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.

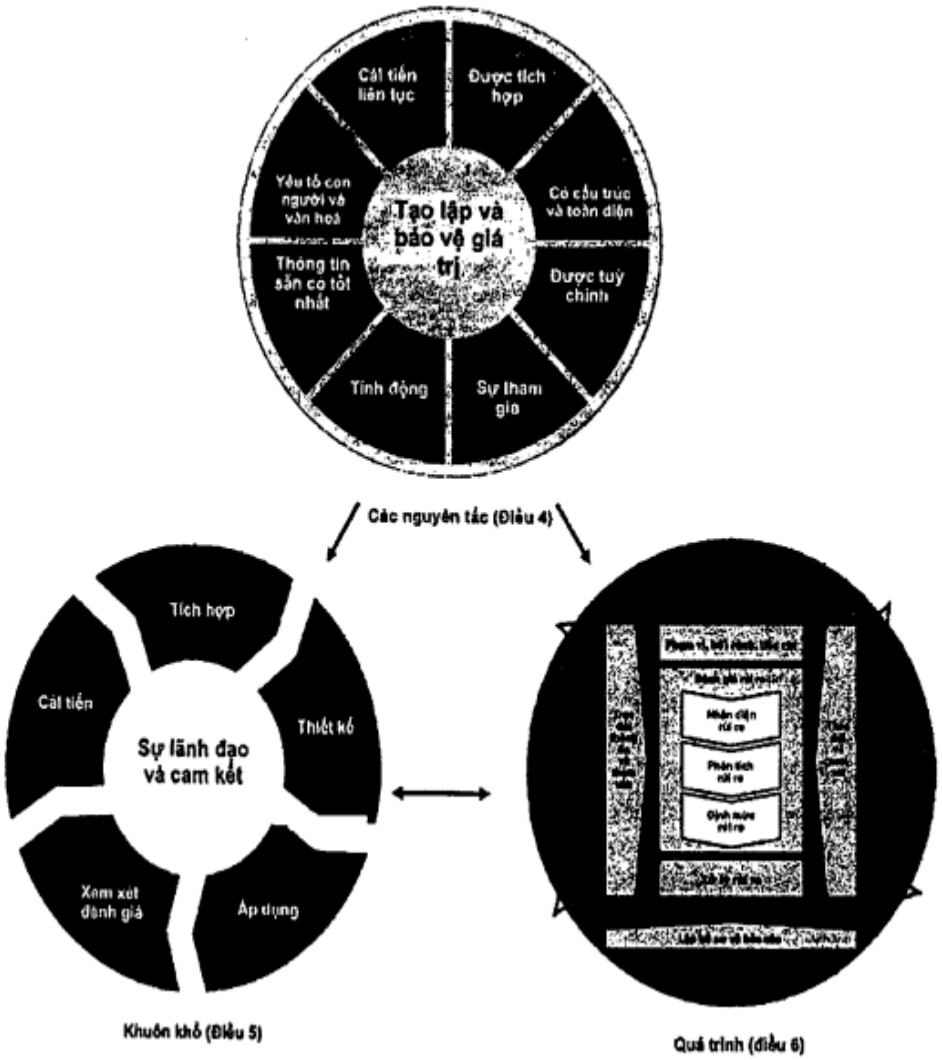
Quản lý rủi ro có tính lặp lại và hỗ trợ tổ chức trong việc thiết lập chiến lược, đạt được các mục tiêu và ra các quyết định đúng đắn.

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

ẩn, *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 kiềm 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 kiềm chế và/hoặc điều chỉnh rủi ro.

