ THÍCH 1: Điều này tạo thành một trong những thuật ngữ chung và định nghĩa cốt lõi của cấu trúc bậc cao đối với các tiêu chuẩn hệ thống quản lý ISO.

3.20 mục tiêu kết quả phải đạt được

CHÚ THÍCH 1: Mục tiêu có thể (can) là chiến lược, chiến thuật hoặc hoạt động.

CHÚ THÍCH 2: Các mục tiêu có thể (can) liên quan đến các lĩnh vực khác nhau (chẳng hạn như các mục tiêutài chính, sức khỏe và an toàn, và môi trường) và có thể (can) áp dụng ở các cấp độ khác nhau (chẳng hạn như chiến lược, toàn tổ chức, dự án, sản phẩm và quy trình (3.26)).

CHÚ THÍCH 3: Mục tiêu có thể (can) được thể hiện theo những cách khác, ví dụ: như một kết quả dự định, một mục đích, một tiêu chí hoạt động, như một mục tiêu liên tục của hoạt động kinh doanh (3.3), hoặc bằng cách sử dụng các từ khác có nghĩa tương tự (ví dụ: mục tiêu, mục tiêu hoặc mục tiêu).

CHÚ THÍCH 4: Trong bối cảnh của các hệ thống quản lý tính liên tục của hoạt động kinh doanh (3.16), các mục tiêu về tính liên tục của hoạt động kinh doanh do tổ chức (3.21) đặt ra, phù hợp với chính sách liên tục của hoạt động kinh doanh (3.24), để đạt được các kết quả cụ thể.

CHÚ THÍCH 5: Đây là một trong những thuật ngữ chung và định nghĩa cốt lõi của cấu trúc bậc cao đối với các tiêu chuẩn hệ thống quản lý ISO.

3.21 tổ chức cá nhân hoặc nhóm người có chức năng riêng với trách nhiệm, quyền hạn và các mối quan hệ để đạt được các mục tiêu của mình (3.20)

CHÚ THÍCH 1: Khái niệm tổ chức bao gồm, nhưng không giới hạn, thương nhân độc quyền, công ty, tập đoàn, công ty, doanh nghiệp, cơ quan, đối tác, tổ chức từ thiện hoặc tổ chức, hoặc một phần hoặc sự kết hợp của chúng, cho dù được hợp nhất hay không, công cộng hoặc tư nhân.

CHÚ THÍCH 2: Đối với các tổ chức có nhiều đơn vị hoạt động, một đơn vị hoạt động duy nhất có thể (can) được xác định là một tổ chức.

CHÚ THÍCH 3: Đây là một trong những thuật ngữ chung và định nghĩa cốt lõi của cấu trúc bậc cao đối với các tiêu chuẩn hệ thống quản lý ISO. Định nghĩa ban đầu đã được sửa đổi bằng cách thêm Chú thích 2 vào.

3.22 thuê ngoài thực hiện một thỏa thuận trong đó một tổ chức bên ngoài (3.21) thực hiện một phần chức năng hoặc quá trình của tổ chức (3.26)

CHÚ THÍCH 1: Tổ chức bên ngoài nằm ngoài phạm vi của hệ thống quản lý (3.16), mặc dù chức năng hoặc quy trình được thuê ngoài nằm trong phạm vi đó.

CHÚ THÍCH 2: Đây là một trong những thuật ngữ chung và định nghĩa cốt lõi của cấu trúc bậc cao đối với các tiêu chuẩn hệ thống quản lý ISO.

3.23 kết quả hoạt động kết quả đo lường được

CHÚ THÍCH 1: Kết quả hoạt động có thể liên quan đến các phát hiện định lượng hoặc định tính.

CHÚ THÍCH 2: Kết quả hoạt động có thể liên quan đến việc quản lý các hoạt động (3.1), quá trình (3.26), sản phẩm (bao gồm cả dịch vụ), hệ thống hoặc tổ chức (3.21).

CHÚ THÍCH 3: Điều này tạo thành một trong những thuật ngữ chung và định nghĩa cốt lõi của cấu trúc bậc cao đối với các tiêu chuẩn hệ thống quản lý ISO,

3.24 chính sách ý định và định hướng của một tổ chức (3.21), được chính thức thể hiện bởi lãnh đạo cao nhất của nó (3.31)

CHÚ THÍCH 1: Điều này tạo thành một trong những thuật ngữ chung và định nghĩa cốt lõi của cấu trúc bậc cao đối với các tiêu chuẩn hệ thống quản lý ISO.

3.25 hoạt động ưu tiên hoạt động (3.1) được đưa ra khẩn cấp để tránh các tác động không thể chấp nhận được (3.13) đối với hoạt động kinh doanh trong thời gian gián đoạn (3.10)

[NGUỒN: ISO 22300: 2018, 3.176, được sửa đổi - Định nghĩa đã được thay thế và Chú thích 1 của mục nhập đã bị xóa.]

3.26 quá trình Tập hợp các hoạt động có liên quan hoặc tương tác với nhau (3.1) biến đầu vào thành đầu ra

CHÚ THÍCH 1: Điều này tạo thành một trong những thuật ngữ chung và định nghĩa cốt lõi của cấu trúc bậc cao đối với các tiêu chuẩn hệ thống quản lý ISO.

3.27 sản phẩm và dịch vụ đầu ra hoặc kết quả do một tổ chức cung cấp (3.21) cho các bên quan tâm (3.15)

VÍ DỤ: Các mặt hàng đã sản xuất, bảo hiểm xe hơi, điều dưỡng cộng đồng.

[NGUỒN: ISO 22300: 2018, 3.181, được sửa đổi - Thuật ngữ "sản phẩm và dịch vụ" đã thay thế "sản phẩm hoặc dịch vụ"; và định nghĩa đã được thay thế.]

