

TIÊU CHUẨN QUỐC GIA

TCVN 31000:2011

ISO 31000:2009

QUẢN LÝ RỦI RO - NGUYÊN TẮC VÀ HƯỚNG DẪN

Risk management - Principles and Guidelines

Lời nói đầu

TCVN ISO 31000:2011 hoàn toàn tương đương với ISO 31000:2009;

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

Mọi loại hình tổ chức, dù lớn hay nhỏ, đều phải đối mặt với các yếu tố và ảnh hưởng cả bên trong và bên ngoài làm cho tổ chức không chắc chắn liệu mình có đạt được mục tiêu hay không và khi nào sẽ đạt được mục tiêu. Tác động của sự không chắc chắn này lên các mục tiêu của một tổ chức chính là "rủi ro".

Mọi hoạt động của một tổ chức đều có rủi ro. Tổ chức quản lý rủi ro bằng cách xác định, phân tích và đánh giá xem liệu có cần thay đổi rủi ro bằng cách xử lý rủi ro để đáp ứng tiêu chí rủi ro của tổ chức hay không. Trong toàn bộ quá trình này, tổ chức trao đổi thông tin và tham vấn các bên liên quan, theo dõi, xem xét rủi ro và các kiểm soát thay đổi rủi ro nhằm bảo đảm rằng không cần xử lý rủi ro thêm nữa. Tiêu chuẩn này mô tả chi tiết quá trình có tính hệ thống và lô gíc này.

Trong khi tất cả các tổ chức đều quản lý rủi ro ở một mức độ nào đó, tiêu chuẩn này thiết lập một số nguyên tắc cần được đáp ứng để làm cho hoạt động quản lý rủi ro đạt hiệu quả. Tiêu chuẩn này khuyến nghị tổ chức xây dựng, áp dụng và cải tiến liên tục khuôn khổ với mục đích là tích hợp quá trình quản lý rủi ro với toàn bộ hoạt động quản trị, chiến lược và hoạch định, quản lý, các quá trình báo cáo, chính sách, các giá trị và văn hóa của tổ chức.

Quản lý rủi ro có thể được áp dụng cho toàn bộ tổ chức, ở nhiều lĩnh vực và cấp độ, tại mọi thời điểm, cũng như cho các chức năng, dự án và hoạt động cụ thể.

Mặc dù thực tiễn quản lý rủi ro đã được phát triển theo thời gian và trong nhiều lĩnh vực để đáp ứng các nhu cầu đa dạng, nhưng việc chấp nhận các quá trình nhất quán trong một khuôn khổ toàn diện có thể giúp đảm bảo rằng việc quản lý rủi ro đạt hiệu lực, hiệu quả và chặt chẽ trong toàn bộ tổ chức. Phương pháp tiếp cận chung mô tả trong tiêu chuẩn này đưa ra các nguyên tắc và hướng dẫn để quản lý mọi loại hình rủi ro một cách hệ thống, minh bạch và đáng tin cậy cũng như trong mọi lĩnh vực và bối cảnh.

Mỗi lĩnh vực hoặc ứng dụng quản lý rủi ro cụ thể đều có những nhu cầu, đối tượng, nhận thức và tiêu chí riêng của nó. Vì vậy, một yếu tố quan trọng của tiêu chuẩn này là việc đưa "thiết lập bối cảnh" thành một hoạt động khởi đầu của quá trình quản lý rủi ro chung. Thiết lập bối cảnh sẽ nắm bắt được các mục tiêu của tổ chức, môi trường mà tổ chức theo đuổi những mục tiêu này, các bên liên quan và sự đa dạng của tiêu chí rủi ro - tất cả những điều này sẽ giúp phát hiện, đánh giá bản chất và tính phức tạp rủi ro của tổ chức.

Mối quan hệ giữa các nguyên tắc quản lý rủi ro, khuôn khổ trong đó mối quan hệ này diễn ra và quá trình quản lý rủi ro được mô tả trong tiêu chuẩn này được thể hiện tại Hình 1.

