**TCVN** TIÊU CHUẨN QUỐC GIA

# TCVN ISO 31000: 2011

# ISO 31000:2009

Xuất bản lần 1

# QUẢN LÝ RỦI RO – NGUYÊN TẮC VÀ HƯỚNG DẪN

***Risk management- Principles and Guidelines***

HÀ NỘI - 2011

## Mục lục

## 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:

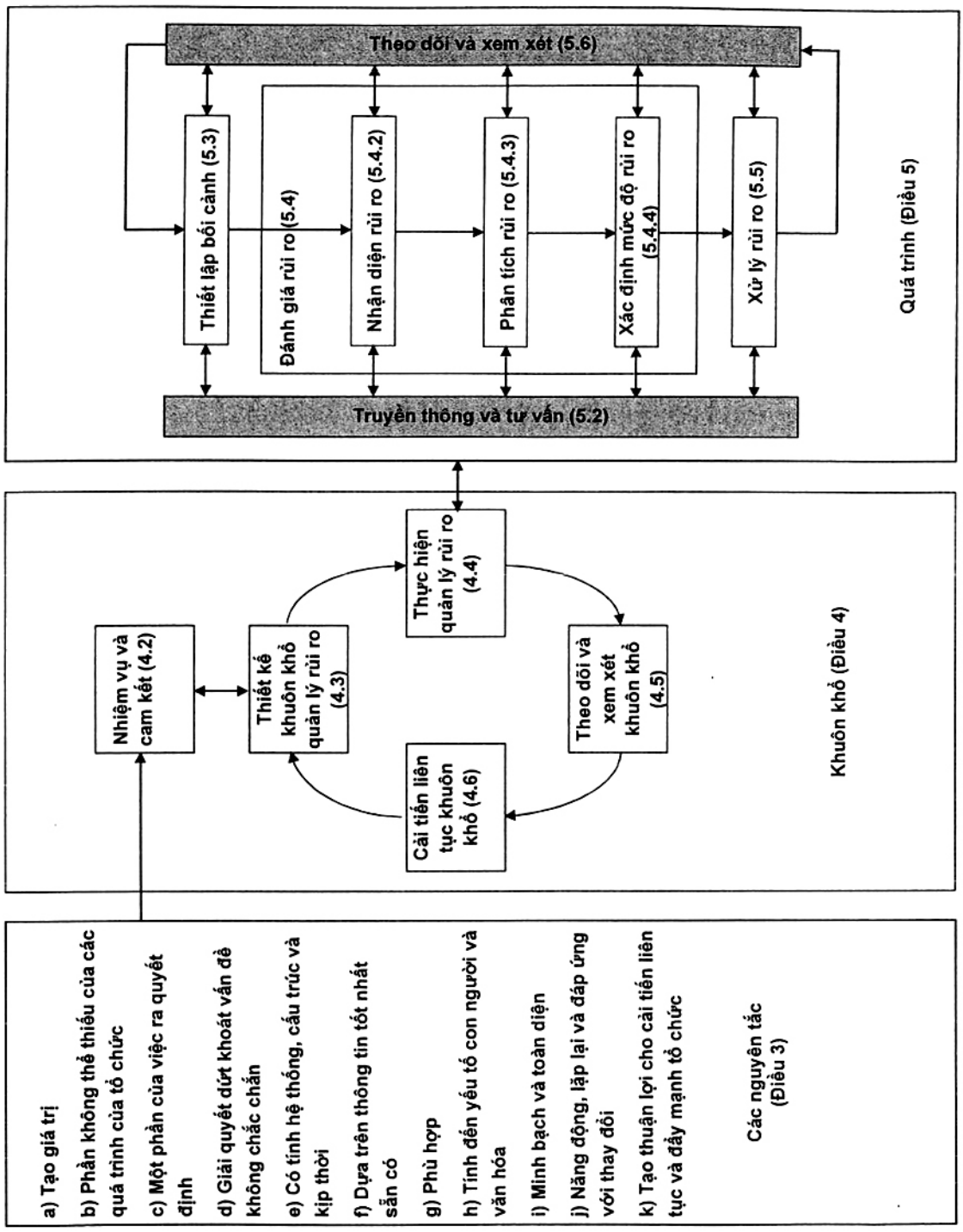
a) những người chịu trách nhiệm xây dựng chính sách quản lý rủi ro trong tổ chức;

b) 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;

c) những người cần đánh giá hiệu lực quản lý rủi ro của tổ chức; và

d) 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 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, kiềm 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).