3.28 Yêu cầu nhu cầu hoặc mong đợi được công bố, ngầm hiểu chung hoặc bắt buộc

CHÚ THÍCH 1: "Ngầm hiểu chung" có nghĩa là thông lệ hoặc tập quán đối với tổ chức (3.21) và các bên quan tâm (3.15) đều ngụ ý nhu cầu hoặc mong đợi đang được xem xét.

CHÚ THÍCH 2: Yêu cầu cụ thể là yêu cầu được nêu rõ, ví dụ: trong thông tin dạng văn bản (3.11).

CHÚ THÍCH 3: Điều này tạo thành một trong những thuật ngữ chung và định nghĩa cốt lõi của cấu trúc bậc cao đối với các tiêu chuẩn hệ thống quản lý ISO,

3.29 Nguồn lực tất cả tài sản (bao gồm cả nhà máy và thiết bị), con người, kỹ năng, công nghệ, cơ sở vật chất và nguồn cung cấp và thông tin (cho dù là điện tử hay không) mà một tổ chức (3.21) phải có sẵn để sử dụng, khi cần, để vận hành và đáp ứng mục tiêu (3.20) [NGUỒN: ISO 22300: 2018, 3.193, được sửa đổi - Định nghĩa đã được thay thế.]

3.30 Rủi ro tác động của sự không chắc chắn đối với các mục tiêu (3.20)

CHÚ THÍCH 1: Tác động là độ lệch so với dự kiến - tích cực hoặc tiêu cực.

CHÚ THÍCH 2: Sự không chắc chắn là trạng thái, thậm chí một phần, thiếu hụt thông tin liên quan đến, sự hiểu biết hoặc kiến thức về một sự kiện, hệ quả của nó hoặc khả năng xảy ra.

CHÚ THÍCH 3: Rủi ro thường được đặc trưng bởi sự tham chiếu đến các "sự kiện" tiềm ẩn (như được định nghĩa trong ISO Guide 73) và "hậu quả" (như được định nghĩa trong ISO Guide 73), hoặc sự kết hợp của những điều này.

CHÚ THÍCH 4: Rủi ro thường được thể hiện dưới dạng sự kết hợp giữa hậu quả của một sự kiện (bao gồm cả những thay đổi trong hoàn cảnh) và khả năng xảy ra liên quan (như được định nghĩa trong ISO Guide 73).

CHÚ THÍCH 5: Đây là một trong những thuật ngữ chung và định nghĩa cốt lõi của cấu trúc bậc cao đối với các tiêu chuẩn hệ thống quản lý ISO. Định nghĩa đã được sửa đổi để bổ sung "mục tiêu" để phù hợp với ISO 31000.

3.31 lãnh đạo cao nhất người hoặc nhóm người chỉ đạo và kiểm soát một tổ chức (3.21) ở cấp cao nhất

CHÚ THÍCH 1: Lãnh đạo cao nhất có quyền ủy quyền và cung cấp các nguồn lực (3.29) trong tổ chức.

CHÚ THÍCH 2: Nếu phạm vi của hệ thống quản lý (3.16) chỉ bao gồm một phần của tổ chức, thì lãnh đạo cao nhất đề cập đến những người chỉ đạo và kiểm soát phần đó của tổ chức.

CHÚ THÍCH 3: Đây là một trong những thuật ngữ chung và định nghĩa cốt lõi của cấu trúc bậc cao đối với các tiêu chuẩn hệ thống quản lý ISO.

4 Bối cảnh của tổ chức

4.1 Hiểu tổ chức và bối cảnh của nó

Tổ chức phải xác định các vấn đề bên ngoài và bên trong có liên quan đến mục đích của mình và ảnh hưởng đến khả năng đạt được (các) kết quả dự kiến của BCMS của mình.

CHÚ THÍCH: Những vấn đề này sẽ bị ảnh hưởng bởi các mục tiêu tổng thể của tổ chức, các sản phẩm và dịch vụ của tổ chức cũng như số lượng và loại rủi ro mà tổ chức có thể chấp nhận hoặc không.

4.2 Hiểu nhu cầu và mong đợi của các bên quan tâm

4.2.1 Khái quát

Khi thiết lập BCMS của mình, tổ chức phải xác định:

a) Các bên quan tâm có liên quan đến BCMS;

b) Các yêu cầu liên quan của các bên quan tâm này.

4.2.2 Các yêu cầu pháp lý và quy định

Tổ chức phải:

a) Thực hiện và duy trì một quá trình để xác định, tiếp cận và đánh giá các yêu cầu pháp lý và quy định hiện hành liên quan đến tính liên tục của các sản phẩm và dịch vụ, các hoạt động và nguồn lực của tổ chức;

b) Đảm bảo rằng các yêu cầu pháp lý, quy định và các yêu cầu khác hiện hành này được tính đến khi thực hiện và duy trì BCMS của mình;

c) Ghi lại thông tin này và cập nhật.

4.3. Xác định phạm vi của hệ thống quản lý kinh doanh liên tục

4.3.1 Khái quát

Tổ chức phải xác định ranh giới và khả năng áp dụng của BCMS để thiết lập phạm vi của nó.

Khi xác định phạm vi này, tổ chức phải xem xét:

a) Các vấn đề bên ngoài và bên trong được đề cập trong 4.1;

b) Các yêu cầu nêu trong 4.2;

c) Sứ mệnh, mục tiêu và các nghĩa vụ bên trong và bên ngoài.

Phạm vi phải sẵn có dưới dạng thông tin dạng văn bản.

4.3.2 Phạm vi của hệ thống quản kinh doanh liên tục

Tổ chức phải:

a) Thiết lập các phần của tổ chức được đưa vào BCMS, có tính đến (các) vị trí, quy mô, bản chất và mức độ phức tạp của tổ chức;

b) Xác định các sản phẩm và dịch vụ được đưa vào BCMS.

Khi xác định phạm vi, tổ chức phải lập thành văn bản và giải thích các loại trừ. Chúng sẽ không ảnh hưởng đến khả năng và trách nhiệm của tổ chức trong việc cung cấp tính liên tục của hoạt động kinh doanh, như được xác định bởi phân tích tác động kinh doanh hoặc đánh giá rủi ro và các yêu cầu pháp lý hoặc quy định hiện hành.