Khi thực hiện và duy trì theo tiêu chuẩn này, quản lý rủi ro cho phép một tổ chức có thể, ví dụ:

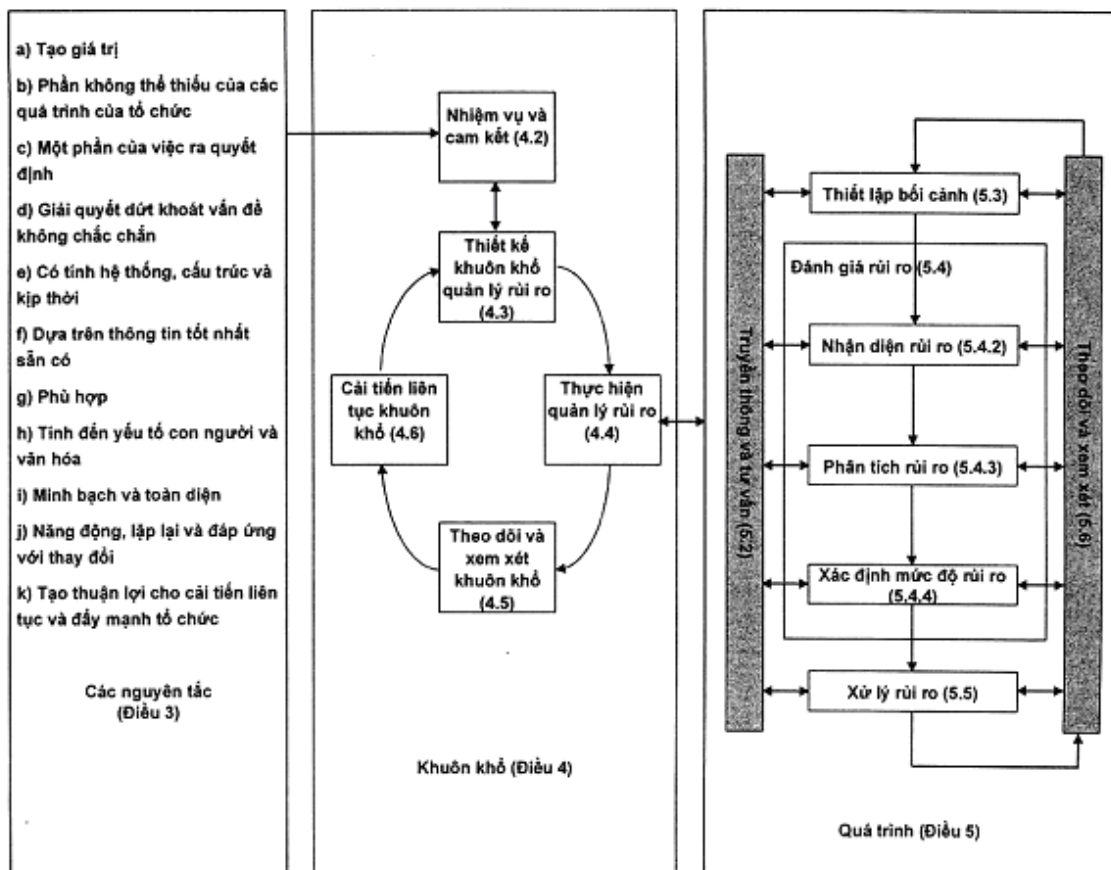
- tăng khả năng đạt được các mục tiêu;
- khuyến khích quản lý chủ động;
- nhận thức được nhu cầu xác định và xử lý rủi ro trong toàn tổ chức;
- cải thiện việc xác định các cơ hội và mối đe dọa;
- tuân thủ các yêu cầu luật định, chế định và các chuẩn mực quốc tế liên quan;
- cải tiến việc lập báo cáo tự nguyện và bắt buộc;
- cải tiến việc quản trị;
- nâng cao lòng tin và sự tin tưởng của các bên liên quan;
- thiết lập cơ sở tin cậy cho việc ra quyết định và lập kế hoạch;
- cải tiến việc kiểm soát;
- phân bổ và sử dụng hiệu quả các nguồn lực để xử lý rủi ro;

- cải tiến hiệu lực và hiệu quả hoạt động;
- nâng cao hoạt động đảm bảo an toàn và sức khỏe, cũng như bảo vệ môi trường;
- cải tiến việc ngăn ngừa tổn thất và quản lý sự cố;
- giảm thiểu thiệt hại;
- nâng cao việc học hỏi trong tổ chức; và
- nâng cao tính kiên cường của tổ chức.

