TIÊU CHUẨN QUỐC GIA

TCVN ISO 22301:2023
ISO 22301:2019

AN NINH VÀ KHẢ NĂNG THÍCH ỨNG -
HỆ THỐNG QUẢN LÝ KINH DOANH LIÊN TỤC - CÁC YÊU CẦU

SOCIETAL SECURITY - BUSINESS CONTINUITY MANAGEMENT SYSTEMS - REQUIREMENTS

Lời nói đầu

TCVN ISO 22301:2023 thay thế TCVN ISO 22301:2018.

TCVN ISO 22301:2023 hoàn toàn tương đương với ISO 22301:2019.

TCVN ISO 22301:2023 do Ban kỹ thuật tiêu chuẩn quốc gia TCVN/TC 176 *Quản lý chất lượng và đảm bảo chất lượng* biên soạn, Tổng cục Tiêu chuẩn Đo lường Chất lượng đề nghị, Bộ Khoa học và Công nghệ công bố.

Lời giới thiệu

0.1 Khái quát

Tiêu chuẩn này quy định cấu trúc và các yêu cầu đối với việc áp dụng và duy trì hệ thống quản lý kinh doanh liên tục (BCMS) giúp thiết lập tính liên tục trong kinh doanh, thích hợp với mức độ và loại hình tác động mà tổ chức cho phép hoặc không cho phép chấp nhận sau gián đoạn.

Kết quả của việc duy trì BCMS được định hình bởi các yêu cầu pháp lý, luật định của tổ chức, các yêu cầu về tổ chức và ngành công nghiệp, bởi sản phẩm và dịch vụ cung cấp, các quá trình được sử dụng, quy mô và cơ cấu của tổ chức và yêu cầu của các bên quan tâm của tổ chức.

BCMS nhấn mạnh tầm quan trọng của:

- việc hiểu nhu cầu của tổ chức và sự cần thiết đối với việc thiết lập chính sách và mục tiêu quản lý kinh doanh liên tục,

- triển khai và duy trì các quá trình, khả năng và cơ cấu ứng phó để đảm bảo rằng tổ chức sẽ vượt qua các gián đoạn,

- theo dõi và xem xét kết quả thực hiện và hiệu lực của BCMS, và

- cải tiến liên tục dựa trên các biện pháp định tính và định lượng.

BCMS cũng giống như các hệ thống quản lý khác có các thành phần chính sau:

a) chính sách;

b) nhân sự có năng lực với các trách nhiệm xác định;

c) các quá trình quản lý liên quan đến:

1) chính sách,

2) hoạch định,

3) áp dụng và triển khai,

4) đánh giá kết quả thực hiện,

5) xem xét của lãnh đạo, và

6) cải tiến liên tục;

d) thông tin dạng văn bản hỗ trợ cho kiểm soát việc thực hiện và giúp đánh giá kết quả thực hiện.

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

Mục đích của BCMS là chuẩn bị, đưa ra và duy trì các kiểm soát và khả năng quản lý năng lực tổng thể của tổ chức để duy trì hoạt động trong thời gian gián đoạn. Để đạt được điều này, tổ chức:

a) ở góc độ hoạt động kinh doanh:

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

2) tạo lợi thế cạnh tranh;

3) bảo vệ và nâng cao uy tín và sự tin cậy cho tổ chức;

4) xây dựng khả năng thích ứng của tổ chức;

b) ở góc độ tài chính:

1) giảm hứng chịu rủi ro về pháp lý và tài chính;

2) giảm chi phí trực tiếp và gián tiếp do việc gián đoạn;

c) ở góc độ các bên quan tâm

1) bảo vệ sinh mạng, tài sản và môi trường;

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

3) mang lại lòng tin vào khả năng thành công của tổ chức;

d) đối với các quá trình nội bộ của tổ chức:

1) nâng cao khả năng duy trì hiệu lực trong quá trình gián đoạn;

2) chứng tỏ việc kiểm soát chủ động các rủi ro một cách hiệu lực và hiệu quả;

3) giải quyết những điểm yếu trong hoạt động của tổ chức.

0.3 Chu trình Hoạch định - Thực hiện - Kiểm tra - Hành động (PDCA)

Tiêu chuẩn này áp dụng chu trình Hoạch định (thiết lập), Thực hiện (áp dụng và triển khai), Kiểm tra (theo dõi và xem xét), Hành động (duy trì và cải tiến) (PDCA) cho việc áp dụng, duy trì và cải tiến liên tục hiệu lực của BCMS của tổ chức.

Điều này đảm bảo mức độ nhất quán với các tiêu chuẩn khác về hệ thống quản lý như TCVN ISO 9001, TCVN ISO 14001, ISO/IEC 20000-1, TCVN ISO/IEC 27001 và TCVN ISO 28000, từ đó hỗ trợ việc áp dụng và triển khai nhất quán và tích hợp với các hệ thống quản lý khác có liên quan.

Theo chu trình PDCA, các Điều từ 4 đến 10 trong tiêu chuẩn này bao trùm các thành phần dưới đây.

- Điều 4 đưa ra các yêu cầu cần thiết cho việc thiết lập bối cảnh của BCMS áp dụng cho tổ chức cũng như các nhu cầu, yêu cầu và phạm vi.

- Điều 5 nêu các yêu cầu cụ thể đối với vai trò của lãnh đạo cao nhất trong BCMS và cách thức sự lãnh đạo kết nối mong đợi của mình với tổ chức thông qua tuyên bố về chính sách.

- Điều 6 quy định các yêu cầu đối với việc thiết lập các mục tiêu chiến lược và hướng dẫn các nguyên tắc đối với tổng thể BCMS.

- Điều 7 hỗ trợ việc thực hiện BCMS liên quan đến việc thiết lập năng lực và trao đổi thông tin trên cơ sở lặp lại/hoặc khi cần với các bên quan tâm, đồng thời lập thành văn bản, kiểm soát, duy trì và lưu giữ thông tin dạng văn bản cần thiết.

- Điều 8 xác định các nhu cầu đối với kinh doanh liên tục, xác định cách thức giải quyết các nhu cầu này và xây dựng các thủ tục/quy trình để quản lý tổ chức trong thời gian gián đoạn.

- Điều 9 nêu các yêu cầu cần thiết đối với việc đo lường kết quả thực hiện kinh doanh liên tục, sự phù hợp của BCMS với tiêu chuẩn này và thực hiện xem xét của lãnh đạo.

- Điều 10 nhận biết và hành động đối với sự không phù hợp của BCMS và cải tiến liên tục thông qua hành động khắc phục.

0.5 Nội dung của tiêu chuẩn

Tiêu chuẩn này phù hợp với các yêu cầu của ISO về tiêu chuẩn hệ thống quản lý. Những yêu cầu này bao gồm cấu trúc cấp cao, nội dung cốt lõi tương đồng và các thuật ngữ, định nghĩa chung được thiết kế để tạo thuận lợi cho người sử dụng trong việc áp dụng nhiều tiêu chuẩn của ISO về hệ thống quản lý.

Tiêu chuẩn này không bao gồm các yêu cầu cụ thể cho hệ thống quản lý khác, mặc dù các yếu tố thành phần của nó có thể được thống nhất hoặc tích hợp với các yếu tố thành phần này của hệ thống quản lý khác.