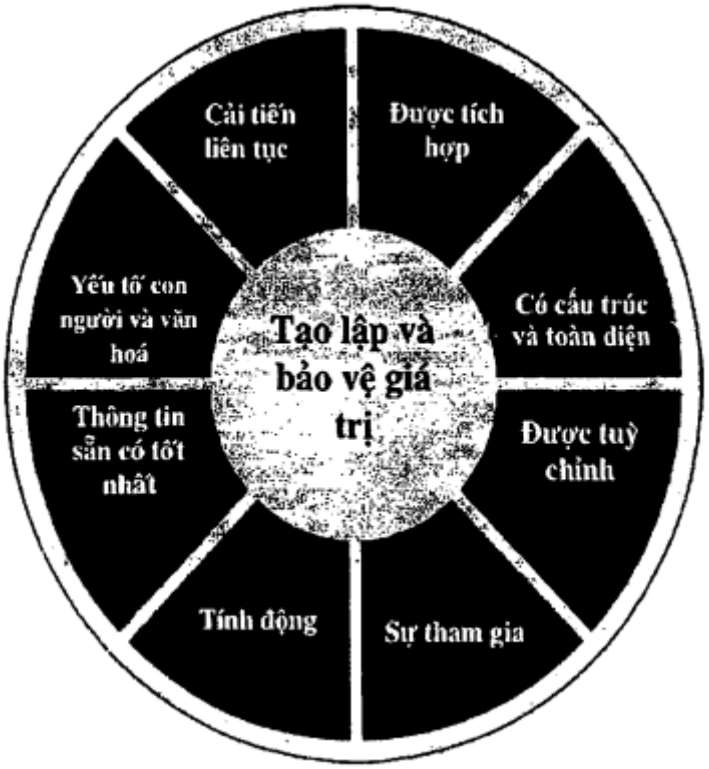
CHÚ THÍCH 2: Kiểm soát có thể không luôn tạo ra tác dụng điều chỉnh dự kiến hoặc được giả định.

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

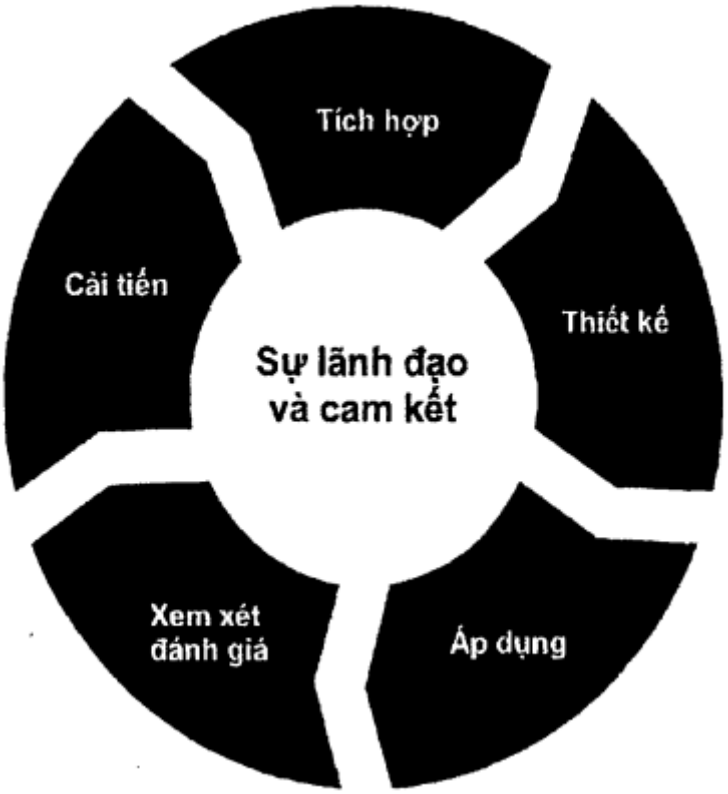
5.1 Khái quát

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 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

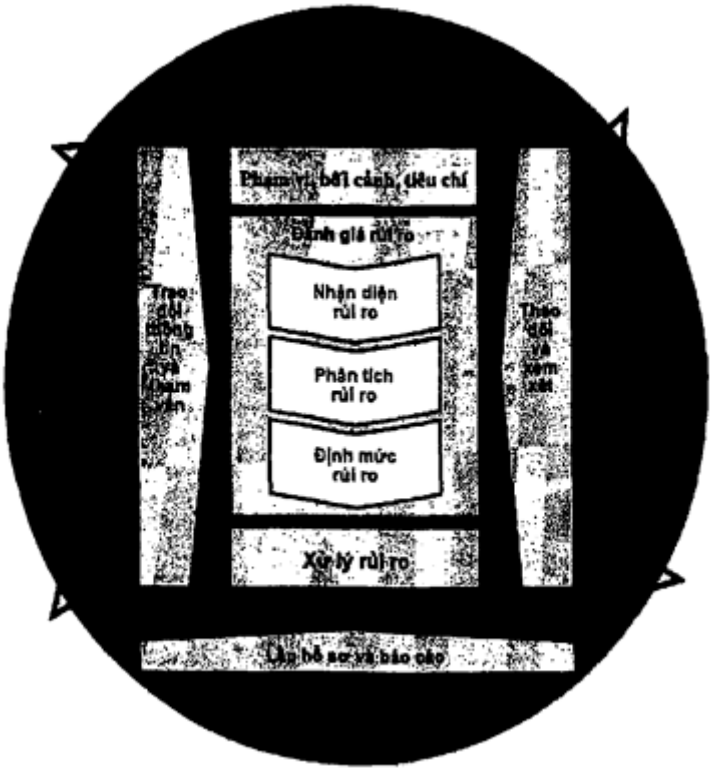
Tổ chức cần cải tiến liên tục sự phù hợp, đầy đủ và hiệu lực của khuôn khổ quản lý rủi ro và cách thức mà quá trình quản lý rủi ro được tích hợp.