Tiêu chuẩn này nhằm đáp ứng nhu cầu của một loạt các bên liên quan, bao gồm:

- những người chịu trách nhiệm xây dựng chính sách quản lý rủi ro trong tổ chức;
- những người có trách nhiệm đảm bảo rằng rủi ro được quản lý hiệu quả trong phạm vi toàn bộ tổ chức hoặc trong một lĩnh vực, dự án hay hoạt động cụ thể.
- những người cần đánh giá hiệu lực quản lý rủi ro của tổ chức; và
- những người xây dựng tiêu chuẩn, hướng dẫn, thủ tục và quy phạm thực hành, trong đó toàn bộ hoặc một phần, lập ra cách thức quản lý rủi ro trong bối cảnh cụ thể của các tài liệu này.

Các quá trình và thực tiễn quản lý hiện hành của nhiều tổ chức bao gồm các thành phần của quản lý rủi ro và nhiều tổ chức đã chấp nhận một quá trình quản lý rủi ro chính thức cho các loại rủi ro và tình huống cụ thể. Trong những trường hợp này, tổ chức có thể quyết định tiến hành xem xét thực tiễn và các quá trình hiện có của mình theo tiêu chuẩn này.



Hình 1 - Quan hệ giữa nguyên tắc, khuôn khổ và quá trình quản lý rủi ro.

QUẢN LÝ RỦI RO - NGUYÊN TẮC VÀ HƯỚNG DẪN

Risk management - Principles and Guidelines

1. Phạm vi áp dụng

Tiêu chuẩn này đưa ra các nguyên tắc và hướng dẫn chung về quản lý rủi ro.

Tiêu chuẩn này có thể được sử dụng cho doanh nghiệp công, tư hay doanh nghiệp cộng đồng, hiệp hội, nhóm hoặc cá nhân. Vì vậy, tiêu chuẩn này không cụ thể cho bất kỳ ngành công nghiệp hoặc lĩnh vực nào.

CHÚ THÍCH: Để thuận tiện, tất cả những đối tượng khác nhau sử dụng tiêu chuẩn này đều được gọi bằng thuật ngữ chung "tổ chức".

Tiêu chuẩn này có thể được áp dụng trong toàn bộ thời gian tồn tại của tổ chức, cho một loạt các hoạt động, bao gồm các chiến lược và quyết định, vận hành, quá trình, chức năng, dự án, sản phẩm, dịch vụ và tài sản.

Tiêu chuẩn này có thể được áp dụng cho mọi loại hình rủi ro, bất kể bản chất, có hệ quả tích cực hay tiêu cực.

Mặc dù tiêu chuẩn này đưa ra các hướng dẫn chung, nó không nhằm tạo nên sự đồng nhất trong quản lý rủi ro ở tất cả các tổ chức. Việc thiết kế và thực hiện các khuôn khổ và kế hoạch quản lý rủi ro cần phải tính đến các nhu cầu khác nhau của một tổ chức cụ thể, mục tiêu cụ thể, bối cảnh, cơ cấu, hoạt động, quá trình, chức năng, các dự án, sản phẩm, dịch vụ hoặc tài sản và các công việc cụ thể được triển khai.

Tiêu chuẩn này được sử dụng để hài hòa các quá trình quản lý rủi ro trong các tiêu chuẩn hiện tại và tương lai. Tiêu chuẩn này đưa ra một cách tiếp cận chung để hỗ trợ các tiêu chuẩn đề cập đến những rủi ro và/hoặc các lĩnh vực cụ thể chứ không thay thế cho các tiêu chuẩn đó.

Tiêu chuẩn này không sử dụng cho mục đích chứng nhận.

2. Thuật ngữ và định nghĩa

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

2.1. Rủi ro (Risk)

Tác động của sự không chắc chắn lên mục tiêu.

CHÚ THÍCH 1: Tác động là một sai lệch so với dự kiến - tích cực và/hoặc tiêu cực.

CHÚ THÍCH 2: Mục tiêu có thể có những khía cạnh khác nhau (như mục tiêu tài chính, sức khỏe, an toàn và môi trường) và có thể áp dụng ở các cấp độ khác nhau (như chiến lược, toàn bộ tổ chức, dự án, sản phẩm và quá trình).