Tiêu chuẩn này bao gồm các yêu cầu có thể được tổ chức sử dụng khi áp dụng BCMS và đánh giá sự phù hợp. Một tổ chức mong muốn chứng tỏ sự phù hợp với tiêu chuẩn có thể thực hiện thông qua việc:

- tự xác định và tự công bố; hoặc

- xác nhận về sự phù hợp của bên có sự quan tâm tới tổ chức, ví dụ như khách hàng; hoặc

- xác nhận tự công bố bởi tổ chức bên ngoài; hoặc

- chứng nhận/đăng ký BCMS bởi tổ chức bên ngoài.

Các điều từ 1 đến 3 của tiêu chuẩn đưa ra phạm vi áp dụng, thuật ngữ và định nghĩa áp dụng khi sử dụng tiêu chuẩn. Các điều từ 4 đến 10 bao gồm các yêu cầu được sử dụng để đánh giá sự phù hợp với tiêu chuẩn.

Trong tiêu chuẩn này, các từ:

a) "phải" chỉ một yêu cầu;

b) "cần/nên" chỉ một khuyến nghị;

c) "được phép" chỉ sự cho phép;

d) "có thể" chỉ một khả năng hoặc năng lực.

Thông tin trong phần "Chú thích" là hướng dẫn để hiểu hoặc làm rõ yêu cầu liên quan. "Chú thích" ở Điều 3 cung cấp thông tin bổ sung về dữ liệu thuật ngữ và có thể bao gồm quy định liên quan đến việc sử dụng thuật ngữ.

AN NINH VÀ KHẢ NĂNG THÍCH ỨNG - HỆ THỐNG QUẢN LÝ KINH DOANH LIÊN TỤC - CÁC YÊU CẦU

SOCIETAL SECURITY - BUSINESS CONTINUITY MANAGEMENT SYSTEMS - REQUIREMENTS

1 Phạm vi áp dụng

Tiêu chuẩn này quy định các yêu cầu đối với việc áp dụng, duy trì và cải tiến liên tục hệ thống quản lý nhằm bảo vệ, giảm khả năng xảy ra, chuẩn bị, ứng phó và khôi phục sau gián đoạn khi chúng xảy ra.

Các yêu cầu được quy định trong tiêu chuẩn này mang tính khái quát và nhằm áp dụng cho mọi tổ chức hoặc các phần của tổ chức, không phân biệt loại hình, quy mô và tính chất của tổ chức. Mức độ áp dụng các yêu cầu này phụ thuộc vào môi trường hoạt động và mức độ phức tạp của tổ chức.

Tiêu chuẩn này áp dụng cho tổ chức ở mọi loại hình và quy mô:

a) áp dụng, duy trì và cải tiến BCMS;

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

c) cần có khả năng duy trì việc cung cấp sản phẩm và dịch vụ ở mức năng lực xác định trước có thể chấp nhận được trong thời gian gián đoạn;

d) muốn nâng cao khả năng thích ứng của mình thông qua việc áp dụng có hiệu lực BCMS.

Tiêu chuẩn này có thể được dùng để đánh giá khả năng của tổ chức trong việc đáp ứng nhu cầu và nghĩa vụ về tính liên tục của chính mình.

2 Tài liệu viện dẫn

Các tài liệu viện dẫn dưới đây rất cần thiết cho việc áp dụng tiêu chuẩn này. Đối với các tài liệu ghi năm công bố thì áp dụng bản được nêu. Đối với các tài liệu không ghi năm công bố thì áp dụng bản mới nhất (bao gồm cả các sửa đổi).

TCVN ISO 22300, *An ninh và khả năng thích ứng - Từ vựng*

3 Thuật ngữ và định nghĩa

Tiêu chuẩn này áp dụng các thuật ngữ và định nghĩa trong TCVN ISO 22300 và các thuật ngữ và định nghĩa dưới đây.

3.1

Hoạt động

Tập hợp một hay nhiều nhiệm vụ với đầu ra xác định.

[NGUỒN: TCVN ISO 22300, 3.1.2]

3.2

Đánh giá

Quá trình (3.26) có hệ thống, độc lập và được lập thành văn bản để thu được bằng chứng đánh giá và xem xét đánh giá chúng một cách khách quan để xác định mức độ thực hiện các chuẩn mực đánh giá.

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

CHÚ THÍCH 2: Đánh giá nội bộ do tổ chức (3.21) tự thực hiện, hoặc tổ chức bên ngoài thực hiện với danh nghĩa của tổ chức.

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

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

CHÚ THÍCH 5: Một cuộc đánh giá nội bộ có thể phục vụ xem xét của lãnh đạo và các mục đích nội bộ khác và có thể hình thành cơ sở cho công bố sự phù hợp của tổ chức. Mức độ độ lập có thể được chứng tỏ thông qua việc không chịu trách nhiệm đối với hoạt động (3.1) được đánh giá. Đánh giá bên ngoài bao gồm đánh giá bên thứ hai và bên thứ ba. Đánh giá bên thứ hai được thực hiện bởi các bên quan tâm tới tổ chức, như khách hàng hoặc người khác với danh nghĩa của khách hàng. Đánh giá bên thứ ba được tiến hành bởi tổ chức đánh giá độc lập bên ngoài, như các tổ chức cấp chứng nhận/đăng ký sự phù hợp hoặc cơ quan chính phủ.

CHÚ THÍCH 6: Thuật ngữ này là một trong những thuật ngữ chung và định nghĩa cốt lõi đối với các tiêu chuẩn hệ thống quản lý của ISO theo cấu trúc cấp cao. Định nghĩa gốc đã được sửa đổi với việc bổ sung Chú thích 4 và Chú thích 5.

3.3

Kinh doanh liên tục

Tính liên tục trong kinh doanh

Khả năng của **tổ chức** (3.21) trong việc duy trì cung cấp **sản phẩm và dịch vụ** (3.27) trong khoảng thời gian có thể chấp nhận được, ở mức năng lực đã định trước, trong thời gian gián đoạn (3.10).

[NGUỒN: TCVN ISO 22300, 3.1.19]

3.4

Kế hoạch kinh doanh liên tục

Thông tin dạng văn bản (3.11) hướng dẫn **tổ chức** (3.21) ứng phó với **gián đoạn** (3.10), tiếp tục lại, phục hồi và khôi phục việc cung cấp **sản phẩm và dịch vụ** (3.27) nhất quán với các **mục tiêu** (3.20) **kinh doanh liên tục** (3.3) của tổ chức.

[NGUỒN: TCVN ISO 22300, 3.1.22]

3.5

Phân tích tác động kinh doanh

Quá trình (3.26) phân tích **tác động** (3.13) theo thời gian của việc **gián đoạn** (3.10) tới **tổ chức** (3.21).

CHÚ THÍCH 1: Kết quả đầu ra là một tuyên bố và lý giải về các yêu cầu (3.28) kinh doanh liên tục (3.3).

[NGUỒN: TCVN ISO 22300, 3.1.24]

3.6

Năng lực

Khả năng áp dụng kiến thức và kỹ năng để đạt được kết quả dự kiến.

CHÚ THÍCH 1: Thuật ngữ này là một trong những thuật ngữ chung và định nghĩa cốt lồi đối với các tiêu chuẩn hệ thống quản lý của ISO theo cấu trúc cấp cao.