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.

6 Quá trình

6.1 Khái quát

Quá trình quản lý rủi ro đòi hỏi việc áp dụng một cách hệ thống các chính sách, thủ tục và thực hành đối với các hoạt động trao đổi thông tin và tham vấn, thiết lập bối cảnh và đánh giá, xử lý, theo dõi, xem xét, ghi nhận lại và báo cáo về rủi ro. Quá trình này được minh họa trong Hình 4



Hình 4 - Quá trình

Quá trình quản lý rủi ro cần là một phần không tách rời trong quản lý, ra quyết định và được tích hợp vào cơ cấu, hoạt động, các quá trình của tổ chức. Quá trình quản lý rủi ro có thể được áp dụng ở cấp chiến lược, tác nghiệp, chương trình hoặc dự án.

Có thể có nhiều cách áp dụng quá trình quản lý rủi ro trong một tổ chức, được tùy chỉnh để đạt được mục tiêu và phù hợp với bối cảnh nội bộ, bên ngoài trong đó chúng được áp dụng.

Tính động và bản chất hay thay đổi trong hành vi và văn hóa của con người cần được xem xét trong suốt quá trình quản lý rủi ro.

Mặc dù quá trình quản lý rủi ro thường được nêu theo trình tự, nhưng trong thực tế nó mang tính lặp lại.

6.2 Trao đổi thông tin và tham vấn

Mục đích của trao đổi thông tin và tham vấn là hỗ trợ các bên liên quan hiểu về rủi ro, về các cơ sở để ra quyết định và lý do tại sao cần các hành động cụ thể. Trao đổi thông tin hướng tới việc thúc đẩy nhận thức và hiểu về rủi ro, còn tham vấn đòi hỏi thu được phản hồi và thông tin để hỗ trợ việc ra quyết định. Phối hợp chặt chẽ cả hai sẽ làm cho việc trao đổi thông tin mang tính thực tiễn, kịp thời, sát thực, chính xác và dễ hiểu, có tính đến tính tin cậy, toàn vẹn của thông tin cũng như các quyền riêng tư của cá nhân.

Việc trao đổi thông tin và tham vấn với các bên liên quan thích hợp trong nội bộ và bên ngoài cần

thực hiện trong các bước và xuyên suốt tất cả các bước của quá trình quản lý rủi ro.

Trao đổi thông tin và tham vấn nhằm:

- đưa các lĩnh vực chuyên môn khác nhau vào từng bước của quá trình quản lý rủi ro;

- đảm bảo rằng các quan điểm khác nhau đều được xem xét một cách thích hợp khi xác định các tiêu chí rủi ro và khi định mức rủi ro;

- cung cấp thông tin đầy đủ để hỗ trợ việc giám sát rủi ro và ra quyết định;

- xây dựng ý thức về sự tham gia và quyền sở hữu trong số những người chịu ảnh hưởng của rủi ro.

6.3 Phạm vi, bối cảnh và tiêu chí

6.3.1 Khái quát

Mục đích của việc thiết lập phạm vi, bối cảnh và tiêu chí là để tùy chỉnh quá trình quản lý rủi ro, cho phép đánh giá rủi ro một cách hiệu lực và xử lý rủi ro một cách thích hợp. Phạm vi, bối cảnh và tiêu chí liên quan đến việc xác định phạm vi của quá trình và hiểu bối cảnh nội bộ, bên ngoài.