CHÚ THÍCH 3: Rủi ro thường đặc trưng bởi sự dẫn chiếu đến các **sự kiện** (2.17) và **hệ quả** (2.18) tiềm ẩn, hoặc sự kết hợp giữa chúng.

CHÚ THÍCH 4: Rủi ro thường thể hiện bằng sự kết nối giữa các hệ quả của một sự kiện (bao gồm cả những thay đổi về hoàn cảnh) và **khả năng xảy ra** (2.19) kèm theo.

CHÚ THÍCH 5: Sự không chắc chắn là tình trạng, thậm chí là một phần, sự thiếu hụt thông tin liên quan tới việc hiểu biết hoặc nhận thức về một sự kiện, hệ quả, hoặc khả năng xảy ra của nó.

[ISO Guide 73:2009, định nghĩa 1.1]

2.2. Quản lý rủi ro (Risk management)

Các hoạt động điều phối để định hướng và kiểm soát một tổ chức về mặt **rủi ro** (2.1).

[ISO Guide 73:2009, định nghĩa 2.1]

2.3. Khuôn khổ quản lý rủi ro (Risk management framework)

Tập hợp các thành phần tạo nền tảng và sự sắp xếp của tổ chức để thiết kế, thực hiện, **theo dõi** (2.28), xem xét và cải tiến liên tục quản lý **rủi ro** (2.2) trong toàn tổ chức.

CHÚ THÍCH 1: Nền tảng bao gồm chính sách, mục tiêu, nghĩa vụ và cam kết để quản lý **rủi ro** (2.1).

CHÚ THÍCH 2: Sự sắp xếp về mặt tổ chức bao gồm các kế hoạch, mối quan hệ, trách nhiệm, nguồn lực, quá trình và hoạt động.

CHÚ THÍCH 3: Khuôn khổ quản lý rủi ro được đưa vào chính sách chiến lược và chiến thuật tổng thể cũng như thực tiễn hoạt động của tổ chức.

[ISO Guide 73:2009, định nghĩa 2.1.1]

2.4. Chính sách quản lý rủi ro (Risk management policy)

Tuyên bố về ý định và định hướng tổng thể của tổ chức liên quan đến **quản lý rủi ro** (2.2).

[ISO Guide 73:2009, định nghĩa 2.1.2]

2.5. Thái độ đối với rủi ro (Risk attitude)

Phương pháp tiếp cận của tổ chức để đánh giá và cuối cùng là theo đuổi, kiểm chế, đối mặt hoặc né tránh **rủi ro** (2.1).

[ISO Guide 73:2009, định nghĩa 3.7.1.1]

2.6. Kế hoạch quản lý rủi ro (Risk management plan)

Chương trình trong phạm vi **khuôn khổ quản lý rủi ro** (2.3) quy định phương pháp tiếp cận, các yếu tố của quản lý và nguồn lực sử dụng cho việc quản lý **rủi ro** (2.1).

CHÚ THÍCH 1: Các yếu tố quản lý thường bao gồm các thủ tục, hoạt động thực tiễn, phân công trách nhiệm, trình tự và thời gian của các hoạt động.

CHÚ THÍCH 2: Kế hoạch quản lý rủi ro có thể áp dụng cho một sản phẩm, quá trình và dự án cụ thể, cho một phần hoặc toàn bộ tổ chức.

[ISO Guide 73:2009, định nghĩa 2.3.1]

2.7. Chủ sở hữu rủi ro (Risk owner)

Người hoặc thực thể có trách nhiệm và thẩm quyền quản lý một **rủi ro** (2.1)

[ISO Guide 73:2009, định nghĩa 3.5.1.5]

2.8. Quá trình quản lý rủi ro (Risk management process)

Việc áp dụng một cách hệ thống các chính sách, thủ tục và thực tiễn quản lý đối với các hoạt động trao đổi thông tin, tư vấn, thiết lập bối cảnh và xác định, phân tích, xác định mức độ, xử lý, **theo dõi** (2.28) và xem xét **rủi ro** (2.1).

[ISO Guide 73:2009, định nghĩa 3.1]

2.9. Thiết lập bối cảnh (Establishing the context)

Xác định các tham số bên ngoài và nội bộ cần tính đến khi quản lý rủi ro và thiết lập phạm vi và **tiêu chí rủi ro** (2.22) cho **chính sách quản lý rủi ro** (2.4).