3.7

Sự phù hợp

Sự đáp ứng một **yêu cầu** (3.28).

CHÚ THÍCH 1: Thuật ngữ này là một trong những thuật ngữ chung và định nghĩa cốt lõi đối với các tiêu chuẩn hệ thống quản lý của ISO theo cấu trúc cấp cao.

3.8

Cải tiến liên tục

Hoạt động (3.1) lặp lại để nâng cao **kết quả thực hiện** (3.23).

CHÚ THÍCH 1: Thuật ngữ này là một trong những thuật ngữ chung và định nghĩa cốt lõi đối với các tiêu chuẩn hệ thống quản lý của ISO theo cấu trúc cấp cao.

3.9

Hành động khắc phục

Hành động nhằm loại bỏ (các) nguyên nhân của **sự không phù hợp** (3.19) và ngăn ngừa việc tái diễn.

CHÚ THÍCH 1: Thuật ngữ này là một trong những thuật ngữ chung và định nghĩa cốt lõi đối với các tiêu chuẩn hệ thống quản lý của ISO theo cấu trúc cấp cao.

3.10

(Sự) gián đoạn

Sự cố (3.14), được dự báo trước hoặc không được dự báo trước, gây ra sai lệch tiêu cực, ngoài kế hoạch trong việc cung cấp theo dự kiến các sản phẩm và dịch vụ (3.27) theo mục tiêu (3.20) của tổ chức (3.21).

[NGUỒN: TCVN ISO 22300, 3.1.75]

3.11

Thông tin dạng văn bản

Thông tin cần được **tổ chức** (3.21) kiểm soát và duy trì và phương tiện chứa đựng thông tin.

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

CHÚ THÍCH 2: Thông tin dạng văn bản có thể đề cập tới:

- **hệ thống quản lý** (3.16), gồm cả các **quá trình** (3.26) liên quan;

- thông tin được tạo ra cho việc vận hành của tổ chức (hệ thống tài liệu);

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

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

3.12

Hiệu lực

Mức độ theo đó các **hoạt động** (3.1) đã hoạch định được thực hiện và đạt được các kết quả theo hoạch định.

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

3.13

Tác động

Hậu quả của việc **gián đoạn** (3.10) ảnh hưởng đến **mục tiêu** (3.20).

[NGUỒN: TCVN ISO 22300, 3.1.118]

3.14

Sự cố

Sự kiện có thể là, hoặc có thể dẫn đến sự **gián đoạn** (3.10), tổn thất, trường hợp khẩn cấp hoặc khủng hoảng.

[NGUỒN: TCVN ISO 22300, 3.1.122]

3.15

Bên quan tâm (thuật ngữ được ưu tiên)

Bên liên quan (thuật ngữ thay thế)

Cá nhân hoặc tổ chức (3.21) có thể ảnh hưởng, chịu ảnh hưởng hoặc cảm thấy bị ảnh hưởng bởi một quyết định hay hoạt động (3.1).

VÍ DỤ: Khách hàng, chủ sở hữu, nhân sự của tổ chức, nhà cung cấp, ngân hàng, cơ quan quản lý, liên minh, đối tác hoặc xã hội, có thể bao gồm cả đối thủ cạnh tranh hoặc các nhóm đối lập gây áp lực.

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

CHÚ THÍCH 2: Cộng đồng chịu ảnh hưởng và dân cư địa phương có thể được coi là các bên quan tâm.

CHÚ THÍCH 3: Đây là một trong những thuật ngữ chung và định nghĩa cốt lõi cho các tiêu chuẩn về hệ thống quản lý theo cấu trúc cấp cao của ISO. Định nghĩa gốc đã được sửa đổi thông qua việc bổ sung thêm ví dụ và chú thích 1 và 2.

3.16

Hệ thống quản lý

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

CHÚ THÍCH 1: Một hệ thống quản lý có thể giải quyết một hay nhiều lĩnh vực.

CHÚ THÍCH 2: Các yếu tố của hệ thống bao gồm cơ cấu tổ chức, vai trò và trách nhiệm, việc hoạch định, thực hiện.

CHÚ THÍCH 3: Phạm vi của hệ thống quản lý có thể bao gồm toàn bộ tổ chức, các chức năng cụ thể được nhận biết trong tổ chức, các bộ phận cụ thể được nhận biết của tổ chức, hoặc một hay nhiều chức năng xuyên suốt một nhóm của tổ chức.

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

3.17

Đo lường

Quá trình (3.26) xác định một giá trị.

CHÚ THÍCH 1: Đây là một trong những thuật ngữ chung và định nghĩa cốt lõi cho các tiêu chuẩn về hệ thống quản lý theo cấu trúc cấp cao của ISO.

3.18

Theo dõi

Xác định tình trạng của hệ thống, **quá trình** (3.26) hay **hoạt động** (3.1).

CHÚ THÍCH 1: Để xác định tình trạng có thể cần kiểm tra, giám sát hay quan trắc chặt chẽ.

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

3.19

Sự không phù hợp

Việc không đáp ứng một **yêu cầu** (3.28).

CHÚ THÍCH 1: Đây là một trong những thuật ngữ chung và định nghĩa cốt lõi cho các tiêu chuẩn về hệ thống quản lý theo cấu trúc cấp cao của ISO.

3.20

Mục tiêu

Kết quả cần đạt được.

CHÚ THÍCH 1: Mục tiêu có thể mang tính chiến lược, chiến thuật hoặc tác nghiệp.

CHÚ THÍCH 2: Các mục tiêu có thể liên quan đến các lĩnh vực khác nhau (như mục tiêu về tài chính, sức khỏe và an toàn, môi trường,...) và có thể áp dụng ở các cáp khác nhau (như chiến lược, toàn bộ tổ chức, dự án, sản phẩm hay quá trình (3.26)).

CHÚ THÍCH 3: Mục tiêu có thể thể hiện theo những cách khác như kết quả dự kiến, mục đích, chuẩn mực về tác nghiệp, như một mục tiêu về kinh doanh liên tục (3.3) hay sử dụng những từ ngữ khác có ý nghĩa tương tự (ví dụ mục đích, mục tiêu hướng tới, hay chỉ tiêu).

CHÚ THÍCH 4: Trong bối cảnh hệ thống quản lý kinh doanh liên tục, các mục tiêu kinh doanh liên tục

được tổ chức (3.21) lập ra, nhất quán với chính sách (3.24) kinh doanh liên tục, nhằm đạt được các kết quả cụ thể.

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

3.21

Tổ chức

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

CHÚ THÍCH 1: Khái niệm tổ chức bao gồm, nhưng không giới hạn ở, thương nhân độc quyền, công ty, tập đoàn, hãng, xí nghiệp, cơ quan quản lý, câu lạc bộ, hiệp hội, hội từ thiện hay viện, hay một phần hoặc sự kết hợp của những loại hình trên dù có được hợp nhất hay không và là tổ chức công hay tư.

CHÚ THÍCH 2: Với tổ chức có nhiều hơn một đơn vị vận hành, một đơn vị vận hành riêng lẻ có thể được coi là một tổ chức.

CHÚ THÍCH 3: Đây là một trong những thuật ngữ chung và định nghĩa cốt lõi cho các tiêu chuẩn về hệ thống quản lý theo cấu trúc cấp cao của ISO. Định nghĩa gốc đã được sửa đổi bằng cách bổ sung Chú thích 2.