4.4 Hệ thống quản lý kinh doanh liên tục
Tổ chức phải thiết lập, thực hiện, duy trì và liên tục cải tiến BCMS, bao gồm các quá trình cần thiết và các tương tác của chúng, phù hợp với các yêu cầu của tiêu chuẩn này.

5 Lãnh đạo

5.1 Vai trò lãnh đạo và cam kết
Lãnh đạo cao nhất phải chứng minh vai trò lãnh đạo và cam kết đối với BCMS bằng cách:

a) Đảm bảo rằng chính sách kinh doanh liên tục và các mục tiêu kinh doanh liên tục được thiết lập và tương thích với định hướng chiến lược của tổ chức;

b) Đảm bảo tích hợp các yêu cầu BCMS vào các quá trình kinh doanh của tổ chức;

c) Đảm bảo rằng các nguồn lực cần thiết cho BCMS luôn sẵn có;

d) truyền đạt tầm quan trọng của kinh doanh liên tục có hiệu quả và sự phù hợp với các yêu cầu BCMS;

e) Đảm bảo rằng BCMS đạt được (các) kết quả dự kiến của nó;

f) Chỉ đạo và hỗ trợ những người đóng góp vào tính hiệu lực của BCMS;

g) Thúc đẩy cải tiến liên tục;

h) Hỗ trợ các vai trò quản lý có liên quan khác để thể hiện khả năng lãnh đạo và cam kết của họ khi nó được áp dụng cho các lĩnh vực trách nhiệm của họ.

CHÚ THÍCH: Tham chiếu đến “kinh doanh” trong tiêu chuẩn này có thể được hiểu theo nghĩa rộng có nghĩa là những hoạt động cốt lõi cho mục đích tồn tại của tổ chức.

5.2 Chính sách
5.2.1 Thiết lập chính sách kinh doanh liên tục
Lãnh đạo cao nhất phải thiết lập một chính sách kinh doanh liên tục:

a) Phù hợp với mục đích của tổ chức;

b) Cung cấp một khuôn khổ để thiết lập các mục tiêu liên tục của hoạt động kinh doanh;

c) Bao gồm cam kết đáp ứng các yêu cầu hiện hành;

d) Bao gồm cam kết cải tiến liên tục BCMS.

5.2.2 Truyền đạt chính sách liên tục của doanh nghiệp
Chính sách liên tục kinh doanh phải:

a) Sẵn có dưới dạng thông tin dạng văn bản;

b) Được thông tin trong tổ chức;

c) Sẵn sàng cung cấp cho các bên quan tâm, nếu thích hợp.

5.3 Vai trò, trách nhiệm và quyền hạn
Lãnh đạo cao nhất phải đảm bảo rằng các trách nhiệm và quyền hạn đối với các vai trò liên quan được phân công và truyền đạt trong tổ chức.

Lãnh đạo cao nhất phải giao trách nhiệm và quyền hạn:

a) Đảm bảo rằng BCMS phù hợp với các yêu cầu của tiêu chuẩn này;

b) Báo cáo về kết quả hoạt động của BCMS cho lãnh đạo cao nhất.

6 Hoạch định

6.1 Các hành động giải quyết rủi ro & cơ hội

6.1.1 Xác định rủi ro & cơ hội
Khi hoạch định BCMS, tổ chức phải xem xét các vấn đề được đề cập trong 4.1 và các yêu cầu đề cập trong 4.2 và xác định các rủi ro và cơ hội cần được giải quyết:

a) Đảm bảo rằng BCMS có thể đạt được (các) kết quả dự kiến của nó;

b) Ngăn ngừa, hoặc giảm thiểu các tác động không mong muốn;

c) Đạt được sự cải tiến liên tục.

6.1.2 Giải quyết rủi ro & cơ hội
Tổ chức phải lập kế hoạch:

a) Các hành động để giải quyết những rủi ro và cơ hội này;

b) Làm thế nào để:

1) Tích hợp và thực hiện các hành động vào các quá trình BCMS của nó (xem 8.1);

2) Đánh giá hiệu lực của các hành động này (xem 9.1).

CHÚ THÍCH: Rủi ro và cơ hội liên quan đến hiệu lực của hệ thống quản lý. Các rủi ro liên quan đến gián đoạn hoạt động kinh doanh được đề cập trong 8.2.

6.2 Mục tiêu kinh doanh liên tục và hoạch định để đạt được chúng

6.2.1 Thiết lập các mục tiêu kinh doanh liên tục
Tổ chức phải thiết lập các mục tiêu kinh doanh liên tục ở các chức năng và cấp độ liên quan.

Các mục tiêu kinh doanh liên tục phải:

a) Phù hợp với chính sách kinh doanh liên tục;

b) Có thể đo lường được (nếu có thể thực hiện được);

c) Tính đến các yêu cầu áp dụng (xem 4.1 và 4.2);

d) Được theo dõi;

e) Được truyền đạt;

f) Được cập nhật khi thích hợp.

Tổ chức phải lưu giữ thông tin dạng văn bản về các mục tiêu kinh doanh liên tục.

6.2.2 Hoạch định để đạt được mục tiêu kinh doanh liên tục
Khi hoạch định cách thức để đạt được các mục tiêu kinh doanh liên tục, tổ chức phải xác định:

a) Những gì sẽ được thực hiện;

b) Những nguồn lực nào sẽ được yêu cầu;

c) Ai sẽ chịu trách nhiệm;

d) Khi nào nó sẽ được hoàn thành;

e) Kết quả sẽ được đánh giá như thế nào.

6.3 Lập kế hoạch thay đổi hệ thống quản lý tính liên tục của doanh nghiệp
Khi tổ chức xác định nhu cầu thay đổi đối với BCMS, bao gồm cả những thay đổi được xác định trong Điều khoản 10, các thay đổi phải được thực hiện theo cách thức có kế hoạch.