2.10. Bối cảnh bên ngoài (External context)

Môi trường bên ngoài ở đó tổ chức theo đuổi để đạt được các mục tiêu của mình.

CHÚ THÍCH: Bối cảnh bên ngoài có thể bao gồm:

- môi trường văn hóa, xã hội, chính trị, pháp lý, chế định, tài chính, công nghệ, kinh tế, tự nhiên và cạnh tranh, dù là quốc tế, quốc gia, khu vực hoặc địa phương;
- các xu hướng và động lực chính tác động đến mục tiêu của tổ chức; và
- mối quan hệ, nhận thức và giá trị của các **bên liên quan** (2.13) bên ngoài.

[ISO Guide 73:2009, định nghĩa 3.3.1.1]

2.11. Bối cảnh nội bộ (Internal context)

Môi trường bên trong ở đó tổ chức theo đuổi để đạt được các mục tiêu của mình.

CHÚ THÍCH: Bối cảnh nội bộ có thể bao gồm:

- quản trị, cơ cấu tổ chức, vai trò và trách nhiệm;
- các chính sách, mục tiêu và chiến lược được đặt ra để đạt mục tiêu;
- khả năng, sự am hiểu về nguồn lực và kiến thức (ví dụ vốn, thời gian, con người, quá trình, hệ thống và công nghệ);
- các hệ thống thông tin, luồng thông tin và các quá trình ra quyết định (cả chính thức và không chính thức);
- mối quan hệ, nhận thức và giá trị của các bên liên quan trong tổ chức;
- văn hóa của tổ chức;
- các tiêu chuẩn, hướng dẫn và mô hình được tổ chức áp dụng; và
- hình thức và mức độ của các mối quan hệ hợp đồng.

[ISO Guide 73:2009, định nghĩa 3.3.1.2]

2.12. Trao đổi thông tin và tham vấn (Communication and consultation)

Quá trình liên tục và lặp đi lặp lại được tổ chức thực hiện để cung cấp, chia sẻ hoặc có được thông tin và để tham gia vào đối thoại với các **bên liên quan** (2.13) về quản lý **rủi ro** (2.1).

CHỈ THÍCH 1: Thông tin có thể liên quan đến sự tồn tại, bản chất, hình thức, **khả năng xảy ra** (2.19), ý nghĩa, xác định mức độ, khả năng chấp nhận và xử lý của quản lý rủi ro.

CHỈ THÍCH 2: Tư vấn là một quá trình trao đổi thông tin hai chiều giữa tổ chức và các bên liên quan về một vấn đề trước khi đưa ra quyết định hoặc xác định định hướng về vấn đề đó. Tư vấn là:

- một quá trình tác động lên quyết định thông qua ảnh hưởng hơn là quyền lực; và
- đầu vào để ra quyết định, chứ không tham gia vào việc ra quyết định.

[ISO Guide 73:2009, định nghĩa 3.2.1]

2.13. Bên liên quan (Stakeholder)

Người hoặc tổ chức có thể gây ảnh hưởng, chịu ảnh hưởng hoặc tự nhận thấy bị ảnh hưởng bởi một quyết định hay hoạt động.

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

[ISO Guide 73:2009, định nghĩa 3.2.1.1]

2.14. Đánh giá rủi ro (Risk assessment)

Quá trình tổng thể **nhận diện rủi ro** (2.15), **phân tích rủi ro** (2.21) và **xác định mức độ rủi ro** (2.24).

[ISO Guide 73:2009, định nghĩa 3.4.1]

2.15. Nhận diện rủi ro (Risk identification)

Quá trình tìm kiếm, nhận biết và mô tả rủi ro (2.1).

CHÚ THÍCH 1: Việc xác định rủi ro đòi hỏi phải xác định các **nguồn rủi ro** (2.16), **sự kiện** (2.17), nguyên nhân và **hệ quả** (2.18) tiềm ẩn của chúng.

CHÚ THÍCH 2: Xác định rủi ro có thể cần phân tích dữ liệu quá khứ, lý thuyết, ý kiến chuyên môn có hiểu biết và nhu cầu của các **bên liên quan** (2.13).