3.22

Thuê ngoài

Thực hiện sự sắp đặt trong đó một tổ chức (3.21) bên ngoài thực hiện một phần chức năng hoặc quá trình (3.26) của tổ chức.

CHÚ THÍCH 1: Một tổ chức bên ngoài nằm ngoài phạm vi của hệ thống quản lý (3.16), mặc dù chức năng hoặc quá trình được thuê ngoài lại thuộc phạm vi của hệ thống quản lý.

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

3.23

Kết quả thực hiện

Kết quả có thể đo được.

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

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

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

3.24

Chính sách

Ý đồ và định hướng của **tổ chức** (3.21) được **lãnh đạo cao nhất** (3.31) của tổ chức công bố một cách chính thức.

CHÚ THÍCH 1: Đây là một trong những thuật ngữ chung và định nghĩa cốt lõi cho các tiêu chuẩn về hệ thống quản lý theo cấu trúc cấp cao của ISO.

3.25

Hoạt động ưu tiên

Hoạt động (3.1) được đưa ra mức độ khẩn cấp để tránh những **tác động** (3.13) không thể chấp nhận được đối với hoạt động kinh doanh trong thời gian **gián đoạn** (3.10).

[NGUỒN: TCVN ISO 22300, 3.1.186]

3.26

Quá trình

Tập hợp các **hoạt động** (3.1) có liên quan hoặc tương tác lẫn nhau để chuyển đầu vào thành đầu ra.

CHÚ THÍCH 1: Đây là một trong những thuật ngữ chung và định nghĩa cốt lõi cho các tiêu chuẩn về

hệ thống quản lý theo cấu trúc cấp cao của ISO.

3.27

Sản phẩm và dịch vụ

Đầu ra hoặc kết quả đầu ra được **tổ chức** (3.21) cung cấp cho các **bên quan tâm** (3.15)

VÍ DỤ: Các mặt hàng được sản xuất, bảo hiểm ô tô, chăm sóc y tế cộng đồng.

[NGUỒN: TCVN ISO 22300, 3.1.191]

3.28

Yêu cầu

Nhu cầu hoặc mong đợi được tuyên bố, ngầm hiểu chung hoặc bắt buộc.

CHÚ THÍCH 1: "Ngầm hiểu chung" nghĩa là đối với tổ chức (3.21) và các bên quan tâm (3.15) nhu cầu hoặc mong đợi được coi là ngầm hiểu mang tính thông lệ hoặc thực hành chung.

CHÚ THÍCH 2: Yêu cầu được quy định là yêu cầu đã được công bố, ví dụ trong **thông tin dạng văn bản** (3.11).

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

3.29

Nguồn lực

Toàn bộ tài sản (bao gồm cả nhà máy và thiết bị), con người, kỹ năng, công nghệ, nhà xưởng, vật tư cung ứng và thông tin (dạng điện tử hoặc không phải điện tử) mà tổ chức (3.21) phải sẵn có để sử dụng khi cần cho hoạt động và đạt được các mục tiêu (3.20) của mình.

[NGUỒN: TCVN ISO 22300, 3.1.207]

3.30

Rủi ro

Ảnh hưởng của sự không chắc chắn tới **mục tiêu** (3.20).

CHÚ THÍCH 1: Ảnh hưởng là một sai lệch so với dự kiến - tích cực hoặc tiêu cực.

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

CHÚ THÍCH 3: Rủi ro thường đặc trưng bởi sự dẫn chiếu đến các "sự kiện" (được định nghĩa trong TCVN 9788) và "hệ quả" (được định nghĩa trong TCVN 9788) tiềm ẩn, hoặc sự kết hợp giữa chúng.

CHÚ THÍCH 4: Rủi ro thường thể hiện theo cách kết hợp các hệ quả của một sự kiện (bao gồm cả những thay đổi về hoàn cảnh) và khả năng xảy ra (được định nghĩa trong TCVN 9788) kèm theo.

CHÚ THÍCH 5: Đấy là một trong những thuật ngữ chung và định nghĩa cốt lõi cho các tiêu chuẩn về hệ thống quản lý theo cấu trúc cấp cao của ISO. Định nghĩa này được sửa đổi bằng việc bổ sung từ "tới mục tiêu" để thống nhất với TCVN ISO 31000.

3.53

Lãnh đạo cao nhất

Người hoặc nhóm người định hướng và kiểm soát **tổ chức** (3.21) ở cấp cao nhất.

CHÚ THÍCH 1: Lãnh đạo cao nhất có quyền ủy quyền và cung cấp nguồn lực (3.29) trong phạm vi 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 chỉ những người định hướng và kiểm soát phần đó của tổ chức.

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

4 Bối cảnh của tổ chức

4.1 Hiểu tổ chức và bối cảnh của tổ chức

Tổ chức phải xác định các vấn đề bên ngoài và nội bộ liên quan đến mục đích của mình và ảnh hưởng đến khả năng của tổ chức trong việc đạt được (các) kết quả dự kiến của hệ thống quản lý kinh

doanh liên tục (BCMS) của tổ chức.

CHÚ THÍCH: Những vấn đề này sẽ chịu ảnh hưởng bởi mục tiêu tổng thể của tổ chức, sản phẩm và dịch vụ của tổ chức và mức độ và loại hình rủi ro mà tổ chức cho phép hoặc không cho phép gánh chịu.

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

4.2.1 Khái quát

Khi thiết lập BCMS, tổ chức phải xác định:

a) các bên quan tâm có liên quan tới BCMS;

b) yêu cầu có liên quan của các bên quan tâm đó.

4.2.2 Yêu cầu pháp lý và chế định

Tổ chức phải:

a) áp dụng và duy trì quá trình nhận biết, tiếp cận và đánh giá các yêu cầu pháp lý và chế định hiện hành liên quan đến tính liên tục của sản phẩm và dịch vụ, các hoạt động và nguồn lực của tổ chức;

b) đảm bảo rằng các yêu cầu pháp lý, chế định hiện hành và các yêu cầu khác được tính đến khi áp dụng và duy trì BCMS;

c) lập thành văn bản và cập nhật thông tin này.

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 hệ thống.

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

a) các vấn đề bên ngoài và nội bộ đề cập ở 4.1;

b) các yêu cầu đề cập ở 4.2;

c) sứ mệnh, mục đích và các nghĩa vụ nội bộ và bên ngoài của tổ chức.

Phạm vi này phải sẵn có bằng thông tin dạng văn bản.

4.3.2 Phạm vi của hệ thống quản lý kinh doanh liên tục

Tổ chức phải:

a) thiết lập các phần của tổ chức thuộc BCMS, có tính đến (các) địa điểm, quy mô, đặc điểm và mức độ phức tạp của tổ chức;

b) nhận biết sản phẩm và dịch vụ đưa vào phạm vi của BCMS.

Khi xác định phạm vi này, tổ chức phải lập thành văn bản và giải thích các ngoại lệ. Những ngoại lệ này không được ảnh hưởng đến khả năng và trách nhiệm của tổ chức trong việc thực hiện kinh doanh liên tục, được xác định trong phân tích tác động kinh doanh hoặc đánh giá rủi ro và các yêu cầu pháp lý hoặc chế định hiện hành.