Tổ chức phải xem xét:

a) Mục đích của những thay đổi và hậu quả tiềm ẩn của chúng;

b) Tính nhất quán của BCMS;

c) Sự sẵn có của các nguồn lực;

d) Sự phân bổ hoặc phân bổ lại trách nhiệm và quyền hạn.

7 Hỗ trợ

7.1 Các nguồn lực
Tổ chức phải xác định và cung cấp các nguồn lực cần thiết cho việc thiết lập, thực hiện, duy trì và cải tiến liên tục BCMS.

7.2 Năng lực
Tổ chức phải:

a) xác định năng lực cần thiết của (những) người đang thực hiện công việc dưới sự kiểm soát của mình mà ảnh hưởng đến hoạt động kinh doanh liên tục của tổ chức;

b) đảm bảo rằng những người này có đủ năng lực trên cơ sở được giáo dục, đào tạo hoặc kinh nghiệm thích hợp;

c) nếu có thể, thực hiện các hành động để đạt được năng lực cần thiết và đánh giá hiệu lực của các hành động đã thực hiện;

d) lưu giữ thông tin dạng văn bản thích hợp làm bằng chứng về năng lực.

CHÚ THÍCH: Các hành động có thể áp dụng có thể bao gồm, ví dụ, cung cấp đào tạo, cố vấn hoặc phân công lại những người hiện đang được tuyển dụng; hoặc việc thuê hoặc ký hợp đồng của những người có năng lực.

7.3 Nhận thức

Những người làm công việc dưới sự kiểm soát của tổ chức phải nhận thức được:

a) chính sách kinh doanh liên tục;

b) đóng góp của họ vào hiệu lực của BCMS, bao gồm cả những lợi ích của việc cải thiện hoạt động kinh doanh liên tục;

c) các tác động của việc không tuân thủ các yêu cầu BCMS;

d) vai trò và trách nhiệm của chính họ trước, trong và sau khi gián đoạn.

7.4 Trao đổi thông tin

Tổ chức phải xác định các thông tin liên lạc nội bộ và bên ngoài liên quan đến BCMS, bao gồm:

a) trao đổi thông tin về cái gì;

b) trao đổi thông tin khí nào;

c) trao đổi thông tin với ai;

d) trao đổi thông tin như thế nào;

e) ai sẽ thực hiện trao đổi thông tin.

7.5 Thông tin được lập thành văn bản

7.5.1 Khái quát

BCMS của tổ chức phải bao gồm:

a) thông tin dạng văn bản được yêu cầu bởi tiêu chuẩn này;

b) thông tin dạng văn bản được tổ chức xác định là cần thiết cho hiệu lực của BCMS.

CHÚ THÍCH: Mức độ thông tin dạng văn bản cho một BCMS có thể khác nhau giữa các tổ chức này do:

- quy mô của tổ chức và loại hình hoạt động, quá trình, sản phẩm và dịch vụ và nguồn lực của tổ chức;

- mức độ phức tạp của các quá trình và sự tương tác của chúng;

- năng lực của con người.

7.5.2 Tạo và cập nhật
Khi tạo và cập nhật thông tin dạng văn bản, tổ chức phải đảm bảo:

a) nhận dạng và mô tả (ví dụ: tiêu đề, ngày tháng, tác giả hoặc số tham chiếu);

b) định dạng (ví dụ: ngôn ngữ, phiên bản phần mềm, đồ họa) và phương tiện (ví dụ: giấy, điện tử);

c) xem xét và phê duyệt tính phù hợp và đầy đủ.

7.5.3. Kiểm soát thông tin dạng văn bản
7.5.3.1 Thông tin dạng văn bản được BCMS yêu cầu và tiêu chuẩn này sẽ được kiểm soát để đảm bảo:

a) sẵn có và thích hợp để sử dụng, ở đâu và khi nào cần;

b) nó được bảo vệ đầy đủ (ví dụ như không bị mất tính bí mật, sử dụng không đúng cách hoặc mất tính toàn vẹn).

7.5.3.2 Để kiểm soát thông tin dạng văn bản, tổ chức phải giải quyết các hoạt động sau, nếu có:

a) phân phối, truy cập, truy xuất và sử dụng;

b) lưu trữ và bảo quản, bao gồm bảo quản tính dễ đọc;

c) kiểm soát các thay đổi (ví dụ: kiểm soát phiên bản);

d) lưu giữ và hủy bỏ.

Thông tin dạng văn bản có nguồn gốc bên ngoài được tổ chức xác định là cần thiết cho việc lập kế hoạch và vận hành BCMS phải được xác định, phù hợp và được kiểm soát.

CHÚ THÍCH: Quyền truy cập có thể ngụ ý một quyết định liên quan đến quyền chỉ xem thông tin dạng văn bản, hoặc quyền và quyền hạn để xem và thay đổi thông tin dạng văn bản.

8 Điều hành

8.1 Hoạch định điều hành và kiểm soát
Tổ chức phải lập kế hoạch, thực hiện và kiểm soát các quá trình cần thiết để đáp ứng các yêu cầu và để thực hiện các hành động được xác định trong 6.1, bằng cách:

a) thiết lập các chuẩn mực cho các quá trình;

b) thực hiện kiểm soát các quá trình phù hợp với các chuẩn mực;

c) lưu giữ thông tin dạng văn bản ở mức độ cần thiết để tin tưởng rằng các quá trình đã được thực hiện theo kế hoạch.

Tổ chức phải kiểm soát những thay đổi theo kế hoạch và xem xét hậu quả của những thay đổi ngoài ý muốn, thực hiện hành động để giảm thiểu mọi tác động bất lợi, nếu cần.

Tổ chức phải đảm bảo rằng các quá trình thuê ngoài và chuỗi cung ứng được kiểm soát.