[ISO Guide 73:2009, định nghĩa 3.5.1]

2.16. Nguồn rủi ro (Risk source)

Yếu tố mà tự nó hoặc khi kết hợp, có tiềm năng nội tại để làm phát sinh **rủi ro** (2.1).

CHÚ THÍCH: Nguồn rủi ro có thể hữu hình hoặc vô hình.

[ISO Guide 73:2009, định nghĩa 3.5.1.2]

2.17. 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.

CHÚ THÍCH 2: Một sự kiện có thể bao gồm một việc gì đó không xảy ra.

CHÚ THÍCH 3: Một sự kiện đôi khi có thể được gọi là một "sự cố" hay "tai nạn".

CHÚ THÍCH 4: Một sự kiện mà không có **hệ quả** (2.18) cũng có thể được gọi là "thoát nạn" hoặc "thoát hiểm".

[ISO Guide 73:2009, định nghĩa 3.5.1.3]

2.18. Hệ quả (Consequence)

Kết quả của một **sự kiện** (2.17) ảnh hưởng đến các mục tiêu.

CHÚ THÍCH 1: Một sự kiện có thể dẫn đến một loạt các hệ quả

CHÚ THÍCH 2: 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 3: Hệ quả có thể biểu thị định tính hoặc định lượng.

CHÚ THÍCH 4: Hệ quả ban đầu có thể tăng theo các hiệu ứng dây chuyền.

[ISO Guide 73:2009, định nghĩa 3.6.1.3]

2.19. Khả năng xảy ra (Likelihood)

Cơ hội xảy ra một điều gì đó.

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

[ISO Guide 73:2009, định nghĩa 3.6.1.1]

2.20. Đặc trưng của rủi ro (Risk profile)

Mô tả của tập hợp các **rủi ro** (2.1) bất kỳ.

CHÚ THÍCH: Tập hợp các rủi ro có thể bao gồm những rủi ro liên quan đến toàn bộ tổ chức, bộ phận của tổ chức, hoặc phân xác định khác.

[ISO Guide 73:2009, định nghĩa 3.8.2.5]

2.21. Phân tích rủi ro (Risk analysis)

Quá trình tìm hiểu bản chất của **rủi ro** (2.1) và xác định **mức rủi ro** (2.23).

CHÚ THÍCH 1: Phân tích rủi ro cung cấp cơ sở để **xác định mức độ rủi ro** (2.24) và quyết định về **xử lý rủi ro** (2.25).

CHÚ THÍCH 2: Phân tích rủi ro bao gồm cả ước lượng rủi ro.

[ISO Guide 73:2009, định nghĩa 3.6.1]

2.22. Tiêu chí rủi ro (Risk criteria)

Điều khoản tham chiếu dựa vào đó xác định mức độ nghiêm trọng của **rủi ro** (2.1)

CHÚ THÍCH 1: Tiêu chí rủi ro dựa vào các mục tiêu của tổ chức, bối cảnh **bên ngoài** (2.10) và **bối cảnh nội bộ** (2.21).

CHÚ THÍCH 2: Tiêu chí rủi ro có thể bắt nguồn từ các tiêu chuẩn, luật, chính sách và các yêu cầu khác.

[ISO Guide 73:2009, định nghĩa 3.3.1.3]

2.23. Mức rủi ro (Level of risk)

Mức độ của một **rủi ro** (2.1) hay một tập hợp các rủi ro, thể hiện bằng sự kết hợp các **hệ quả** (2.18) và **khả năng xảy ra** (2.19) của chúng.

[ISO Guide 73:2009, định nghĩa 3.6.1.8]

2.24. Xác định mức độ rủi ro (Risk evaluation)

Quá trình so sánh kết quả **phân tích rủi ro** (2.21) với các **tiêu chí rủi ro** (2.22) để xác định xem **rủi ro** (2.1) và/hoặc mức độ của nó có thể chấp nhận hay chịu đựng được hay không.

CHÚ THÍCH: Xác định mức độ rủi ro hỗ trợ trong quyết định về **xử lý rủi ro** (2.25).

[ISO Guide 73:2009, định nghĩa 3.7.1]

2.25. Xử lý rủi ro (Risk treatment)

Quá trình thay đổi **rủi ro** (2.1).