4.4 Hệ thống quản lý kinh doanh liên tục

Tổ chức phải thiết lập, thực hiện, duy trì và cải tiến liên tục BCMS, bao gồm các quá trình cần thiết và sự tương tác giữa các quá trình, theo các yêu cầu của tiêu chuẩn này.

5 Sự lãnh đạo

5.1 Sự lãnh đạo và cam kết

Lãnh đạo cao nhất phải chứng tỏ sự lãnh đạo và cam kết đối với BCMS thông qua việc:

a) đảm bảo rằng chính sách kinh doanh liên tục và 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 của BCMS vào các quá trình hoạt động chủ chốt của tổ chức;

c) đảm bảo sẵn có các nguồn lực cần thiết cho BCMS;

d) trao đổi thông tin về tầm quan trọng của kinh doanh liên tục có hiệu lực và của sự phù hợp với các yêu cầu của BCMS;

e) đảm bảo BCMS đạt được (các) kết quả dự kiến;

f) định hướng và hỗ trợ mọi người cùng đóng góp cho hiệu lực của BCMS;

g) thúc đẩy cải tiến liên tục;

h) hỗ trợ các vị trí quản lý liên quan khác chứng tỏ sự lãnh đạo và cam kết của họ ở các khu vực họ chịu trách nhiệm.

CHÚ THÍCH: Từ "hoạt động chủ chốt" được đề cập trong tiêu chuẩn này có thể được diễn giải theo nghĩa rộng gồm các hoạt động cốt lõi đối với 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 chính sách kinh doanh liên tục:

a) thích hợp với mục đích của tổ chức;

b) đưa ra khuôn khổ cho việc thiết lập các mục tiêu kinh doanh liên tục;

c) bao gồm việc cam kết thỏa mãn các yêu cầu được áp dụng;

d) bao gồm việc cam kết cải tiến liên tục BCMS.

5.2.2 Trao đổi thông tin về chính sách kinh doanh liên tục

Chính sách kinh doanh liên tục phải:

a) sẵn có bằng thông tin dạng văn bản;

b) được truyền đạt trong tổ chức;

c) sẵn có cho các bên quan tâm liên quan, khi thích hợp.

5.3 Vai trò, trách nhiệm và quyền hạn

Lãnh đạo cao nhất phải đảm bảo rằng trách nhiệm và quyền hạn của các vị trí thích hợp được phân công và truyền đạt trong tổ chức.

Lãnh đạo cao nhất phải phân công trách nhiệm và quyền hạn:

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

b) báo cáo về kết quả thực hiện BCMS cho lãnh đạo cao nhất.

6 Hoạch định

6.1 Hành động giải quyết rủi ro và cơ hội

6.1.1 Xác định rủi ro và cơ hội

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

a) mang lại sự đảm bảo rằng BCMS có thể đạt được (các) kết quả dự kiến;

b) ngăn ngừa hoặc giảm bớt những tác động không mong muốn;

c) đạt được cải tiến liên tục.

6.1.2 Giải quyết rủi ro và cơ hội

Tổ chức phải hoạch định:

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

b) cách thức để:

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

2) xem xét đánh giá hiệu lực của những hành động này (xem 9.1).

CHÚ THÍCH: Rủi ro và cơ hội liên quan đến hiệu lực của hệ thống quản lý. Việc xử lý rủi ro liên quan đến việc gián đoạn hoạt động được đề cập ở 8.2.

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

6.2.1 Thiết lập mục tiêu kinh doanh liên tục

Tổ chức phải thiết lập mục tiêu kinh doanh liên tục ở các cấp và bộ phận chức năng thích hợp.

Mục tiêu kinh doanh liên tục phải:

a) nhất quán với chính sách kinh doanh liên tục;

b) đo được (khi có thể);

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

d) được theo dõi;

e) được trao đổi thông tin;

f) được cập nhật khi thích hợp.

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

6.2.2 Xác định mục tiêu kinh doanh liên tục

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

a) việc gì sẽ thực hiện;

b) nguồn lực nào là cần thiết;

c) ai là người chịu trách nhiệm;

d) khi nào sẽ hoàn thành;

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

6.3 Hoạch định các thay đổi đối với BCMS

Khi tổ chức xác định nhu cầu thay đổi đối với BCMS, bao gồm cả các thay đổi được nhận biết ở Điều 10, thì những thay đổi này phải được thực hiện theo cách thức đã hoạch định.

Tổ chức phải xem xét:

a) mục đích của những thay đổi và hệ quả tiềm ẩn của chúng;

b) tính toàn vẹn của BCMS;

c) sự sẵn có các nguồn lực;

d) việc phân công và phân công lại trách nhiệm và quyền hạn.

7 Hỗ trợ

7.1 Nguồn lực

Tổ chức phải xác định và cung cấp nguồn lực cần thiết cho việc thiết lập, áp dụng, 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 thực hiện công việc dưới sự kiểm soát của tổ chức có ảnh hưởng tới kết quả thực hiện kinh doanh liên tục của tổ chức;

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

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

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

CHÚ THÍCH: Hành động thích hợp có thể bao gồm, ví dụ cung cấp đào tạo, kèm cặp hoặc phân công lại nhân sự đang được sử dụng; hay thuê hoặc ký hợp đồng với nhân sự có năng lực.

7.3 Nhận thức

Người thực hiện công việc dưới sự kiểm soát của tổ chức phải nhận thức được về:

a) chính sách kinh doanh liên tục;

b) đóng góp của họ cho hiệu lực của BCMS, bao gồm cả lợi ích của kết quả thực hiện kinh doanh liên tục được cải tiến;

c) hậu quả của việc không tuân thủ các yêu cầu của BCMS;

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

7.4 Trao đổi thông tin

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

a) trao đổi thông tin gì;

b) trao đổi thông tin khi nào;

c) trao đổi thông tin với ai;

d) trao đổi thông tin như thế nào;

e) người thực hiện trao đổi thông tin.

7.5 Thông tin dạng văn bản

7.5.1 Khái quát

BCMS của tổ chức phải bao gồm:

a) thông tin dạng văn bản theo yêu cầu của tiêu chuẩn này;

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

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

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

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

- năng lực của nhân sự.

7.5.2 Tạo lập và cập nhật

Khi tạo lập và cập nhật thông tin dạng văn bản, tổ chức phải đảm bảo sự thích hợp của:

a) việc nhận biết và mô tả (ví dụ tiêu đề, thời gian, tác giả hoặc số tham chiếu);

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

c) việc xem xét và phê duyệt sự phù hợp và thỏa đáng.

7.5.3 Kiểm soát thông tin dạng văn bản

7.5.3.1 Thông tin dạng văn bản theo theo yêu cầu của BCMS và của tiêu chuẩn này phải được kiểm soát nhằm đảm bảo:

a) sẵn có và phù hợp để sử dụng tại nơi và khi cần;

b) được bảo vệ một cách thỏa đáng (ví dụ tránh mất tính bảo mật, sử dụng sai mục đích 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, khi có thể áp dụng được:

a) phân phối, tiếp cận, khôi phục và sử dụng;

b) lưu trữ và bảo quản, bao gồm cả giữ gìn để có thể đọc được;

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 hoạch định và thực hiện BCMS phải được nhận biết khi thích hợp và được kiểm soát.