6.3.2 Xác định phạm vi

Tổ chức cần xác định phạm vi các hoạt động quản lý rủi ro của mình.

Vì quá trình quản lý rủi ro có thể được áp dụng ở các cấp khác nhau (ví dụ cấp chiến lược, tác nghiệp, chương trình, dự án hoặc các hoạt động khác), nên quan trọng là cần nêu rõ phạm vi được xem xét, các mục tiêu liên quan cần được xem xét và sự thống nhất của chúng với các mục tiêu của tổ chức.

Khi hoạch định cho cách tiếp cận này, các xem xét bao gồm:

- các mục tiêu và quyết định cần được thực hiện;

- các kết quả mong đợi từ các bước được thực hiện trong quá trình;

- thời gian, địa điểm, các nội dung cụ thể được đưa vào và được loại trừ;

- các công cụ và kỹ thuật đánh giá rủi ro thích hợp;

- nguồn lực cần thiết, các trách nhiệm và hồ sơ được lưu giữ;

- mối quan hệ với các dự án, quá trình và hoạt động khác.

6.3.3 Bối cảnh nội bộ và bên ngoài

Bối cảnh nội bộ và bên ngoài là môi trường mà tổ chức hướng tới để xác định và đạt được các mục tiêu của mình.

Bối cảnh của quá trình quản lý rủi ro cần được thiết lập từ sự hiểu biết về môi trường nội bộ và bên ngoài trong đó tổ chức hoạt động và cần phản ánh môi trường cụ thể của hoạt động mà theo đó quá trình quản lý rủi ro được áp dụng.

Hiểu bối cảnh rất quan trọng vì:

- quản lý rủi ro diễn ra trong bối cảnh của các mục tiêu và các hoạt động của tổ chức;

- các yếu tố từ phía tổ chức cũng có thể là nguồn rủi ro;

- mục đích và phạm vi của quá trình quản lý rủi ro có thể có mối quan hệ tương tác với các mục tiêu chung của tổ chức;

Tổ chức cần thiết lập bối cảnh nội bộ, bên ngoài của quá trình quản lý rủi ro thông qua việc xem xét các yếu tố được đề cập ở 5.4.1.

6.3.4 Xác định tiêu chí rủi ro

Tổ chức cần quy định số lượng và loại rủi ro mà mình được phép hoặc không được phép chấp nhận, liên quan đến các mục tiêu. Tổ chức cũng cần xác định các tiêu chí để đánh giá mức độ nghiêm trọng của rủi ro và để hỗ trợ các quá trình ra quyết định. Tiêu chí rủi ro cần thống nhất với khuôn khổ quản lý rủi ro và được điều chỉnh theo mục đích và phạm vi cụ thể của hoạt động đang được xem xét. Tiêu chí rủi ro cần phản ánh các giá trị, mục tiêu và nguồn lực của tổ chức và nhất quán với chính sách, các công bố về quản lý rủi ro. Các tiêu chí cần được xác định có tính đến các nghĩa vụ tuân thủ của tổ chức và quan điểm của các bên liên quan.

Mặc dù tiêu chí rủi ro cần được thiết lập khi bắt đầu quá trình đánh giá rủi ro, nhưng chúng mang tính động nên cần được xem xét và sửa đổi liên tục khi cần.

Để thiết lập tiêu chí rủi ro cần xem xét:

- bản chất và loại hình sự không chắc chắn có thể ảnh hưởng đến kết quả đầu ra và các mục tiêu (cả hữu hình và vô hình);

- cách thức các hệ quả (cả tích cực và tiêu cực) và khả năng xảy ra sẽ được xác định và đo lường;

- các yếu tố liên quan đến thời gian;

- tính nhất quán trong việc sử dụng các phép đo;

- cách thức định mức rủi ro;

- sự kết hợp và chuỗi rủi ro sẽ được xem xét như thế nào;

- khả năng của tổ chức.

6.4 Đánh giá rủi ro

6.4.1 Khái quát

Đánh giá rủi ro là quá trình tổng thể gồm nhận diện rủi ro, phân tích rủi ro và định mức rủi ro.

Đánh giá rủi ro cần được tiến hành một cách hệ thống, lặp lại và mang tính cộng tác, dựa trên kiến thức và quan điểm của các bên liên quan. Cần sử dụng thông tin sẵn có tốt nhất, được bổ sung bởi yêu cầu rộng hơn khi cần.