8.2 Phân tích tác động kinh doanh và đánh giá rủi ro

8.2.1 Khái quát

Tổ chức phải:

a) thực hiện và duy trì các quá trình có hệ thống để phân tích tác động kinh doanh và đánh giá rủi ro gián đoạn;

b) xem xét việc phân tích tác động kinh doanh và đánh giá rủi ro trong các khoảng thời gian đã được lên kế hoạch và khi có những thay đổi đáng kể trong tổ chức hoặc bối cảnh mà tổ chức đó hoạt động.

CHÚ THÍCH: Tổ chức xác định thứ tự tiến hành phân tích tác động kinh doanh và đánh giá rủi ro.

8.2.2 Phân tích tác động kinh doanh

Tổ chức phải sử dụng quá trình phân tích các tác động kinh doanh để xác định các yêu cầu và ưu tiên về tính liên tục của hoạt động kinh doanh. Quá trình phải:

a) xác định các loại tác động và tiêu chí liên quan đến bối cảnh của tổ chức;

b) xác định các hoạt động hỗ trợ việc cung cấp các sản phẩm và dịch vụ;

c) sử dụng các loại tác động và tiêu chí để đánh giá các tác động theo thời gian do sự gián đoạn của các hoạt động này;

d) xác định khung thời gian mà trong đó các tác động của việc không tiếp tục hoạt động sẽ trở nên không thể chấp nhận được đối với tổ chức;

CHÚ THÍCH 1 Khung thời gian này có thể được coi là "khoảng thời gian gián đoạn tối đa có thể chấp nhận được (MTPD)".

e) thiết lập các khung thời gian ưu tiên trong khoảng thời gian được xác định tại mục d) để tiếp tục các hoạt động bị gián đoạn với khả năng chấp nhận được tối thiểu nhất định;

CHÚ THÍCH 2: Khung thời gian này có thể được gọi là "mục tiêu thời gian phục hồi (RTO)";

f) sử dụng phân tích này để xác định các hoạt động ưu tiên;

g) xác định nguồn lực nào cần thiết để hỗ trợ các hoạt động ưu tiên;

h) xác định sự phụ thuộc, bao gồm các đối tác và nhà cung cấp, và sự phụ thuộc lẫn nhau của các hoạt động ưu tiên.

8.2.3. Đánh giá rủi ro
Tổ chức phải thực hiện và duy trì quá trình đánh giá rủi ro.

CHÚ THÍCH: Quá trình đánh giá rủi ro được đề cập trong ISO 31000.

Tổ chức phải:

a) xác định các rủi ro gây gián đoạn đối với các hoạt động ưu tiên của tổ chức và các nguồn lực cần thiết của họ;

b) phân tích và đánh giá các rủi ro đã xác định;

c) xác định những rủi ro nào cần được xử lý.

CHÚ THÍCH Rủi ro trong điều khoản này liên quan đến sự gián đoạn các hoạt động kinh doanh. Các rủi ro và cơ hội liên quan đến hiệu lực của hệ thống quản lý được đề cập trong 6.1.

8.3. Các chiến lược và giải pháp kinh doanh liên tục
8.3.1 Khái quát
Dựa trên kết quả đầu ra từ việc phân tích tác động kinh doanh và đánh giá rủi ro, tổ chức phải xác định và lựa chọn các chiến lược kinh doanh liên tục có cân nhắc các lựa chọn trước, trong và sau khi gián đoạn. Các chiến lược kinh doanh liên tục phải bao gồm một hoặc nhiều giải pháp.

8.3.2 Xác định các chiến lược và giải pháp
Việc xác định sẽ dựa trên mức độ mà các chiến lược và giải pháp:

a) đáp ứng các yêu cầu để tiếp tục và phục hồi các hoạt động ưu tiên trong các khung thời gian đã

xác định và khả năng đã thỏa thuận;

b) bảo vệ các hoạt động ưu tiên của tổ chức;

c) giảm khả năng bị gián đoạn;

d) rút ngắn thời gian gián đoạn;

e) hạn chế tác động của sự gián đoạn đối với các sản phẩm và dịch vụ của tổ chức;

f) cung cấp sự sẵn có của các nguồn lực thích hợp.

8.3.3 Lựa chọn các chiến lược và giải pháp
Việc lựa chọn phải dựa trên mức độ mà các chiến lược và giải pháp:

a) đáp ứng các yêu cầu để tiếp tục và phục hồi các hoạt động ưu tiên trong các khung thời gian đã xác định và khả năng đã thỏa thuận;

b) xem xét số lượng và loại rủi ro mà tổ chức có thể chấp nhận hoặc không;

c) xem xét các chi phí và lợi ích liên quan.

8.3.4 Yêu cầu về nguồn lực
Tổ chức phải xác định các yêu cầu về nguồn lực để thực hiện các giải pháp kinh doanh liên tục đã

chọn. Các loại tài nguyên được xem xét sẽ bao gồm, nhưng không giới hạn ở:

a) con người;

b) thông tin và dữ liệu;

c) cơ sở hạ tầng vật chất như tòa nhà, nơi làm việc hoặc các cơ sở khác và các tiện ích liên quan;

d) thiết bị và vật tư tiêu hao;

e) hệ thống công nghệ thông tin và truyền thông (ICT);

f) vận tải và hậu cần;

g) tài chính;

h) các đối tác và nhà cung cấp.

8.3.5 Thực hiện các giải pháp
Tổ chức phải thực hiện và duy trì các giải pháp kinh doanh liên tục đã chọn để chúng có thể được kích hoạt khi cần thiết.

8.4 Các kế hoạch và thủ tục liên tục của doanh nghiệp
8.4.1 Khái quát
Tổ chức phải thực hiện và duy trì một cấu trúc phản ứng để có thể cảnh báo và thông tin kịp thời cho các bên quan tâm có liên quan. Tổ chức phải cung cấp các kế hoạch và thủ tục để quản lý tổ chức trong thời gian gián đoạn. Các kế hoạch và thủ tục phải được sử dụng khi cần thiết để kích hoạt các giải pháp kinh doanh liên tục.