CHÚ THÍCH: Tiếp cận hàm ý một quyết định về việc chỉ cho phép xem thông tin dạng văn bản hoặc cho phép và giao quyền xem và thay đổi thông tin dạng văn bản.

8 Thực hiện

8.1 Hoạch định và kiểm soát việc thực hiện

Tổ chức phải hoạch định, 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 ở 6.1, thông qua việc:

a) thiết lập tiêu chí đối với các quá trình,

b) thực hiện kiểm soát các quá trình theo các tiêu chí này;

c) duy trì và lưu giữ thông tin dạng văn bản ở mức độ cần thiết để có sự tin tưởng rằng các quá trình

được thực hiện như đã hoạch định.

Tổ chức phải kiểm soát những thay đổi theo hoạch định và xem xét các hệ quả của những thay đổi ngoài dự kiến, thực hiện hành động để giảm nhẹ mọi tác động bất lợi khi cần.

Tổ chức phải đảm bảo rằng các quá trình thuê ngoài và chuỗi cung ứng đều 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 của việc gián đoạn;

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

CHÚ THÍCH: Tổ chức xác định trình tự theo đó việc phân tích tác động kinh doanh và đánh giá rủi ro được tiến hành.

8.2.2 Phân tích tác động kinh doanh

Tổ chức phải sử dụng quá trình cho việc phân tích tác động kinh doanh để xác định thứ tự ưu tiên và các yêu cầu kinh doanh liên tục. Quá trình này phải:

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

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

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

d) nhận biết khung thời gian (khoảng thời gian) theo đó các tác động của việc không tiếp tục lại hoạt động có thể trở nên không thể chấp nhận được với tổ chức;

CHÚ THÍCH 1: Khung thời gian này có thể được gọi là “thời gian chịu gián đoạn tối đa (MTPD)”

e) thiết lập các khung thời gian theo thứ tự ưu tiên trong khoảng thời gian nhận biết ở điểm

d) để tiếp tục lại các hoạt động bị gián đoạn ở mức năng lực tối thiểu chấp nhận được đã xác định;

CHÚ THÍCH 2: Khung thời gian này có thể được gọi là “mục tiêu về thời gian phục hồi (RTO)”.

f) sử dụng phân tích này để nhận biết các hoạt động ưu tiên;

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

h) xác định sự phụ thuộc, bao gồm cả các đối tác và nhà cung ứng 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 này được đề cập trong TCVN ISO 31000.

Tổ chức phải:

a) nhận diện rủi ro của việc gián đoạn các hoạt động ưu tiên của tổ chức và các nguồn lực cần thiết cho các hoạt động này;

b) phân tích và định mức rủi ro được nhận diện;

c) xác định rủi ro nào cần xử lý.

CHÚ THÍCH: Rủi ro nêu ở điều này liên quan đến việc gián đoạn hoạt động kinh doanh. Rủi ro và cơ hội liên quan đến hiệu lực của hệ thống quản lý được đề cập ở 6.1.

8.3 Chiến lược và giải pháp kinh doanh liên tục

8.3.1 Khái quát

Dựa trên kết quả đầu ra của việc phân tích tác động kinh doanh và đánh giá rủi ro, tổ chức phải nhận biết và lựa chọn chiến lược kinh doanh liên tục và xem xét các phương án cho trước, trong và sau gián đoạn. Chiến lược kinh doanh liên tục phải bao gồm một hay nhiều giải pháp.

8.3.2 Nhận biết chiến lược và giải pháp

Việc nhận biết phải dựa trên mức độ chiến lược và giải pháp:

a) đáp ứng yêu cầu duy trì và phục hồi các hoạt động ưu tiên trong các khung thời gian đã định và năng lực đã thống nhất;

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

c) giảm khả năng xảy ra gián đoạn;

d) rút ngắn thời gian gián đoạn;

e) hạn chế tác động của việc gián đoạn tới sản phẩm và dịch vụ của tổ chức;

f) đảm bảo sẵn có các nguồn lực thỏa đáng.

8.3.3 Lựa chọn chiến lược và giải pháp

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

a) đáp ứng yêu cầu duy trì và phục hồi các hoạt động ưu tiên trong các khung thời gian đã định và năng lực đã thống nhất;

b) xem xét mức độ và loại hình rủi ro mà tổ chức được phép hay không được phép đối mặt;

c) xem xét chi phí và lợi ích kèm theo.

8.3.4 Yêu cầu về nguồn lực

Tổ chức phải xác định các yêu cầu về nguồn lực cho việc thực hiện các giải pháp kinh doanh liên tục được lựa chọn. Loại nguồn lực được xem xét phải bao gồm, nhưng không giới hạn ở:

a) con người;

b) thông tin và dữ liệu;

c) cơ sở hạ tầng vật lý như tòa nhà, nơi làm việc hoặc cơ sở vật chất khác và 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 chuyển và logistic;

g) tài chính;

h) đối tác và nhà cung ứng.

8.3.5 Thực hiện giải pháp

Tổ chức phải thực hiện và duy trì các giải pháp kinh doanh liên tục để các giải pháp này có thể được kích hoạt khi cần.

8.4 Kế hoạch và thủ tục kinh doanh liên tục

8.4.1 Khái quát

Tổ chức phải thực hiện và duy trì cơ cấu ứng phó có khả năng cảnh báo kịp thời và trao đổi thông tin với các bên quan tâm có liên quan. Tổ chức phải đưa ra các kế hoạch và thủ tục cho việc quản lý tổ chức trong thời gian gián đoạn. Các kế hoạch và thủ tục phải được sử dụng khi cần 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 nhận biết và lập thành văn bản các kế hoạch và thủ tục kinh doanh liên tục trên cơ sở đầu ra của chiến lược và giải pháp được lựa chọn.

Các thủ tục phải:

a) cụ thể về các bước phải thực hiện ngay lập tức khi gián đoạn;

b) linh hoạt trong việc ứng phó với các điều kiện gián đoạn nội bộ và bên ngoài thay đổi;

c) tập trung vào tác động của sự cố có thể tiềm ẩn dẫn đến gián đoạn;

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

e) phân công vai trò và trách nhiệm đối với các nhiệm vụ trong đó.

8.4.2 Cơ cấu ứng phó

8.4.2.1 Tổ chức phải thực hiện và duy trì cơ cấu xác định rõ một hay nhiều nhóm chịu trách nhiệm

ứng phó với gián đoạn.

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

8.4.2.3 Các nhóm phải có năng lực tổng thể đối với việc:

a) đánh giá tính chất và mức độ của việc gián đoạn và tác động tiềm ẩn của nó;

b) đánh giá tác động theo các ngưỡng đã được xác định để lý giải cho việc bắt đầu ứng phó chính thức;

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

d) hoạch định các hành động cần thực hiện;

e) thiết lập thứ tự ưu tiên (trong đó an toàn sinh mạng là ưu tiên hàng đầu);

f) theo dõi ảnh hưởng của gián đoạn và việc ứng phó của tổ chức;

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

h) trao đổi thông tin với các bên quan tâm có liên quan, cơ quan quản lý và truyền thông.

