

TIÊU CHUẨN QUỐC GIA

TCVN ISO 31000:2018

ISO 31000: 2018

QUẢN LÝ RỦI RO - HƯỚNG DẪN

Risk management - Guidelines

Lời nói đầu

TCVN ISO 31000:2018 (ISO 31000:2018) thay thế cho TCVN ISO 31000:2011 (ISO 31000:2009);

TCVN ISO 31000:2018 hoàn toàn tương đương với ISO 31000:2018;

TCVN ISO 31000:2011 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

Tiêu chuẩn này dùng cho những người tạo lập và bảo vệ các giá trị của tổ chức thông qua việc quản lý rủi ro, ra quyết định, thiết lập và đạt được các mục tiêu, cải tiến kết quả thực hiện.

Các tổ chức ở mọi loại hình và quy mô đều đối mặt với các yếu tố và các ảnh hưởng nội bộ và bên ngoài dẫn đến sự không chắc chắn cho tổ chức trong việc đạt được các mục tiêu của mình.

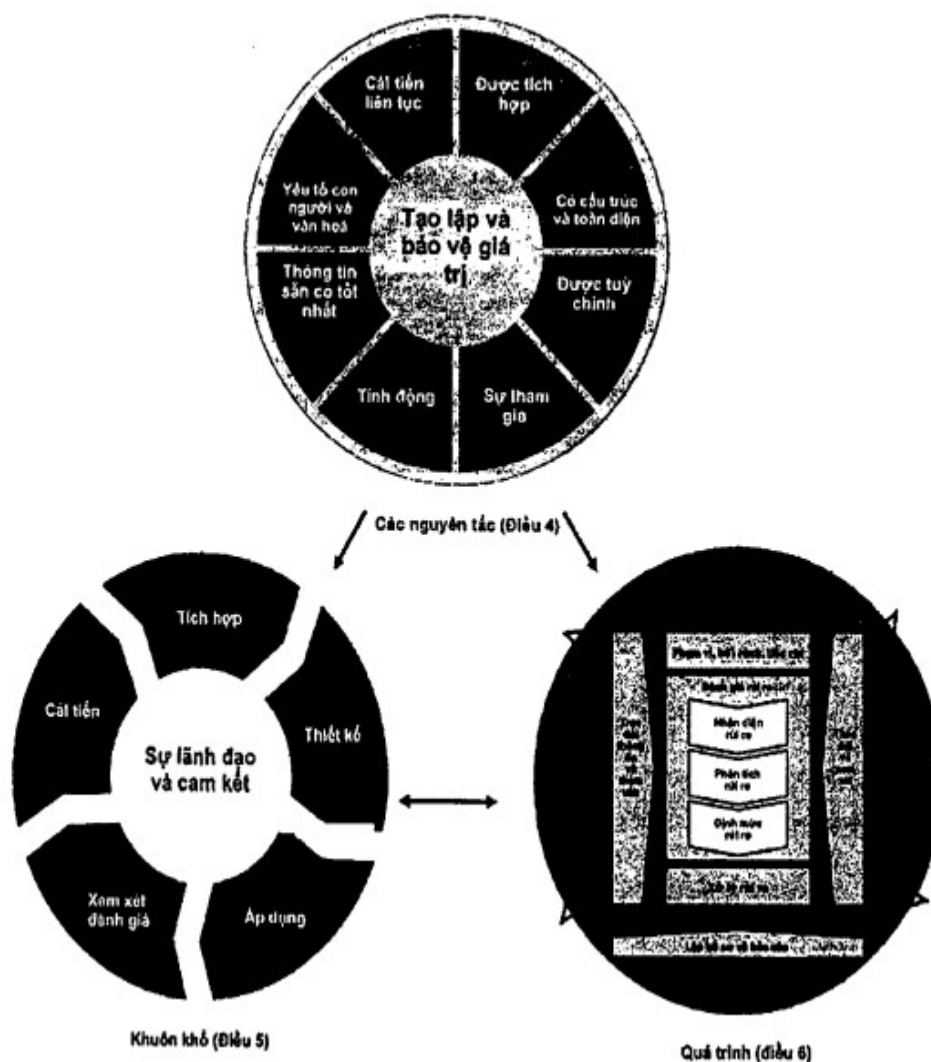
Quản lý rủi ro có tính lặp lại và hỗ trợ tổ chức trong việc thiết lập chiến lược, đạt được các mục tiêu và ra các quyết định đúng đắn.