CHÚ THÍCH: Có nhiều loại thủ tục khác nhau bao gồm các kế hoạch kinh doanh liên tục. Tổ chức phải xác định và lập thành văn bản các kế hoạch và thủ tục kinh doanh liên tục dựa trên kết quả đầu ra của các chiến lược và giải pháp đã chọn.

Các thủ tục phải:

a) cụ thể về các bước ngay lập tức phải được thực hiện trong thời gian gián đoạn;

b) linh hoạt để ứng phó với các điều kiện bên trong và bên ngoài thay đổi của sự gián đoạn;

c) tập trung vào tác động của các sự cố có khả năng dẫn đến gián đoạn;

d) có hiệu quả trong việc giảm thiểu tác động thông qua việc thực hiện các giải pháp thích hợp;

e) phân công vai trò và trách nhiệm cho các nhiệm vụ bên trong họ.

8.4.2 Cấu trúc ứng phó
8.4.2.1 Tổ chức phải thực hiện và duy trì một cấu trúc, xác định một hoặc nhiều nhóm chịu trách nhiệm ứng phó với sự gián đoạn.

8.4.2.2 Vai trò và trách nhiệm của mỗi đội và mối quan hệ giữa các đội phải được nêu rõ.

8.4.2.3 Nói chung, các nhóm phải có năng lực:

a) đánh giá bản chất và mức độ của sự gián đoạn và tác động tiềm tàng của nó;

b) đánh giá tác động đối với các ngưỡng được xác định trước để biện minh cho việc bắt đầu phản ứng chính thức;

c) kích hoạt một ứng phó kinh doanh liên tục thích hợp;

d) lập kế hoạch các hành động cần được thực hiện;

e) thiết lập các ưu tiên (sử dụng an toàn tính mạng làm ưu tiên hàng đầu);

f) giám sát các tác động của sự gián đoạn và phản ứng của tổ chức;

g) kích hoạt các giải pháp kinh doanh liên tục;

h) trao đổi với các bên quan tâm có liên quan, các cơ quan chức năng và giới truyền thông.

8.4.2.4 Đối với mỗi đội phải có:

a) nhân sự đã được xác định và những người thay thế họ có trách nhiệm, quyền hạn và năng lực cần thiết để thực hiện vai trò được chỉ định của họ;

b) các thủ tục được lập thành văn bản để hướng dẫn các hành động của họ (xem 8.4.4), bao gồm các thủ tục để kích hoạt, điều hành, điều phối và truyền đạt ứng phó.

8.4.3. Cảnh báo và thông tin liên lạc
8.4.3.1 Tổ chức phải lập thành văn bản và duy trì các thủ tục về:

a) thông tin liên lạc nội bộ và bên ngoài với các bên quan tâm có liên quan, bao gồm cái gì, khi nào, với ai và giao tiếp như thế nào;

CHÚ THÍCH: Tổ chức có thể lập thành văn bản và duy trì các thủ tục về cách thức và trong những trường hợp nào, tổ chức liên lạc với nhân viên và những người liên hệ khẩn cấp của họ.

b) nhận, lập hồ sơ và phản hồi thông tin liên lạc từ các bên quan tâm, bao gồm bất kỳ hệ thống tư vấn rủi ro quốc gia hoặc khu vực nào hoặc hệ thống tương đương;

c) đảm bảo sự sẵn có của các phương tiện liên lạc trong thời gian gián đoạn;

d) hỗ trợ thông tin liên lạc có cấu trúc với những người ứng cứu khẩn cấp;

e) cung cấp chi tiết về phản hồi truyền thông của tổ chức sau một sự cố, bao gồm cả chiến lược truyền thông;

f) ghi lại các chi tiết của sự gián đoạn, các hành động được thực hiện và các quyết định được đưa ra.

8.4.3.2 Nếu có thể, những điều sau đây cũng phải được xem xét và thực hiện:

a) cảnh báo cho các bên quan tâm có khả năng bị ảnh hưởng bởi sự gián đoạn thực tế hoặc sắp xảy ra;

b) đảm bảo sự phối hợp và liên lạc thích hợp giữa nhiều tổ chức ứng phó. Các thủ tục cảnh báo và thông tin liên lạc sẽ được thực hiện như một phần của chương trình thực hành của tổ chức được mô tả trong 8.5.

8.4.4 Kế hoạch kinh doanh liên tục

8.4.4.1 Tổ chức phải lập thành văn bản và duy trì các kế hoạch và thủ tục kinh doanh liên tục. Các kế hoạch kinh doanh liên tục phải cung cấp hướng dẫn và thông tin để hỗ trợ các nhóm ứng phó với sự gián đoạn và hỗ trợ tổ chức đối phó và phục hồi.

8.4.4.2 Nói chung, kế hoạch liên tục kinh doanh phải bao gồm:

a) chi tiết về các hành động mà các nhóm phải thực hiện để:

1) tiếp tục hoặc phục hồi các hoạt động được ưu tiên trong các khung thời gian định trước;

2) giám sát tác động của sự gián đoạn và phản ứng của tổ chức đối với nó;

b) tham chiếu đến (các) ngưỡng được xác định trước và quá trình để kích hoạt phản ứng;

c) các thủ tục để cho phép cung cấp các sản phẩm và dịch vụ với năng lực đã thỏa thuận;

d) các chi tiết để quản lý các hậu quả tức thời của sự gián đoạn có liên quan đến:

1) phúc lợi của các cá nhân;

2) ngăn ngừa việc mất thêm hoặc không có các hoạt động ưu tiên;

3) tác động đến môi trường.

8.4.4.3 Mỗi kế hoạch phải bao gồm:

a) mục đích, phạm vi và mục tiêu;

b) vai trò và trách nhiệm của nhóm sẽ thực hiện kế hoạch;

c) các hành động để thực hiện các giải pháp;

d) hỗ trợ thông tin cần thiết để kích hoạt (bao gồm các tiêu chí kích hoạt), vận hành, phối hợp và truyền đạt các hành động của nhóm;

e) sự phụ thuộc lẫn nhau bên trong và bên ngoài;

f) các yêu cầu về nguồn lực;

g) các yêu cầu báo cáo;

h) quá trình ngừng hoạt động.