CHÚ 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.

CHÚ 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 về 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 phần 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 độ 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** (2.11).

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 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
- kiềm chế rủi ro bằng quyết định đúng đắn.

CHÚ THÍCH 2: Xử lý rủi ro đối với những hệ quả tiêu cực đôi 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 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 lực hơn.

## 4 Khuôn khổ

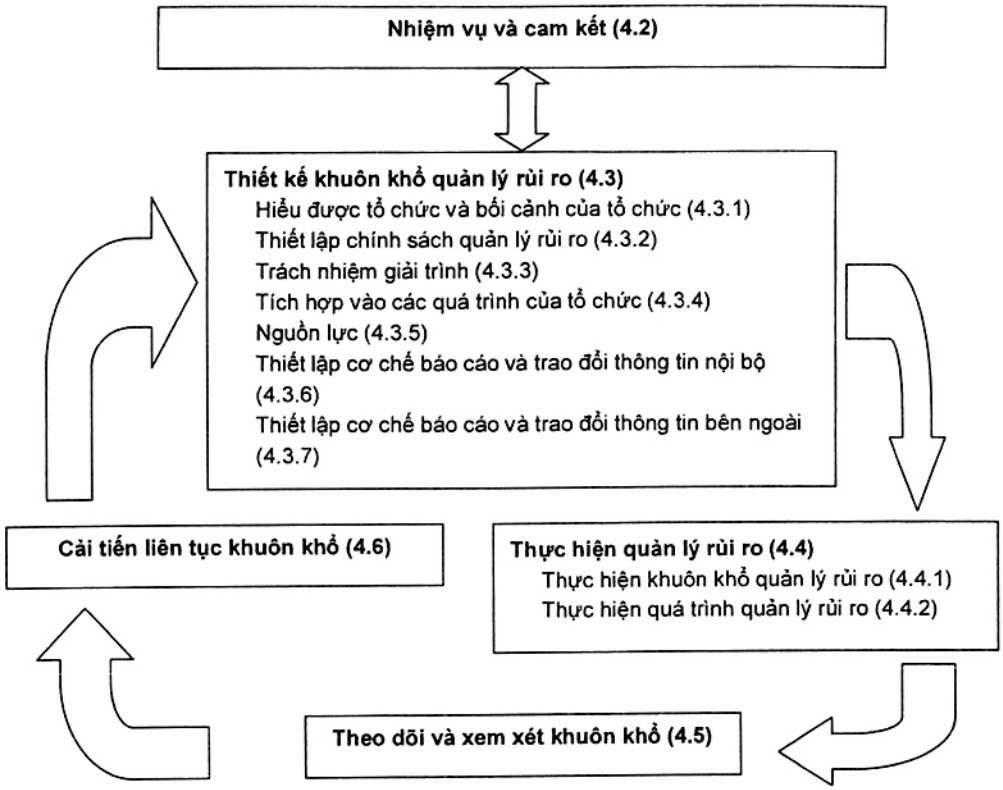
### 4.1. Khái quát

Sự thành công của quản lý rủi ro sẽ phụ thuộc vào hiệu lực của khuôn khổ quản lý đưa ra nền tảng và sự sắp xếp được lồng ghép vào tất cả các cấp của tổ chức. Khuôn khổ hỗ trợ việc quản lý rủi ro một cách hiệu quả thông qua việc áp dụng quá trình quản lý rủi ro (xem Điều 5) ở các cấp khác nhau và trong các bối cảnh cụ thể của tổ chức. Khuôn khổ đảm bảo rằng thông tin về rủi ro bắt nguồn từ quá trình quản lý rủi ro được báo cáo đầy đủ và được sử dụng làm cơ sở cho việc ra quyết định và trách nhiệm giải trình ở các cấp có liên quan của tổ chức.