Quản lý rủi ro là một phần của việc điều hành, lãnh đạo và là nền tảng cho cách thức tổ chức được quản lý ở mọi cấp. Quản lý rủi ro đóng góp cho việc cải tiến hệ thống quản lý.

Quản lý rủi ro là một phần trong tất cả các hoạt động liên quan đến tổ chức và bao gồm cả sự tương tác với các bên liên quan.

Quản lý rủi ro xem xét bối cảnh nội bộ và bên ngoài của tổ chức, kể cả hành vi của con người và các yếu tố văn hóa.

Quản lý rủi ro dựa trên các nguyên tắc, khuôn khổ và quá trình được nêu trong tiêu chuẩn này, như minh họa trong Hình 1. Những yếu tố cấu thành này hầu như đã có sẵn một phần hoặc toàn bộ ở một tổ chức, tuy nhiên, nó có thể cần được điều chỉnh hoặc cải tiến để quản lý rủi ro một cách hiệu lực, hiệu quả và nhất quán.



Hình 1 - Nguyên tắc, khuôn khổ và quá trình

QUẢN LÝ RỦI RO - HƯỚNG DẪN

Risk management - Guidelines

1 Phạm vi áp dụng

Tiêu chuẩn này đưa ra hướng dẫn quản lý các rủi ro mà tổ chức phải đối mặt. Việc áp dụng các hướng dẫn này có thể được tùy chỉnh theo tổ chức và bối cảnh của tổ chức.

Tiêu chuẩn này đưa ra cách tiếp cận chung để quản lý mọi loại rủi ro và không cho một ngành công nghiệp hay lĩnh vực cụ thể.

Tiêu chuẩn này có thể được sử dụng trong suốt vòng đời của tổ chức và có thể được áp dụng cho bất kỳ hoạt động nào, kể cả việc ra quyết định ở tất cả các cấp.

2 Tài liệu viện dẫn

Không có tài liệu viện dẫn.

3 Thuật ngữ và định nghĩa

Tiêu chuẩn này áp dụng các thuật ngữ và các định nghĩa dưới đây.

3.1

Rủi ro (risk)

Ảnh hưởng của sự không chắc chắn tới mục tiêu.

CHÚ THÍCH 1: Ảnh hưởng là sự sai lệch so với dự kiến. Ảnh hưởng có thể tích cực, tiêu cực hoặc cả hai và có thể được giải quyết, có thể tạo ra hay dẫn đến cơ hội và mối đe dọa.

CHÚ THÍCH 2: Các mục tiêu có thể có những khía cạnh và các phạm trù khác nhau và có thể được áp dụng ở các cấp khác nhau.

CHÚ THÍCH 3: Rủi ro thường được thể hiện theo các thuật ngữ *nguồn rủi ro* (3.4), *sự kiện* (3.5) tiềm

ấn, *hệ quả* (3.6) và *khả năng xảy ra* (3.7) của chúng.

3.2

Quản lý rủi ro (risk management)

Các hoạt động có phối hợp để định hướng và kiểm soát một tổ chức về *rủi ro* (3.1).

3.3

Bên liên quan (stakeholder)

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

CHÚ THÍCH 1: Thuật ngữ “Bên quan tâm” có thể được dùng thay thế cho “Bên liên quan”.

3.4

Nguồn rủi ro (risk source)

Yếu tố mà tự nó hoặc khi kết hợp có tiềm năng nội tại làm nảy sinh *rủi ro* (3.1).

3.5

Sự kiện (event)

Sự xuất hiện hoặc thay đổi của một tập hợp các tình huống cụ thể.