8.4.2.4 Từng nhóm phải có:

a) nhân sự xác định và người thay thế họ với các trách nhiệm, quyền hạn và năng lực cần thiết để thực hiện vai trò được phân công;

b) thủ tục dạng văn bản hướng dẫn các hành động (xem 8.4.4), bao gồm những hành động cho việc kích hoạt, triển khai, điều phối và trao đổi thông tin về việc ứng phó.

8.4.3 Cảnh báo và trao đổi thông tin

8.4.3.1 Tổ chức phải lập thành văn bản và duy trì các thủ tục đối với việc:

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

CHÚ THÍCH: Tổ chức có thể lập thành văn bản và duy trì thủ tục về cách thức và trong những hoàn cảnh nào tổ chức trao đổi thông tin với nhân viên và các đầu mối liên lạc trong trường hợp khẩn cấp của mình.

b) tiếp nhận, lập thành văn bản và trả lời trong trao đổi thông tin từ các bên quan tâm, bao gồm cả hệ thống tư vấn về rủi ro quốc gia hoặc khu vực hay hệ thống tương tự;

c) đảm bảo sẵn có các phương tiện trao đổi thông tin trong thời gian gián đoạn;

d) hỗ trợ việc trao đổi thông tin có cấu trúc với các bên ứng phó khẩn cấp;

e) cung cấp chi tiết về ứng phó truyền thông của tổ chức sau sự cố, bao gồm cả chiến lược trao đổi thông tin;

f) ghi nhận chi tiết về gián đoạn, hành động được thực hiện và quyết định được đưa ra.

8.4.3.2 Khi có thể phải xem xét và thực hiện các việc sau:

a) cảnh báo cho các bên quan tâm có thể bị ảnh hưởng bởi gián đoạn đang hoặc sắp xảy ra;

b) đảm bảo sự điều phối và trao đổi thông tin thích hợp giữa nhiều tổ chức ứng phó.

Thủ tục cảnh báo và trao đổi thông tin phải được luyện tập như một phần trong chương trình luyện tập của tổ chức quy định ở 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 này phải đưa ra hướng dẫn và thông tin hỗ trợ cho các nhóm ứng phó với gián đoạn và hỗ trợ tổ chức ứng phó và phục hồi.

8.4.4.2 Toàn bộ các kế hoạch kinh doanh liên tục phải bao gồm:

a) chi tiết về hành động mà các nhóm sẽ thực hiện nhằm:

1) duy trì hoặc phục hồi các hoạt động ưu tiên theo khung thời gian đã định;

2) theo dõi tác động của gián đoạn và việc ứng phó của tổ chức với gián đoạn đó;

b) đề cập đến (các) ngưỡng đã xác định và quá trình kích hoạt ứng phó;

c) các thủ tục giúp cung cấp sản phẩm và dịch vụ ở mức năng lực đã thống nhất;

d) chi tiết cho việc quản lý các hệ quả tức thời của việc gián đoạn liên quan tới:

1) lợi ích của cá nhân;

2) ngăn ngừa thiệt hại thêm hoặc sự không sẵn có các hoạt động ưu tiên;

3) tác động tới môi trường.

8.4.4.3 Từng 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 giải pháp;

d) hỗ trợ thông tin cần thiết để kích hoạt (bao gồm tiêu chí kích hoạt), triển khai, điều phối và trao đổi thông tin về các hành động của nhóm;

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

f) các yêu cầu về nguồn lực;

g) các yêu cầu về báo cáo;

h) quá trình cho việc dừng thực hiện.

Từng kế hoạch phải sẵn có để sử dụng được tại nơi và khi cần.

8.4.5 Phục hồi

Tổ chức phải có các quá trình được lập thành văn bản đối với việc khôi phục và trở lại hoạt động kinh doanh sau các biện pháp tạm thời được chấp nhận trong và sau gián đoạn.

8.5 Chương trình luyện tập

Tổ chức phải thực hiện và duy trì chương trình luyện tập và thử nghiệm để xác nhận giá trị sử dụng theo thời gian về hiệu lực của các chiến lược và giải pháp kinh doanh liên tục của mình.

Tổ chức phải thực hiện các bài luyện tập và bài kiểm tra:

a) nhất quán với mục tiêu kinh doanh liên tục của tổ chức;

b) dựa trên các kịch bản thích hợp được lập kế hoạch với các mục đích và mục tiêu được xác định rõ;

c) xây dựng nhóm công tác, năng lực, sự tin cậy và hiểu biết cho những người có vai trò thực hiện liên quan đến gián đoạn;

d) được thực hiện đồng thời theo thời gian, xác nhận giá trị sử dụng của các chiến lược và giải pháp kinh doanh liên tục của tổ chức;

e) lập các báo cáo chính thức sau tập luyện bao gồm các kết quả, khuyến nghị và hành động để thực hiện 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 hoạch định và khi có những thay đổi đáng kể trong tổ chức hoặc bối cảnh trong đó tổ chức hoạt động.

Tổ chức phải hành động dựa trên kết quả việc luyện tập và thử nghiệm để thực hiện những thay đổi và cải tiến.

8.6 Đánh giá hệ thống tài liệu và năng lực kinh doanh liên tục

Tổ chức phải:

a) đánh giá sự thích hợp, thỏa đáng và hiệu lực của việc phân tích tác động kinh doanh, đánh giá rủi ro, các chiến lược, giải pháp, kế hoạch và thủ tục;

b) thực hiện việc đánh giá thông qua xem xét, phân tích, các bài tập, bài thử, báo cáo sau sự cố và đánh giá kết quả thực hiện;

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

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

e) cập nhật tài liệu và quy trình một cách kịp thời;

Những đánh giá này phải được tiến hành theo các khoảng thời gian hoạch định, sau sự cố hoặc sau

kích hoạt và khi có những thay đổi đáng kể xảy ra.

9 Đánh giá kết quả thực hiện

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) phương pháp theo dõi, đo lường, phân tích và đánh giá, khi có thể thực hiện được, để đảm bảo kết quả có giá trị sử dụng;

c) khi nào và ai phải thực hiện và ai thực hiện theo dõi và đo lường;

d) khi nào và ai phải phân tích và đánh giá các kết quả theo dõi và đo lường.

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

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

9.2 Đánh giá nội bộ

9.2.1 Khái quát

Tổ chức phải tiến hành các cuộc đánh giá nội bộ theo những khoảng thời gian được hoạch định để cung cấp thông tin về việc BCMS có hay không:

a) phù hợp với

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

2) các yêu cầu của tiêu chuẩn này;

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

9.2.2 (Các) chương trình đánh giá

Tổ chức phải:

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

b) xác định chuẩn mực đánh giá và phạm vi của từng cuộc đánh giá;

c) lựa chọn chuyên gia đánh giá và tiến hành các cuộc đánh giá để đảm bảo tính vô tư và tính khách quan của quá trình đánh giá;

d) đảm bảo rằng kết quả đánh giá được báo cáo tới cấp lãnh đạo thích hợp;

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 các hành động khắc phục thích hợp được thực hiện không chậm trễ để loại bỏ mọi sự không phù hợp được phát hiện và các nguyên nhân của sự không phù hợp;

g) đảm bảo các hành động sau đánh giá bao gồm kiểm tra xác nhận hành động được thực hiện và báo cáo kết quả kiểm tra xác nhận.