CHÚ THÍCH 1: Xử lý rủi ro có thể liên quan đến:

- tránh rủi ro bằng cách quyết định không bắt đầu hoặc tiếp tục hoạt động làm phát sinh rủi ro;
- đối mặt hoặc làm tăng rủi ro để theo đuổi một cơ hội;
- loại bỏ **nguồn rủi ro** (2.16);
- thay đổi **khả năng xảy ra** (2.19);
- thay đổi **hệ quả** (2.18);
- chia sẻ rủi ro với một bên hoặc nhiều bên khác (bao gồm hợp đồng và tài trợ rủi ro); và
- kiểm chế rủi ro bằng quyết định đúng đắn.

CHÚ THÍCH 2: Xử lý rủi ro đối với những hệ quả tiêu cực khi được gọi là "giảm nhẹ rủi ro", "loại bỏ rủi ro", "ngăn ngừa rủi ro" và "giảm bớt rủi ro".

CHÚ THÍCH 3: Xử lý rủi ro có thể tạo ra những rủi ro mới hoặc làm thay đổi những rủi ro hiện có.

[ISO Guide 73:2009, định nghĩa 3.8.1]

2.26. Kiểm soát (control)

Biện pháp làm thay đổi **rủi ro** (2.1).

CHÚ THÍCH 1: Kiểm soát bao gồm mọi quá trình, chính sách, thiết bị, thực tiễn, hoặc hành động khác làm thay đổi rủi ro.

CHÚ THÍCH 2: Kiểm soát có thể không luôn tạo ra tác dụng thay đổi theo dự kiến hoặc giả định.

[ISO Guide 73:2009, định nghĩa 3.8.1.1]

2.27. Rủi ro tồn đọng (Residual risk)

Rủi ro (2.1) còn lại sau khi **xử lý rủi ro** (2.25).

CHÚ THÍCH 1: Rủi ro tồn đọng có thể gồm rủi ro chưa được nhận diện.

CHÚ THÍCH 2: Rủi ro tồn đọng cũng có thể được gọi là "rủi ro còn lại".

[ISO Guide 73:2009, định nghĩa 3.8.1.6]

2.28. Theo dõi (Monitoring)

Kiểm tra, giám sát liên tục, quan sát nghiêm ngặt hoặc xác định tình trạng nhằm nhận biết thay đổi so với mức độ thực hiện yêu cầu hoặc mong đợi.

CHÚ THÍCH: Theo dõi có thể được áp dụng cho một **khuôn khổ quản lý rủi ro** (2.3), **quá trình quản lý rủi ro** (2.8), **rủi ro** (2.1) hoặc **kiểm soát** (2.26).

[ISO Guide 73:2009, định nghĩa 3.8.2.1]

2.29. Xem xét (Review)

Hoạt động thực hiện để xác định sự phù hợp, thỏa đáng và hiệu quả vấn đề liên quan để đạt được mục tiêu đề ra.

CHÚ THÍCH: Xem xét có thể được áp dụng cho một **khuôn khổ quản lý rủi ro** (2.3), **quá trình quản lý rủi ro** (2.8), **rủi ro** (2.1) hoặc **kiểm soát** (2.26).

[ISO Guide 73:2009, định nghĩa 3.8.2.2]

3. Nguyên tắc

Để quản lý rủi ro có hiệu quả, tất cả các cấp của một tổ chức cần tuân thủ những nguyên tắc dưới đây.

a) Quản lý rủi ro tạo ra và bảo vệ giá trị.

Quản lý rủi ro góp phần vào việc đạt được mục tiêu và cải tiến việc thực hiện, như an toàn và sức khỏe con người, an ninh, tuân thủ luật định và chế định, sự chấp nhận của công chúng, bảo vệ môi trường, chất lượng sản phẩm, quản lý dự án, hiệu quả hoạt động, quản trị và uy tín.

b) Quản lý rủi ro là một phần không thể thiếu của tất cả các quá trình của tổ chức.

Quản lý rủi ro không phải là một hoạt động độc lập, tách biệt với các hoạt động và quá trình chính của tổ chức. Quản lý rủi ro là một phần trong trách nhiệm quản lý và là phần không thể thiếu trong tất cả các quá trình của tổ chức, bao gồm các quá trình hoạch định chiến lược, tất cả các dự án và quản lý thay đổi.

c) Quản lý rủi ro là một phần của việc ra quyết định.