CHÚ THÍCH 1: Một sự kiện có thể xảy ra một hoặc nhiều lần và có thể có nhiều nguyên nhân và *hệ quả* (3.6).

CHÚ THÍCH 2: Một sự kiện cũng có thể là điều được mong đợi mà không xảy ra, hoặc điều không mong đợi nhưng lại xảy ra.

CHÚ THÍCH 3: Một sự kiện có thể là một nguồn rủi ro.

3.6

Hệ quả (consequence)

Kết quả của một *sự kiện* (3.5) ảnh hưởng đến các mục tiêu.

CHÚ THÍCH 1: Một hệ quả có thể chắc chắn hoặc không chắc chắn và có thể có tác động tích cực hoặc tiêu cực đến các mục tiêu.

CHÚ THÍCH 2: Hệ quả có thể được biểu thị một cách định tính hoặc định lượng.

CHÚ THÍCH 3: Bất kỳ hệ quả nào cũng có thể gia tăng theo những hiệu ứng dây chuyền và tích lũy.

3.7

Khả năng xảy ra (likelihood)

Cơ hội xảy ra điều gì đó

CHÚ THÍCH 1: Trong thuật ngữ về quản lý *rủi ro* (3.2), từ “khả năng xảy ra” được sử dụng để chỉ cơ hội xảy ra điều gì đó, có thể được định rõ, đo lường hay xác định một cách khách quan hoặc chủ quan, định tính hoặc định lượng và được mô tả bằng cách sử dụng thuật ngữ chung hay theo toán học (như xác suất trong một khoảng thời gian cho trước).

CHÚ THÍCH 2: Từ “khả năng xảy ra” trong tiếng Anh có thể không có từ tương đương trực tiếp trong những ngôn ngữ khác, thay vào đó thường dùng từ “xác suất”. Tuy nhiên, từ “xác suất” được diễn giải hẹp hơn trong thuật ngữ toán học. Vì vậy, trong quản lý rủi ro sử dụng thuật ngữ “khả năng xảy ra” với mục đích diễn đạt cùng phạm vi với thuật ngữ “xác suất” được dùng nhiều hơn trong các ngôn ngữ khác với tiếng Anh.

3.8

Kiểm soát (control)

Biện pháp kiểm chế và/hoặc điều chỉnh rủi ro (3.1).

CHÚ THÍCH 1: Kiểm soát bao gồm, nhưng không giới hạn ở, mọi quá trình, chính sách, thiết bị, thực hành hoặc các điều kiện và/hoặc các hành động khác có thể kiểm chế và/hoặc điều chỉnh rủi ro.

CHÚ THÍCH 2: Kiểm soát có thể không luôn tạo ra tác dụng điều chỉnh dự kiến hoặc được giả định.

4 Nguyên tắc

Mục đích của quản lý rủi ro là tạo lập và bảo vệ giá trị. Quản lý rủi ro cải tiến kết quả thực hiện, khuyến khích đổi mới và hỗ trợ việc đạt được các mục tiêu.

Các nguyên tắc nêu trong Hình 2 đưa ra hướng dẫn về các đặc trưng của việc quản lý rủi ro hiệu lực và hiệu quả, trao đổi thông tin về giá trị, giải thích ý đồ và mục đích của quản lý rủi ro. Các nguyên tắc

này là nền tảng cho việc quản lý rủi ro và cần được xem xét khi thiết lập khuôn khổ quản lý rủi ro và các quá trình quản lý rủi ro của tổ chức. Những nguyên tắc này cần cho phép tổ chức quản lý ảnh hưởng của sự không chắc chắn tới các mục tiêu của mình.