6.4.2 Nhận diện rủi ro

Mục đích của việc nhận diện rủi ro là phát hiện, ghi nhận và mô tả các rủi ro có thể giúp hoặc cản trở tổ chức đạt được các mục tiêu của mình. Thông tin có liên quan, thích hợp và cập nhật đều quan trọng trong việc nhận diện rủi ro.

Tổ chức có thể sử dụng nhiều kỹ thuật để nhận diện sự không chắc chắn có thể ảnh hưởng đến một hoặc nhiều mục tiêu. Các yếu tố sau và mối quan hệ giữa các yếu tố này, cần được xem xét:

- các nguồn rủi ro hữu hình và vô hình;

- nguyên nhân và các sự kiện;

- các mối đe dọa và các cơ hội;

- các yếu điểm và khả năng;

- những thay đổi trong bối cảnh nội bộ, bên ngoài;

- chỉ số về những rủi ro đang hình thành;

- tính chất và giá trị của các tài sản, nguồn lực;

- hệ quả và tác động của chúng tới các mục tiêu;

- những hạn chế về kiến thức và tính tin cậy của thông tin;

- các yếu tố liên quan đến thời gian;

- những định kiến, các giả định và niềm tin của những người liên quan.

Tổ chức cần nhận diện các rủi ro, cho dù nguồn rủi ro có thuộc kiểm soát của tổ chức hay không. Cần lưu ý rằng, có thể có nhiều loại kết quả đầu ra nên có thể dẫn đến sự đa dạng của các hệ quả hữu hình hoặc vô hình.

6.4.3 Phân tích rủi ro

Mục đích của phân tích rủi ro là hiểu bản chất của rủi ro và các đặc trưng của rủi ro bao gồm cả mức độ rủi ro, khi thích hợp. Phân tích rủi ro đòi hỏi việc xem xét một cách chi tiết sự không chắc chắn, các nguồn rủi ro, các hệ quả, khả năng xảy ra, các sự kiện, các kịch bản, các kiểm soát và hiệu lực của chúng. Một sự kiện có thể có nhiều nguyên nhân và hệ quả và có thể ảnh hưởng đến nhiều mục tiêu.

Phân tích rủi ro có thể được thực hiện với mức độ chi tiết và phức tạp khác nhau, tùy thuộc vào mục đích của phân tích, sự sẵn có, độ tin cậy của các thông tin và các nguồn lực sẵn có. Các kỹ thuật phân tích có thể định tính, định lượng hoặc kết hợp cả hai, tùy thuộc vào hoàn cảnh và mục đích sử dụng.

Phân tích rủi ro cần cân nhắc các yếu tố như:

- khả năng xảy ra của các sự kiện và hệ quả;

- bản chất và mức độ của các hệ quả;

- mức độ phức tạp và sự kết nối;

- các yếu tố liên quan đến thời gian và sự biến động;

- hiệu lực của các kiểm soát hiện có;

- mức độ nhạy cảm và tin cậy.

Phân tích rủi ro có thể bị ảnh hưởng bởi bất kỳ sự khác biệt về quan điểm, các định kiến, cảm nhận về rủi ro và các đánh giá. Các ảnh hưởng bổ sung còn có thể là chất lượng của các thông tin được sử

dụng, các giả định và những loại trừ đã được thực hiện, các hạn chế của các kỹ thuật và cách chúng được triển khai. Những ảnh hưởng này cần được cân nhắc, lập thành văn bản và trao đổi thông tin với những người ra quyết định.

Các sự kiện không chắc chắn ở mức cao có thể khó định lượng. Đây có thể là vấn đề khi phân tích các sự kiện có những hệ quả nghiêm trọng. Trong những trường hợp như vậy, việc sử dụng kết hợp các kỹ thuật thường cho cái nhìn thấu đáo, sâu sắc hơn.

Phân tích rủi ro cung cấp đầu vào cho việc định mức rủi ro, ra các quyết định về việc liệu rủi ro có cần được xử lý hay không, cách thức xử lý như thế nào và phương pháp và chiến lược xử lý rủi ro thích hợp nhất. Những kết quả này mang lại cái nhìn thấu đáo cho các quyết định, khi thực hiện các lựa chọn và các phương án liên quan đến các loại hình và mức độ rủi ro khác nhau.