Mỗi kế hoạch sẽ có thể sử dụng được và có sẵn tại thời điểm và địa điểm mà nó được yêu cầu.

8.4.5 Khôi phục

Tổ chức phải có các quá trình được lập thành văn bản để khôi phục và quay trở lại các hoạt động kinh doanh từ các biện pháp tạm thời được áp dụng trong và sau khi bị gián đoạn.

8.5 Chương trình diễn tập
Tổ chức phải thực hiện và duy trì một chương trình thực hiện và thử nghiệm để xác nhận theo thời gian tính hiệu lực của các chiến lược và giải pháp kinh doanh liên tục của mình.

Tổ chức phải tiến hành các diễn tập và thử nghiệm:

a) phù hợp với các mục tiêu kinh doanh liên tục;

b) dựa trên các kịch bản thích hợp đã được hoạch định tốt với các mục tiêu và mục tiêu được xác định rõ ràng;

c) phát triển tinh thần đồng đội, năng lực, sự tự tin và kiến thức cho những người có vai trò thực hiện liên quan đến sự gián đoạn;

d) được thực hiện cùng nhau theo thời gian, xác nhận các chiến lược và giải pháp kinh doanh liên tục của mình;

e) đưa ra các báo cáo sau thực hiện chính thức có chứa các kết quả, khuyến nghị và hành động để thực hiện các cải tiến;

f) được xem xét trong bối cảnh thúc đẩy cải tiến liên tục;

g) được thực hiện theo các khoảng thời gian đã định và khi có những thay đổi đáng kể trong tổ chức hoặc bối cảnh tổ chức hoạt động. Tổ chức phải hành động dựa trên kết quả thực hiện và thử nghiệm của mình để thực hiện các thay đổi và cải tiến.

8.6 Đánh giá văn bản và khả năng kinh doanh liên tục
Tổ chức phải:

a) đánh giá tính phù hợp, đầy đủ và hiệu quả của phân tích tác động kinh doanh, đánh giá rủi ro, các chiến lược, giải pháp, kế hoạch và thủ tục;

b) thực hiện đánh giá thông qua xem xét, phân tích, diễn tập, thử nghiệm, báo cáo sau sự cố và đánh giá kết quả hoạt động;

c) tiến hành đánh giá khả năng kinh doanh liên tục của các đối tác và nhà cung cấp có liên quan;

d) đánh giá sự tuân thủ với các yêu cầu pháp lý và quy định hiện hành, các thực hành tốt nhất của ngành, và sự phù hợp với chính sách và mục tiêu liên tục của doanh nghiệp;

e) cập nhật tài liệu và thủ tục một cách kịp thời. Các đánh giá này phải được thực hiện theo các khoảng thời gian đã định, sau khi xảy ra sự cố hoặc kích hoạt, và khi xảy ra các thay đổi quan trọng.

9 Đánh giá kết quả hoạt động

9.1 Theo dõi, đo lường, phân tích và đánh giá
Tổ chức phải xác định:

a) những gì cần được theo dõi và đo lường;

b) các phương pháp theo dõi, đo lường, phân tích và đánh giá, nếu có thể, để đảm bảo kết quả tin cậy;

c) việc giám sát và đo lường sẽ được thực hiện khi nào và bởi ai;

d) Khi nào và bởi ai các kết quả từ việc theo dõi và đo lường sẽ được phân tích và đánh giá.

Tổ chức phải lưu giữ thông tin dạng văn bản thích hợp làm bằng chứng về kết quả.

Tổ chức phải đánh giá việc thực hiện BCMS và hiệu lực của BCMS.

9.2 Đánh giá nội bộ

9.2.1 Khái quát

Tổ chức phải tiến hành đánh giá nội bộ theo các khoảng thời gian đã được lên kế hoạch để cung cấp thông tin về việc liệu BCMS có:

a) phù hợp với:

1) các yêu cầu riêng của tổ chức đối với BCMS của mình;

2) các yêu cầu của tiêu chuẩn này;

b) được thực hiện và duy trì một cách có hiệu lực.

9.2.2 (Các) chương trình đánh giá

Tổ chức phải:

a) lập kế hoạch, thiết lập, thực hiện và duy trì (các) chương trình đánh giá bao gồm tần suất, phương pháp, trách nhiệm, yêu cầu lập kế hoạch và báo cáo, trong đó có xem xét đến tầm quan trọng của các quá trình liên quan và kết quả của các cuộc đánh giá trước đó;

b) xác định các chuẩn mực và phạm vi đánh giá cho mỗi cuộc đánh giá;

c) lựa chọn đánh giá viên và thực hiện đánh giá để đảm bảo tính khách quan và công bằng của quá trình đánh giá;

d) đảm bảo rằng kết quả của các cuộc đánh giá được báo cáo cho các nhà quản lý có liên quan;

e) lưu giữ thông tin dạng văn bản làm bằng chứng về việc thực hiện (các) chương trình đánh giá và kết quả đánh giá;

f) đảm bảo rằng mọi hành động khắc phục cần thiết được thực hiện không chậm trễ để loại bỏ sự không phù hợp đã phát hiện và nguyên nhân của chúng;

g) đảm bảo rằng các hành động đánh giá tiếp theo bao gồm việc xác minh các hành động đã thực hiện và báo cáo kết quả xác minh.

9.3. Xem xét của lãnh đạo

9.3.1 Khái quát

Lãnh đạo cao nhất phải xem xét BCMS của tổ chức, theo các khoảng thời gian đã định, để đảm bảo tính phù hợp, đầy đủ và hiệu lực liên tục của nó.