Hình 2 - Nguyên tắc

Quản lý rủi ro có hiệu lực, đòi hỏi các yếu tố ở Hình 2 và các yếu tố này có thể được diễn giải như sau:

a) Được tích hợp

Quản lý rủi ro là một phần không thể tách rời của tất cả các hoạt động tổ chức.

b) Có cấu trúc và toàn diện

Một cách tiếp cận toàn diện và có cấu trúc để quản lý rủi ro mang lại kết quả nhất quán và có thể so sánh được.

c) Được tùy chỉnh

Khuôn khổ và quá trình quản lý rủi ro được tùy chỉnh và thích hợp với bối cảnh nội bộ và bên ngoài của tổ chức có liên quan đến các mục tiêu của tổ chức.

d) Sự tham gia

Sự tham gia thích hợp và kịp thời của các bên liên quan cho phép xem xét tri thức, quan điểm và cảm nhận của họ. Điều này dẫn đến việc nâng cao nhận thức và việc quản lý rủi ro có đầy đủ thông tin.

e) Tính động

Rủi ro có thể hình thành, thay đổi hoặc biến mất do bối cảnh nội bộ, bên ngoài của tổ chức thay đổi. Quản lý rủi ro dự đoán, phát hiện, ghi nhận và ứng phó một cách kịp thời, thích hợp với những thay đổi và sự kiện đó.

f) Thông tin sẵn có tốt nhất

Đầu vào cho quản lý rủi ro dựa trên thông tin trong quá khứ, hiện tại, cũng như dự báo trong tương lai. Quản lý rủi ro tính đến một cách rõ ràng mọi hạn chế và sự không chắc chắn gắn liền với những thông tin và dự báo đó. Thông tin cần kịp thời, rõ ràng và có sẵn cho các bên liên quan.

g) Yếu tố con người và văn hóa

Hành vi của con người và văn hóa ảnh hưởng đáng kể đến tất cả các khía cạnh của quản lý rủi ro tại mỗi cấp và giai đoạn.

h) Cải tiến liên tục

Quản lý rủi ro được cải tiến liên tục thông qua học hỏi và kinh nghiệm.

5 Khuôn khổ

5.1 Khái quát

Mục đích của khuôn khổ quản lý rủi ro là hỗ trợ tổ chức tích hợp quản lý rủi ro vào các hoạt động và các chức năng quan trọng. Hiệu lực của quản lý rủi ro sẽ phụ thuộc việc tích hợp quản lý rủi ro vào hoạt động điều hành của tổ chức, kể cả việc ra quyết định. Điều này đòi hỏi sự hỗ trợ từ các bên liên quan, đặc biệt là lãnh đạo cao nhất.

Việc xây dựng khuôn khổ bao gồm việc tích hợp, thiết kế, thực hiện, đánh giá và cải tiến quản lý rủi ro trong toàn tổ chức. Hình 3 minh họa các thành phần của khuôn khổ.

Tổ chức cần đánh giá các thực hành và các quá trình quản lý rủi ro hiện tại của mình, đánh giá mọi cách biệt và giải quyết những cách biệt đó trong khuôn khổ quản lý rủi ro.

Các thành phần của khuôn khổ quản lý rủi ro và cách thức các thành phần này cùng hoạt động cần được tùy chỉnh theo nhu cầu của tổ chức.



Hình 3 - Khuôn khổ

5.2 Sự lãnh đạo và cam kết

Lãnh đạo cao nhất và bộ phận giám sát nếu có, cần đảm bảo rằng quản lý rủi ro được tích hợp vào tất cả các hoạt động của tổ chức và cần chứng tỏ sự lãnh đạo và cam kết bằng cách:

- tùy chỉnh và áp dụng tất cả các thành phần của khuôn khổ;
- ban hành tuyên bố hoặc chính sách thiết lập cách tiếp cận, kế hoạch hoặc lộ trình hành động quản lý rủi ro;
- đảm bảo rằng các nguồn lực cần thiết được phân bổ cho việc quản lý rủi ro;
- phân công quyền hạn, trách nhiệm và trách nhiệm giải trình ở các cấp thích hợp trong tổ chức.