Điều này mô tả các thành phần cần thiết của một khuôn khổ quản lý rủi ro và cách mà chúng tương tác với nhau một cách lặp đi lặp lại, như thể hiện trên Hình 2.

Khuôn khổ này không nhằm quy định một hệ thống quản lý, mà hỗ trợ tổ chức tích hợp quản lý rủi ro vào hệ thống quản lý tổng thể của mình. Do đó, tổ chức cần phải điều chỉnh các thành phần của khuôn khổ cho phù hợp với các nhu cầu cụ thể của mình.

Nếu thực tiễn quản lý và các quá trình hiện hành của tổ chức bao gồm các thành phần của quản lý rủi ro, hoặc nếu tổ chức đã chấp nhận một quá trình quản lý rủi ro chính thức cho các loại rủi ro hay hoàn cảnh cụ thể, thì các đối tượng đó phải được xem xét và đánh giá theo tiêu chuẩn này, bao gồm cả các thuộc tính nêu trong Phụ lục A, nhằm xác định tính thỏa đáng và hiệu lực.




**Hình 2 – Mối quan hệ giữa các thành phần trong khuôn khổ quản lý rủi ro**

### 4.2 Nhiệm vụ và cam kết

Cần có cam kết mạnh mẽ và chắc chắn của lãnh đạo tổ chức để đưa ra và đảm bảo hiệu lực liên tục việc quản lý rủi ro, cũng như cần hoạch định chiến lược chặt chẽ để đạt được cam kết ở tất cả các cấp. Lãnh đạo cần:

- xác định và thông qua chính sách quản lý rủi ro;
- đảm bảo rằng chính sách quản lý rủi ro hài hòa với văn hóa của tổ chức;
- xác định các chỉ số thực hiện quản lý rủi ro hài hòa với các chỉ số thực hiện của tổ chức;
- hài hòa các mục tiêu quản lý rủi ro với các mục tiêu và chiến lược của tổ chức;
- đảm bảo việc tuân thủ luật định và chế định;
- ấn định trách nhiệm giải trình và trách nhiệm ở các cấp thích hợp trong tổ chức;
- đảm bảo rằng các nguồn lực cần thiết được phân bổ để quản lý rủi ro;
- trao đổi thông tin về những lợi ích của quản lý rủi ro tới tất cả các bên liên quan; và
- đảm bảo rằng khuôn khổ quản lý rủi ro luôn duy trì tính thích hợp.

### 4.3 Thiết kế khuôn khổ quản lý rủi ro

#### 4.3.1 Hiểu về tổ chức và bối cảnh của tổ chức

Trước khi bắt đầu thiết kế và thực hiện khuôn khổ quản lý rủi ro, điều quan trọng là phải đánh giá và hiểu rõ cả bối cảnh bên ngoài và bên trong của tổ chức, vì điều này có thể ảnh hưởng đáng kể tới việc thiết kế khuôn khổ.

Đánh giá bối cảnh bên ngoài tổ chức có thể bao gồm, nhưng không giới hạn ở:

a) môi trường xã hội và văn hóa, chính trị, luật định, chế định, tài chính, công nghệ, kinh tế, tự nhiên và cạnh tranh, cho dù là quốc tế, quốc gia, khu vực hoặc địa phương;

b) những động lực và xu hướng chính tác động đến mục tiêu của tổ chức; và

c) mối liên hệ, nhận thức và giá trị của các bên liên quan bên ngoài.