6.4.4 Định mức rủi ro

Mục đích của việc định mức rủi ro là để hỗ trợ các quyết định. Định mức rủi ro đòi hỏi việc so sánh kết quả phân tích rủi ro với các tiêu chí rủi ro đã được thiết lập để xác định khi nào cần có hành động bổ sung. Điều này có thể dẫn đến quyết định:

- không làm gì thêm;

- cân nhắc các phương án xử lý rủi ro;

- tiến hành phân tích sâu hơn để hiểu rõ hơn về rủi ro;

- duy trì các kiểm soát hiện có;

- xem xét lại các mục tiêu.

Các quyết định cần tính đến bối cảnh rộng hơn và các hệ quả thực tế cũng như hệ quả được cảm nhận đối với các bên liên quan nội bộ và bên ngoài.

Kết quả định mức rủi ro cần được lưu hồ sơ, trao đổi thông tin và sau đó được xác nhận giá trị sử dụng ở các cấp thích hợp trong tổ chức.

6.5 Xử lý rủi ro

6.5.1 Khái quát

Mục đích của xử lý rủi ro là lựa chọn và thực hiện các phương án để giải quyết rủi ro.

Xử lý rủi ro liên quan đến quá trình lặp lại gồm:

- hình thành và lựa chọn các phương án xử lý rủi ro;

- hoạch định và thực hiện việc xử lý rủi ro;

- đánh giá hiệu lực của việc xử lý đó;

- quyết định xem rủi ro còn lại có chấp nhận được hay không;

- nếu không chấp nhận được, thực hiện xử lý tiếp.

6.5.2 Lựa chọn các phương án xử lý rủi ro

Để lựa chọn (các) phương án xử lý rủi ro thích hợp nhất đòi hỏi cân đối các lợi ích tiềm năng bắt nguồn từ việc đạt được các mục tiêu với các chi phí, các nỗ lực hoặc các bất lợi của việc thực hiện.

Các phương án xử lý rủi ro không nhất thiết loại trừ lẫn nhau hoặc phải thích hợp trong mọi hoàn cảnh. Các phương án xử lý rủi ro có thể bao gồm một hoặc nhiều nội dung sau:

- tránh rủi ro bằng cách quyết định không bắt đầu hoặc không tiếp tục hoạt động làm tăng rủi ro;

- chấp nhận hoặc làm tăng rủi ro để theo đuổi một cơ hội;

- loại bỏ nguồn rủi ro;

- thay đổi khả năng xảy ra;

- thay đổi hệ quả;

- chia sẻ rủi ro (ví dụ thông qua các hợp đồng, mua bảo hiểm);

- kiềm chế rủi ro bằng quyết định đúng đắn.

Lý giải cho việc xử lý rủi ro rộng hơn so với việc chỉ xem xét về mặt kinh tế và cần tính đến tất cả các nghĩa vụ tuân thủ của tổ chức, các cam kết tự nguyện và quan điểm của các bên liên quan. Việc lựa chọn các phương án xử lý rủi ro cần được thực hiện phù hợp với các mục tiêu, các tiêu chí rủi ro và các nguồn lực sẵn có của tổ chức.

Khi lựa chọn các phương án xử lý rủi ro, tổ chức cần cân nhắc các giá trị, cảm nhận và khả năng tham gia của các bên liên quan, những cách thích hợp nhất để trao đổi thông tin và tham vấn các bên liên quan. Mặc dù có hiệu lực như nhau nhưng việc xử lý rủi ro có thể dễ chấp nhận hơn đối với một

số bên liên quan so với một số bên khác.

Việc xử lý rủi ro, ngay cả khi nó được thiết kế và triển khai thận trọng cũng có thể không mang lại kết quả mong đợi và có thể gây ra những hệ quả không mong muốn. Do vậy, việc theo dõi và xem xét cần là một phần không thể thiếu khi thực hiện xử lý rủi ro nhằm đảm bảo rằng các hình thức xử lý khác nhau đều đạt được hiệu lực.

Bản thân việc xử lý rủi ro cũng có thể tạo ra những rủi ro mới cần được quản lý.