Điều này sẽ giúp tổ chức:

- thống nhất quản lý rủi ro với các mục tiêu, chiến lược và văn hóa của tổ chức;
- nhận biết và giải quyết mọi nghĩa vụ, cũng như các cam kết tự nguyện của tổ chức;
- thiết lập số lượng về loại rủi ro được phép hoặc không được phép đưa vào hướng dẫn xây dựng các tiêu chí rủi ro, đảm bảo rằng chúng được trao đổi thông tin trong tổ chức và với các bên liên quan;
- trao đổi thông tin về giá trị của quản lý rủi ro trong tổ chức và với các bên liên quan;
- thúc đẩy việc theo dõi một cách hệ thống các rủi ro;
- đảm bảo rằng khuôn khổ quản lý rủi ro giữ được sự phù hợp với bối cảnh của tổ chức.

Lãnh đạo cao nhất chịu trách nhiệm giải trình về quản lý rủi ro còn bộ phận giám sát chịu trách nhiệm giải trình đối với việc giám sát quản lý rủi ro. Bộ phận giám sát thường được kỳ vọng hoặc yêu cầu:

- đảm bảo rằng các rủi ro được xem xét một cách thỏa đáng khi thiết lập các mục tiêu của tổ chức;
- hiểu những rủi ro mà tổ chức phải đối mặt khi theo đuổi các mục tiêu của mình;
- đảm bảo rằng hệ thống để quản lý những rủi ro này được triển khai và vận hành một cách hiệu lực;
- đảm bảo rằng những rủi ro này thích hợp với bối cảnh các mục tiêu của tổ chức;
- đảm bảo rằng thông tin về những rủi ro này và việc quản lý chúng được trao đổi một cách thích hợp.

5.3 Tích hợp

Việc tích hợp quản lý rủi ro dựa bên sự hiểu biết về cơ cấu và bối cảnh của tổ chức. Cơ cấu khác nhau tùy thuộc vào mục đích, mục tiêu và sự phức tạp của tổ chức. Rủi ro được quản lý tại từng phần trong cơ cấu của tổ chức. Mọi người trong tổ chức đều có trách nhiệm quản lý rủi ro.

Việc điều hành giúp định hướng cho tổ chức, các mối quan hệ nội bộ, bên ngoài, các quy tắc, quá trình và thực hành cần thiết để đạt được mục đích của tổ chức. Cơ cấu quản lý chuyển định hướng điều hành thành chiến lược và các mục tiêu liên quan cần thiết để đạt được các mức mong muốn về kết quả thực hiện bền vững và khả năng tồn tại lâu dài. Xác định trách nhiệm giải trình về quản lý rủi ro và vai trò giám sát trong tổ chức là một phần không thể thiếu trong điều hành của tổ chức.

Tích hợp quản lý rủi ro vào tổ chức là một quá trình động, lặp lại và cần được tùy chỉnh theo nhu cầu và văn hóa của tổ chức. Quản lý rủi ro cần là một phần không tách biệt với mục đích, việc điều hành, sự lãnh đạo và cam kết, chiến lược, mục tiêu và hoạt động của tổ chức.

5.4 Thiết kế

5.4.1 Hiểu về tổ chức và bối cảnh của tổ chức

Khi thiết kế khuôn khổ quản lý rủi ro, tổ chức cần xem xét và hiểu bối cảnh nội bộ và bên ngoài của mình.

Xem xét bối cảnh bên ngoài của tổ chức có thể bao gồm, nhưng không giới hạn ở:

- các yếu tố xã hội, văn hóa, chính trị, pháp lý, chế định, tài chính, công nghệ, kinh tế và môi trường ở cấp quốc tế, quốc gia, khu vực hoặc địa phương;
- những động lực và xu hướng chính ảnh hưởng đến mục tiêu của tổ chức;
- các mối quan hệ, cảm nhận, các giá trị, nhu cầu và mong đợi của các bên liên quan bên ngoài;
- các mối quan hệ và cam kết theo hợp đồng;
- mức độ phức tạp của mạng lưới và sự lệ thuộc lẫn nhau.