9.3 Xem xét của lãnh đạo

9.3.1 Khái quát

Lãnh đạo cao nhất phải xem xét BCMS của tổ chức theo những khoảng thời gian được hoạch định, để đảm bảo nó luôn thích hợp, thỏa đáng và có hiệu lực.

9.3.2 Đầu vào xem xét của lãnh đạo

Xem xét của lãnh đạo phải bao gồm xem xét về:

a) tình trạng của các hành động từ xem xét của lãnh đạo trước đó;

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

c) thông tin về kết quả thực hiện BCMS, bao gồm các xu hướng về:

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

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

3) các kết quả đánh giá;

d) phản hồi từ các bên quan tâm;

e) nhu cầu thay đổi 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 tiến kết quả thực hiện và hiệu lực của BCMS;

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

h) đầu ra của việc đánh giá tài liệu và năng lực kinh doanh liên tục (xem 8.6);

i) rủi ro hoặc vấn đề chưa được giải quyết một cách đầy đủ trong đánh giá rủi ro bất kỳ nào trước đó;

j) các bài học rút ra và các hành động nảy sinh từ những lần thoát nạn và gián đoạn;

k) các cơ hội cải tiến liên tục.

9.3.3 Đầu ra xem xét của lãnh đạo

9.3.3.1 Đầu ra xem xét của lãnh đạo phải bao gồm các quyết định liên quan đến cơ hội cải tiến liên tục và mọi nhu cầu thay đổi đối với BCMS để cải tiến hiệu lực và hiệu quả của hệ thống và bao gồm:

a) những thay đổi về 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, các kế hoạch kinh doanh liên tục;

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

d) cách thức đo lường hiệu lực của các kiểm soát.

9.3.3.2 Tổ chức phải lưu giữ thông tin dạng văn bản làm bằng chứng về các kết quả xem xét của lãnh đạo. Tổ chức phải:

a) trao đổi thông tin về kết quả xem xét của lãnh đạo với các bên quan tâm có liên quan;

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

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.

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

a) ứng phó với sự không phù hợp và khi có thể

1) thực hiện hành động để kiểm soát và khắc phục sự không phù hợp;

2) xử lý các hệ quả.

b) đánh giá nhu cầu đối với hành động nhằm loại bỏ (các) nguyên nhân dẫn đến sự không phù hợp, để không tái diễn hoặc xảy ra ở nơi khác bằng việc:

1) xem xét sự không phù hợp;

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

3) xác định liệu sự không phù hợp tương tự có tồn tại hoặc có khả năng xảy ra hay không;

c) thực hiện mọi hành động cần thiết;

d) xem xét hiệu lực của mọi hành động khắc phục được thực hiện;

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

Hành động khắc phục phải tương ứng với 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 hành động bất kỳ được thực hiện sau đó;

b) kết quả của mọi hành động khắc phục.

10.2 Cải tiến liên tục

Tổ chức phải cải tiến liên tục sự thích hợp, thỏa đáng và hiệu lực của BCMS, trên cơ sở các thước đo

định tính và định lượng.

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

CHÚ THÍCH: Tổ chức có thể sử dụng các quá trình của BCMS như sự lãnh đạo, hoạch định và đánh giá kết quả thực hiện để đạt được cải tiến.

Thư mục tài liệu tham khảo

[1] TCVN ISO 9001, *Hệ thống quản lý chất lượng - Các yêu cầu*

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

[3] TCVN ISO 19011, *Hướng dẫn đánh giá hệ thống quản lý*

[4] TCVN ISO/IEC/TS 17021-6, *Đánh giá sự phù hợp - Yêu cầu đối với tổ chức đánh giá và chứng nhận hệ thống quản lý - Phần 6: Yêu cầu về năng lực đối với tổ chức đánh giá và chứng nhận hệ thống quản lý kinh doanh liên tục*

[5] ISO/IEC 20000-1, *Công nghệ thông tin - Quản lý dịch vụ*

[6] ISO 22313, *An ninh xã hội - Hệ thống quản lý kinh doanh liên tục - Hướng dẫn*

[7] ISO 22316, *An ninh và khả năng thích ứng - Khả năng thích ứng của tổ chức - Các nguyên tắc và thuộc tính*

[8] ISO/TS 22317, *An ninh xã hội - Hệ thống quản lý kinh doanh liên tục - Hướng dẫn phân tích tác động kinh doanh (BIA)*

[9] ISO/TS 22318, *An ninh xã hội - Hệ thống quản lý kinh doanh liên tục - Hướng dẫn về tính liên tục của chuỗi cung ứng*

[10] ISO/TS 22330, *An ninh và khả năng thích ứng - Hệ thống quản lý kinh doanh liên tục - Hướng dẫn về khía cạnh con người trong kinh doanh liên tục*

[11] ISO/TS 22331, *An ninh và khả năng thích ứng - Hệ thống quản lý kinh doanh liên tục - Hướng dẫn về chiến lược kinh doanh liên tục*

[12] TCVN ISO/IEC 27001, *Hệ thống quản lý an toàn thông tin*

[13] TCVN ISO/IEC 27031, *Công nghệ thông tin - Các kỹ thuật an toàn - Hướng dẫn về đảm bảo sự sẵn sàng về công nghệ thông tin và truyền thông cho kinh doanh liên tục*

[14] TCVN ISO 28000, *Quy định đối với hệ thống quản lý an toàn chuỗi cung ứng*

[15] TCVN ISO 31000, *Quản lý rủi ro - Hướng dẫn*

[16] TCVN ISO/IEC 31010, *Quản lý rủi ro - Kỹ thuật đánh giá rủi ro*

[17] TCVN 9788, *Quản lý rủi ro - Từ vựng*

Mục lục

Lời nói đầu

Lời giới thiệu

1 Phạm vi áp dụng

2 Tài liệu viện dẫn

3 Thuật ngữ và định nghĩa

4 Bối cảnh của tổ chức

4.1 Hiểu tổ chức và bối cảnh của tổ chức

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

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

4.4 Hệ thống quản lý kinh doanh liên tục

5 Sự lãnh đạo

5.1 Sự lãnh đạo và cam kết

5.2 Chính sách
5.3 Vai trò, trách nhiệm và quyền hạn
6 Hoạch định
6.1 Hành động giải quyết rủi ro và cơ hội
6.2 Mục tiêu kinh doanh liên tục và hoạch định để đạt được mục tiêu
6.3 Hoạch định các thay đổi đối với BCMS
7 Hỗ trợ
7.1 Nguồn lực
7.2 Năng lực
7.3 Nhận thức
7.4 Trao đổi thông tin
7.5 Thông tin dạng văn bản
8 Thực hiện
8.1 Hoạch định và kiểm soát việc thực hiện
8.2 Phân tích tác động kinh doanh và đánh giá rủi ro
8.3 Chiến lược và giải pháp kinh doanh liên tục
8.4 Kế hoạch và thủ tục kinh doanh liên tục
8.5 Chương trình luyện tập
8.6 Đánh giá hệ thống tài liệu và năng lực kinh doanh liên tục
9 Đánh giá kết quả thực hiện
9.1 Theo dõi, đo lường, phân tích và đánh giá
9.2 Đánh giá nội bộ
9.3 Xem xét của lãnh đạo
10 Cải tiến
10.1 Sự không phù hợp và hành động khắc phục
10.2 Cải tiến liên tục
Thư mục tài liệu tham khảo