Nếu không sẵn có phương án xử lý hoặc nếu các phương án xử lý không điều chỉnh được một cách đầy đủ rủi ro đó, thì rủi ro cần được ghi nhận và đảm bảo việc xem xét liên tục rủi ro đó.

Những người ra quyết định và các bên liên quan khác cần có nhận thức về bản chất và mức độ rủi ro còn lại sau khi xử lý rủi ro. Rủi ro còn lại cần được lập thành văn bản và chịu sự theo dõi, xem xét và nếu thích hợp, xử lý tiếp.

6.5.3 Chuẩn bị và thực hiện các kế hoạch xử lý rủi ro

Mục đích của các kế hoạch xử lý rủi ro là quy định cách thức phương án xử lý đã được lựa chọn sẽ được triển khai sao cho các sắp đặt đều được hiểu bởi những người liên quan và tiến trình so với kế hoạch đó có thể được theo dõi. Kế hoạch xử lý cần xác định rõ ràng trình tự theo đó việc xử lý rủi ro cần được thực hiện.

Các kế hoạch xử lý cần được tích hợp vào các kế hoạch và các quá trình quản lý của tổ chức có sự tham vấn với các bên liên quan thích hợp.

Thông tin được nêu trong kế hoạch xử lý cần bao gồm:

- lý do lựa chọn các phương án xử lý, kể cả các lợi ích dự kiến đạt được;

- những người chịu trách nhiệm và trách nhiệm giải trình đối với việc phê duyệt và triển khai kế hoạch;

- các hành động được đề xuất;

- các nguồn lực cần thiết, bao gồm cả dự phòng;

- các thước đo kết quả thực hiện;

- các ràng buộc;

- việc báo cáo và theo dõi cần thiết;

- khi nào các hành động dự kiến sẽ được thực hiện và hoàn thành.

6.6 Theo dõi và xem xét

Mục đích của theo dõi và xem xét là đảm bảo và cải tiến chất lượng, hiệu lực của việc thiết kế, áp dụng và các kết quả của quá trình. Theo dõi liên tục và xem xét định kỳ về quá trình quản lý rủi ro và những kết quả đầu ra của nó cần là một phần được hoạch định của quá trình quản lý rủi ro, gắn với các trách nhiệm đã được xác định rõ ràng.

Việc theo dõi và xem xét cần được thực hiện trong tất cả các giai đoạn của quá trình. Theo dõi và xem xét bao gồm hoạch định, thu thập và phân tích thông tin, ghi nhận các kết quả và cung cấp thông tin phản hồi.

Các kết quả theo dõi và xem xét cần được kết hợp với toàn bộ hoạt động quản lý kết quả thực hiện, đo lường và báo cáo của tổ chức.

6.7 Lập hồ sơ và báo cáo

Quá trình quản lý rủi ro và các kết quả của nó cần được lập thành văn bản và báo cáo thông qua các cơ chế thích hợp. Việc lập hồ sơ và báo cáo nhằm:

- trao đổi thông tin về các hoạt động quản lý rủi ro và kết quả trong toàn tổ chức;

- cung cấp thông tin cho việc ra quyết định;

- cải tiến hoạt động quản lý rủi ro;

- hỗ trợ việc tương tác với các bên liên quan, bao gồm cả những người có trách nhiệm và trách nhiệm giải trình đối với các hoạt động quản lý rủi ro.

Các quyết định liên quan đến việc tạo lập, lưu giữ và xử lý thông tin dạng văn bản cần tính đến, nhưng không giới hạn ở việc sử dụng chúng, tính nhạy cảm của thông tin và bối cảnh nội bộ, bên ngoài.

Báo cáo là một phần không thể thiếu trong việc điều hành của tổ chức và nó cần nâng cao chất lượng việc đối thoại với các bên liên quan, hỗ trợ lãnh đạo cao nhất, bộ phận giám sát trong việc thực hiện các trách nhiệm của họ. Các yếu tố cần xem xét khi báo cáo bao gồm, nhưng không giới hạn ở:

- các bên liên quan khác nhau và nhu cầu và yêu cầu về thông tin cụ thể của họ;

- chi phí, tần suất và thời điểm báo cáo;
- phương pháp báo cáo;
- sự phù hợp của thông tin với các mục tiêu và việc ra quyết định của tổ chức.

Thư mục tài liệu tham khảo

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

MỤC LỤC