Việc xem xét bối cảnh nội bộ của tổ chức có thể bao gồm, nhưng không giới hạn ở:

- tầm nhìn, sứ mệnh và các giá trị;
- điều hành, cơ cấu tổ chức, vai trò và trách nhiệm giải trình;
- chiến lược, mục tiêu và chính sách;
- văn hóa của tổ chức;
- các tiêu chuẩn, hướng dẫn và các mô hình đã được tổ chức chấp nhận;
- khả năng, sự hiểu biết xét theo nghĩa nguồn lực và tri thức (ví dụ: vốn, thời gian, con người, tài sản trí tuệ, các quá trình, các hệ thống và công nghệ);
- dữ liệu, các hệ thống thông tin và các dòng thông tin;
- mối quan hệ với các bên liên quan nội bộ, có tính đến cảm nhận và các giá trị của họ;
- các mối quan hệ và cam kết theo hợp đồng;
- sự phụ thuộc và liên hệ lẫn nhau.

5.4.2 Khẳng định cam kết quản lý rủi ro

Lãnh đạo cao nhất và bộ phận giám sát, nếu có, cần chứng tỏ và khẳng định rõ cam kết liên tục của mình đối với quản lý rủi ro thông qua chính sách, tuyên bố hoặc các hình thức khác để truyền đạt rõ ràng các mục tiêu và cam kết của tổ chức đối với quản lý rủi ro. Cam kết cần bao gồm, nhưng không giới hạn ở:

- mục đích của tổ chức đối với quản lý rủi ro và các mối liên hệ với các mục tiêu và các chính sách khác của tổ chức;
- củng cố nhu cầu tích hợp quản lý rủi ro vào văn hóa tổng thể của tổ chức;
- dẫn dắt việc tích hợp quản lý rủi ro vào các hoạt động kinh doanh cốt lõi và ra quyết định;
- quyền hạn, trách nhiệm và trách nhiệm giải trình;

- tạo sự sẵn có các nguồn lực cần thiết;
- cách thức để giải quyết các mục tiêu mâu thuẫn nhau;
- đo lường và báo cáo qua các chỉ số kết quả thực hiện của tổ chức;
- xem xét và cải tiến.

Cam kết về quản lý rủi ro cần được trao đổi thông tin trong tổ chức và với các bên liên quan, khi thích hợp.

5.4.3 Phân công vai trò, quyền hạn, trách nhiệm và trách nhiệm giải trình trong tổ chức

Lãnh đạo cao nhất và bộ phận giám sát, nếu có, cần đảm bảo rằng quyền hạn, trách nhiệm và trách nhiệm giải trình của những vị trí liên quan đến quản lý rủi ro được phân công và trao đổi thông tin cho tất cả các cấp trong tổ chức, và cần:

- nhấn mạnh rằng quản lý rủi ro là trách nhiệm cốt lõi;
- xác định các cá nhân có trách nhiệm giải trình và quyền hạn đối với việc quản lý rủi ro (chủ sở hữu rủi ro).

5.4.4 Phân bổ nguồn lực

Lãnh đạo cao nhất và bộ phận giám sát, nếu có, cần đảm bảo phân bổ các nguồn lực thích hợp cho việc quản lý rủi ro, bao gồm, nhưng không giới hạn ở:

- con người, các kỹ năng, kinh nghiệm và năng lực;
- các quá trình, phương pháp và công cụ của tổ chức được sử dụng cho việc quản lý rủi ro;
- các quá trình và thủ tục được lập thành văn bản;
- hệ thống quản lý thông tin và tri thức;
- nhu cầu đào tạo và phát triển chuyên môn.

Tổ chức cần xem xét các khả năng và cả các trở ngại về nguồn lực hiện có.

5.4.5 Thiết lập việc trao đổi thông tin và tham vấn

Tổ chức cần thiết lập cách tiếp cận được phê duyệt để trao đổi thông tin và tham vấn nhằm hỗ trợ khuôn khổ quản lý rủi ro và tạo thuận lợi cho việc áp dụng có hiệu lực quản lý rủi ro. Việc trao đổi thông tin bao gồm việc chia sẻ thông tin với các đối tượng mục tiêu. Hoạt động tham vấn cũng đòi hỏi những người tham gia đưa ra phản hồi với mong muốn sẽ đóng góp và hình thành các quyết định hay các hoạt động khác. Các phương pháp và nội dung trao đổi thông tin và tham vấn cần phản ánh mong đợi của các bên liên quan khi thích hợp.