Đánh giá bối cảnh bên trong tổ chức có thể bao gồm, nhưng không giới hạn ở:

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

#### 4.3.2 Thiết lập chính sách quản lý rủi ro

Chính sách quản lý rủi ro cần nêu rõ những mục tiêu của tổ chức và cam kết với việc quản lý rủi ro và thường nêu những nội dung sau:

- lý do quản lý rủi ro của tổ chức;
- các liên kết giữa các mục tiêu, chính sách của tổ chức và chính sách quản lý rủi ro;
- trách nhiệm giải trình và trách nhiệm quản lý rủi ro;
- cách thức giải quyết xung đột lợi ích;
- cam kết sẵn sàng cung cấp các nguồn lực cần thiết để hỗ trợ những người có trách nhiệm giải trình và trách nhiệm với quản lý rủi ro;
- cách thức đo lường và báo cáo việc thực hiện quản lý rủi ro; và

- cam kết xem xét và cải tiến định kỳ các chính sách và khuôn khổ quản lý rủi ro, đáp ứng sự kiện hoặc sự thay đổi hoàn cảnh.

Cần trao đổi thông tin một cách thích hợp về chính sách quản lý rủi ro.

#### 4.3.3 Trách nhiệm giải trình

Tổ chức cần đảm bảo có trách nhiệm giải trình, thẩm quyền và năng lực thích hợp để quản lý rủi ro, bao gồm cả việc thực hiện và duy trì quá trình quản lý rủi ro và đảm bảo tính đầy đủ, hiệu lực và hiệu quả của mọi kiểm soát. Điều này có thể được đơn giản hóa nhờ:

- xác định chủ sở hữu rủi ro có trách nhiệm và quyền hạn quản lý rủi ro;
- xác định người chịu trách nhiệm xây dựng, thực hiện và duy trì khuôn khổ quản lý rủi ro;
- xác định trách nhiệm khác của những người ở tất cả các cấp trong tổ chức đối với quá trình quản lý rủi ro;
- thiết lập các quá trình đo lường việc thực hiện, điều chỉnh, báo cáo nội bộ và/hoặc bên ngoài; và
- đảm bảo các cấp nhận biết rủi ro thích hợp.

#### 4.3.4 Tích hợp vào các quá trình của tổ chức

Quản lý rủi ro cần được đưa vào tất cả các quá trình và thực tiễn của tổ chức theo cách thức thích hợp, hiệu quả và hiệu lực. Quá trình quản lý rủi ro cần trở thành một phần không tách rời các quá trình của tổ chức. Cụ thể, quản lý rủi ro cần được lồng ghép vào các quá trình xây dựng chính sách, hoạch định, xem xét hoạt động chiến lược và quản lý thay đổi.

Cần có một kế hoạch quản lý rủi ro trong toàn tổ chức nhằm đảm bảo rằng chính sách quản lý rủi ro được thực hiện và quản lý rủi ro được đưa vào tất cả các quá trình và thực tiễn của tổ chức. Kế hoạch quản lý rủi ro có thể được tích hợp vào các kế hoạch khác của tổ chức, như kế hoạch chiến lược.

#### 4.3.5 Nguồn lực

Tổ chức cần phân bổ nguồn lực thích hợp cho việc quản lý rủi ro.

Cần tính đến những yếu tố sau:

- con người, kỹ năng, kinh nghiệm và năng lực;
- nguồn lực cần thiết cho mỗi bước của quá trình quản lý rủi ro;
- các quá trình của tổ chức, phương pháp và công cụ được sử dụng để quản lý rủi ro;
- các quá trình và thủ tục bằng văn bản;
- các hệ thống quản lý thông tin và tri thức; và
- các chương trình đào tạo.

#### 4.3.6 Thiết lập cơ chế báo cáo và trao đổi thông tin nội bộ

Tổ chức cần thiết lập cơ chế báo cáo và trao đổi thông tin nội bộ để hỗ trợ và khuyến khích trách nhiệm giải trình và quan hệ sở hữu rủi ro. Những cơ chế này cần đảm bảo:

- việc trao đổi thông tin một cách thích hợp về các thành phần chính trong khuôn khổ quản lý rủi ro và mọi thay đổi sau đó;
- có báo cáo nội bộ đầy đủ về khuôn khổ, hiệu lực và kết quả của nó;
- sẵn có thông tin liên quan rút ra từ việc áp dụng quản lý rủi ro ở các cấp và thời điểm thích hợp; và
- có các quá trình tham vấn với các bên liên quan nội bộ.