9.3.2 Đầu vào của xem xét

Việc xem xét của lãnh đạo phải bao gồm việc xem xét:

a) trạng thái của các hành động từ các lần xem xét trước của ban quản lý;

b) những thay đổi về các vấn đề bên ngoài và bên trong có liên quan đến BCMS;

c) thông tin về kết quả hoạt động của BCMS, bao gồm các xu hướng của:

1) sự không phù hợp và các hành động khắc phục;

2) kết quả đánh giá theo dõi và đo lường;

3) kết quả đánh giá;

d) phản hồi từ các bên quan tâm;

e) nhu cầu thay đổi đối với BCMS, bao gồm cả chính sách và mục tiêu;

f) các thủ tục và nguồn lực có thể được sử dụng trong tổ chức để cải thiện kết quả hoạt động và hiệu lực của BCMS;

g) thông tin từ phân tích tác động kinh doanh và đánh giá rủi ro;

h) đầu ra từ việc đánh giá văn bản và khả năng kinh doanh liên tục (xem 8.6);

i) rủi ro hoặc các vấn đề chưa được giải quyết thỏa đáng trong bất kỳ đánh giá rủi ro nào trước đó;

j) các bài học kinh nghiệm và các hành động phát sinh từ những lần suýt xảy ra và gián đoạn;

k) cơ hội cải tiến liên tục.

9.3.3. Đầu ra của xem xét

9.3.3.1 Các đầu ra của việc xem xét của lãnh đạo phải bao gồm các quyết định liên quan đến các cơ hội cải tiến liên tục và bất kỳ nhu cầu thay đổi nào đối với BCMS để cải thiện hiệu quả và hiệu lực của nó, bao gồm các nội dung sau:

a) các thay đổi đối với phạm vi của BCMS;

b) cập nhật phân tích tác động kinh doanh, đánh giá rủi ro, chiến lược và giải pháp kinh doanh liên tục, và kế hoạch kinh doanh liên tục;

c) sửa đổi các thủ tục và kiểm soát để ứng phó với các vấn đề nội bộ hoặc bên ngoài có thể ảnh hưởng đến BCMS;

d) mức độ hiệu quả của các biện pháp kiểm soát sẽ được đo lường như thế nào. 9.3.3.2 Tổ chức phải lưu giữ thông tin dạng văn bản làm bằng chứng về kết quả xem xét của lãnh đạo. Tổ chức phải:

a) thông báo kết quả xem xét của lãnh đạo cho các bên quan tâm có liên quan;

b) thực hiện hành động thích hợp liên quan đến các kết quả đó.

10 Cải tiến

10.1 Sự không phù hợp và hành động khắc phục

10.1.1 Tổ chức phải xác định các cơ hội cải tiến và thực hiện các hành động cần thiết để đạt được các kết quả dự kiến của BCMS của mình.

10.1.2 Khi xảy ra sự không phù hợp, tổ chức phải:

a) phản ứng với sự không phù hợp và nếu có:

1) thực hiện hành động để kiểm soát và khắc phục nó;

2) deal with the consequences;

b) đánh giá nhu cầu hành động để loại bỏ (các) nguyên nhân của sự không phù hợp, để nó không tái diễn hoặc xảy ra ở nơi khác, bằng cách:

1) xem xét sự không phù hợp;

2) xác định nguyên nhân của sự không phù hợp;

3) xác định xem sự không phù hợp tương tự có tồn tại hoặc có thể xảy ra hay không;

c) thực hiện bất kỳ hành động nào cần thiết;

d) xem xét tính hiệu lực của bất kỳ hành động khắc phục nào đã thực hiện;

e) thực hiện các thay đổi đối với BCMS, nếu cần.

Các hành động khắc phục phải phù hợp với các tác động của sự không phù hợp gặp phải.

10.1.3. Tổ chức phải lưu giữ thông tin dạng văn bản làm bằng chứng về:

a) bản chất của sự không phù hợp và bất kỳ hành động tiếp theo nào được thực hiện;

b) kết quả của bất kỳ hành động khắc phục nào.

10.2 Cải tiến liên tục

Tổ chức phải liên tục cải tiến tính phù hợp, đầy đủ và hiệu quả của BCMS, dựa trên các đo lường định tính và định lượng.

Tổ chức phải xem xét các kết quả phân tích và đánh giá, và các kết quả từ việc xem xét của lãnh đạo, để xác định xem liệu có nhu cầu hoặc cơ hội, liên quan đến doanh nghiệp hoặc BCMS, phải được giải quyết như một phần của cải tiến liên tục.

CHÚ THÍCH: Tổ chức có thể sử dụng các quá trình của BCMS, chẳng hạn như lãnh đạo, lập kế hoạch và đánh giá kết quả hoạt động, để đạt được sự cải tiến.

Bibliography

[1] ISO 9001, Quality management systems — Requirements

[2] ISO 14001, Environmental management systems — Requirements with guidance for use

[3] ISO 19011, Guidelines for auditing management systems

[4] ISO/IEC/TS 17021-6, Conformity assessment — Requirements for bodies providing audit and certification of management systems — Part 6: Competence requirements for auditing and certification of business continuity management systems

[5] ISO/IEC 20000-1, Information technology — Service management — Part 1: Service management system requirements

[6] ISO 22313, Societal security — Business continuity management systems — Guidance

[7] ISO 22316, Security and resilience — Organizational resilience — Principles and attributes

[8] ISO/TS 22317, Societal security — Business continuity management systems — Guidelines for business impact analysis (BIA)

[9] ISO/TS 22318, Societal security — Business continuity management systems — Guidelines for supply chain continuity

[10] ISO/TS 22330, Security and resilience — Business continuity management systems — Guidelines for people aspects of business continuity

[11] ISO/TS 22331, Security and resilience — Business continuity management systems — Guidelines for business continuity strategy

[12] ISO/IEC 27001, Information technology — Security techniques — Information security management systems — Requirements

[13] ISO/IEC 27031, Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity

[14] ISO 28000, Specification for security management systems for the supply chain

[15] ISO 31000, Risk management — Guidelines

[16] IEC 31010, Risk management — Risk assessment techniques

[17] ISO Guide 73, Risk management — Vocabulary