Việc trao đổi thông tin và tham vấn cần kịp thời và đảm bảo rằng thông tin liên quan được thu thập, đối chiếu, tổng hợp và chia sẻ khi thích hợp và đảm bảo rằng, thông tin phản hồi được cung cấp, việc cải tiến được thực hiện.

5.5 Áp dụng

Tổ chức cần áp dụng khuôn khổ quản lý rủi ro thông qua việc:

- xây dựng kế hoạch thích hợp bao gồm thời gian và các nguồn lực;
- xác định ở đâu, khi nào và cách thức ra các loại quyết định khác nhau trong toàn bộ tổ chức và do ai thực hiện;
- điều chỉnh quá trình ra quyết định hiện hành khi cần;
- đảm bảo các sắp đặt của tổ chức để quản lý rủi ro được hiểu rõ và thực hiện.

Việc áp dụng thành công khuôn khổ quản lý rủi ro đòi hỏi sự tham gia và nhận thức của các bên liên quan. Điều này cho phép các tổ chức giải quyết một cách rõ ràng sự không chắc chắn trong việc ra quyết định, đồng thời cũng đảm bảo rằng bất kỳ sự không chắc chắn mới hoặc tiếp nối, đều có thể được tính đến khi nó nảy sinh.

Một khuôn khổ quản lý rủi ro được thiết kế và triển khai đúng sẽ đảm bảo rằng quá trình quản lý rủi ro là một phần của tất cả các hoạt động trong toàn tổ chức, bao gồm cả việc ra quyết định và những thay đổi về bối cảnh nội bộ và bên ngoài sẽ được nắm bắt một cách đầy đủ.

5.6 Xem xét đánh giá

Để xem xét đánh giá tính hiệu lực của khuôn khổ quản lý rủi ro, tổ chức cần:

- định kỳ đo lường kết quả thực hiện khuôn khổ quản lý rủi ro theo mục đích, kế hoạch thực hiện, các chỉ số và những hành vi dự kiến;
- xác định xem khuôn khổ quản lý rủi ro có duy trì sự thích hợp để hỗ trợ đạt được các mục tiêu của tổ chức hay không.

5.7 Cải tiến

5.7.1 Điều chỉnh

Tổ chức cần liên tục theo dõi và điều chỉnh khuôn khổ quản lý rủi ro để giải quyết những thay đổi nội bộ, bên ngoài. Khi làm như vậy, tổ chức có thể nâng cao giá trị của mình.

5.7.2 Cải tiến liên tục

Tổ chức cần cải tiến liên tục sự phù hợp, đầy đủ và hiệu lực của khuôn khổ quản lý rủi ro và cách thức mà quá trình quản lý rủi ro được tích hợp.

Khi xác định các cách biệt hoặc cơ hội cải tiến có liên quan, tổ chức cần xây dựng các kế hoạch, nhiệm vụ và giao chúng cho những người chịu trách nhiệm giải trình đối với việc thực hiện. Ngay khi đã được triển khai, những cải tiến này cần góp phần thúc đẩy quản lý rủi ro.

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 Nguyên tắc

5 Khuôn khổ

5.1 Khái quát

5.2 Sự lãnh đạo và cam kết

5.3 Tích hợp

5.4 Thiết kế

5.5 Áp dụng

5.6 Xem xét đánh giá

5.7 Cải tiến

6 Quá trình

6.1 Khái quát

6.2 Trao đổi thông tin và tham vấn

6.3 Phạm vi, bối cảnh và tiêu chí

6.4 Đánh giá rủi ro

6.5 Xử lý rủi ro

6.6 Theo dõi và xem xét

6.7 Lập hồ sơ và báo cáo

Thư mục tài liệu tham khảo