Quản lý rủi ro giúp những người ra quyết định đưa ra những lựa chọn sáng suốt, hành động ưu tiên và phân biệt giữa các kế hoạch hành động thay thế.

d) Quản lý rủi ro đặc biệt chú trọng những vấn đề không chắc chắn.

Quản lý rủi ro tính đến sự không chắc chắn, bản chất của sự không chắc chắn và cách thức giải quyết.

e) Quản lý rủi ro có tính hệ thống, cấu trúc và kịp thời.

Phương pháp tiếp cận kịp thời, có cấu trúc và mang tính hệ thống của quản lý rủi ro tạo ra hiệu quả và các kết quả nhất quán, có thể so sánh được và đáng tin cậy.

f) Quản lý rủi ro dựa trên những thông tin tốt nhất sẵn có.

Đầu vào cho quá trình quản lý rủi ro dựa trên các nguồn thông tin như dữ liệu quá khứ, kinh nghiệm, phản hồi của các bên liên quan, quan trắc, dự báo và phán đoán của chuyên gia. Tuy nhiên, những người ra quyết định nên tự tìm hiểu, xem xét bất kỳ hạn chế nào về dữ liệu hay mô hình được sử dụng hoặc khả năng bất đồng giữa các chuyên gia.

g) Quản lý rủi ro cần phù hợp.

Quản lý rủi ro phù hợp với bối cảnh bên trong và bên ngoài của tổ chức và đặc trưng của rủi ro.

h) Quản lý rủi ro có tính đến các yếu tố con người và văn hóa.

Quản lý rủi ro thừa nhận khả năng, nhận thức và ý định của mọi người bên trong và bên ngoài tổ chức có thể tạo thuận lợi hoặc cản trở việc đạt được mục tiêu của tổ chức.

i) Quản lý rủi ro cần minh bạch và có sự tham gia của các bên.

Việc tham gia thích hợp và kịp thời của các bên liên quan, đặc biệt là những người ra quyết định ở các cấp của tổ chức, đảm bảo rằng việc quản lý rủi ro do duy trì sự phù hợp và cập nhật. Việc tham gia này cũng cho phép các bên liên quan có được sự đại diện thích hợp và quan điểm của họ được xem xét khi xác định tiêu chí rủi ro.

j) Quản lý rủi ro cần năng động, lặp lại và đáp ứng với sự thay đổi

Việc quản lý rủi ro cảm nhận và đáp ứng liên tục với thay đổi. Vì các sự kiện nội bộ và bên ngoài xảy ra, bối cảnh và kiến thức thay đổi, việc theo dõi và xem xét rủi ro diễn ra, những rủi ro mới xuất hiện, một số rủi ro thay đổi và những rủi ro khác biến mất.

k) Quản lý rủi ro tạo thuận lợi cho việc cải tiến liên tục của tổ chức.

Tổ chức cần xây dựng và thực hiện các chiến lược để nâng cao sự nhuần nhuyễn trong việc quản lý rủi ro của mình cùng với tất cả các khía cạnh khác của tổ chức.

Phụ lục A cung cấp thêm chỉ dẫn cho các tổ chức mong muốn quản lý rủi ro có hiệu quả hơn.

MỤC LỤC

Lời nói đầu

Lời giới thiệu

1. Phạm vi áp dụng

2. Thuật ngữ và định nghĩa

3. Nguyên tắc

4. Khuôn khổ

4.1. Khái quát

4.2. Nhiệm vụ và cam kết

4.3. Thiết kế khuôn khổ quản lý rủi ro

4.4. Thực hiện quản lý rủi ro

4.5. Theo dõi và xem xét khuôn khổ

4.6. Cải tiến liên tục khuôn khổ

5. Quá trình

5.1. Khái quát

5.2 Trao đổi thông tin và tham vấn

5.3. Thiết lập bối cảnh

5.4. Đánh giá rủi ro

5.5. Xử lý rủi ro

5.6. Theo dõi và xem xét

5.7. Lập hồ sơ quá trình quản lý rủi ro

Phụ lục A (tham khảo) Các thuộc tính của Quản lý rủi ro nâng cao

Thư mục tài liệu tham khảo