Khi thích hợp, những cơ chế này cần bao gồm các quá trình tổng hợp thông tin rủi ro từ nhiều nguồn khác nhau và có thể cần xem xét tính nhạy cảm của thông tin.

#### 4.3.7 Thiết lập cơ chế báo cáo và trao đổi thông tin bên ngoài

Tổ chức cần xây dựng và thực hiện một kế hoạch về cách thức trao đổi thông tin với các bên liên quan bên ngoài. Kế hoạch này cần liên quan đến:

- sự tham gia các bên liên quan thích hợp từ bên ngoài và đảm bảo hiệu quả trao đổi thông tin;
- báo cáo bên ngoài về sự tuân thủ các yêu cầu pháp lý, luật định và quản trị;
- cung cấp phản hồi và báo cáo về trao đổi thông tin và tham vấn;
- sử dụng việc trao đổi thông tin để xây dựng lòng tin với tổ chức; và
- liên hệ với các bên liên quan trong trường hợp khủng hoảng hoặc sự kiện bất thường xảy ra.

Khi thích hợp, những cơ chế này cần bao gồm các quá trình tổng hợp thông tin rủi ro có được từ nhiều nguồn khác nhau và có thể cần xem xét tính nhạy cảm của thông tin.

### 4.4 Thực hiện quản lý rủi ro

#### 4.4.1 Thực hiện khuôn khổ quản lý rủi ro

Khi thực hiện khuôn khổ quản lý rủi ro, tổ chức cần:

- xác định thời điểm và chiến lược thích hợp cho việc thực hiện khuôn khổ;
- áp dụng chính sách và quá trình quản lý rủi ro vào các quá trình của tổ chức;
- tuân thủ các yêu cầu luật định và chế định;
- đảm bảo rằng việc ra quyết định, bao gồm cả xây dựng và thiết lập mục tiêu, phù hợp với các kết quả của quá trình quản lý rủi ro;
- tổ chức các buổi trao đổi thông tin và đào tạo; và
- trao đổi và tham vấn các bên liên quan nhằm đảm bảo rằng khuôn khổ quản lý rủi ro duy trì tính thích hợp.

### 4.4.2 Thực hiện quá trình quản lý rủi ro

Quản lý rủi ro cần được thực hiện bằng việc đảm bảo rằng quá trình quản lý rủi ro nêu tại Điều 5 được áp dụng thông qua một kế hoạch quản lý rủi ro ở tất cả các cấp và chức năng liên quan của tổ chức như một phần trong thực tiễn và các quá trình của tổ chức.

### 4.5 Theo dõi và xem xét khuôn khổ

Để đảm bảo quản lý rủi ro có hiệu quả và liên tục hỗ trợ việc thực hiện của tổ chức, tổ chức cần:

- đo lường việc thực hiện quản lý rủi ro theo các chỉ số được định kỳ xem xét về tính phù hợp;
- định kỳ đo lường tiến trình và sai lệch so với kế hoạch quản lý rủi ro;
- định kỳ xem xét các khuôn khổ, chính sách, kế hoạch và quản lý rủi ro có phù hợp hay không, trong bối cảnh bên ngoài và nội bộ của tổ chức;
- báo cáo về rủi ro, tiến trình với kế hoạch quản lý rủi ro và chính sách quản lý rủi ro được tuân thủ tốt đến đâu; và
- xem xét hiệu lực của khuôn khổ quản lý rủi ro.

### 4.6 Cải tiến liên tục khuôn khổ

Căn cứ vào kết quả theo dõi và xem xét, cần đưa ra các quyết định về cách thức cải tiến khuôn khổ, chính sách, kế hoạch quản lý rủi ro. Những quyết định này cần dẫn đến những cải tiến trong quản lý rủi ro của tổ chức và văn hóa quản lý rủi ro của tổ chức.

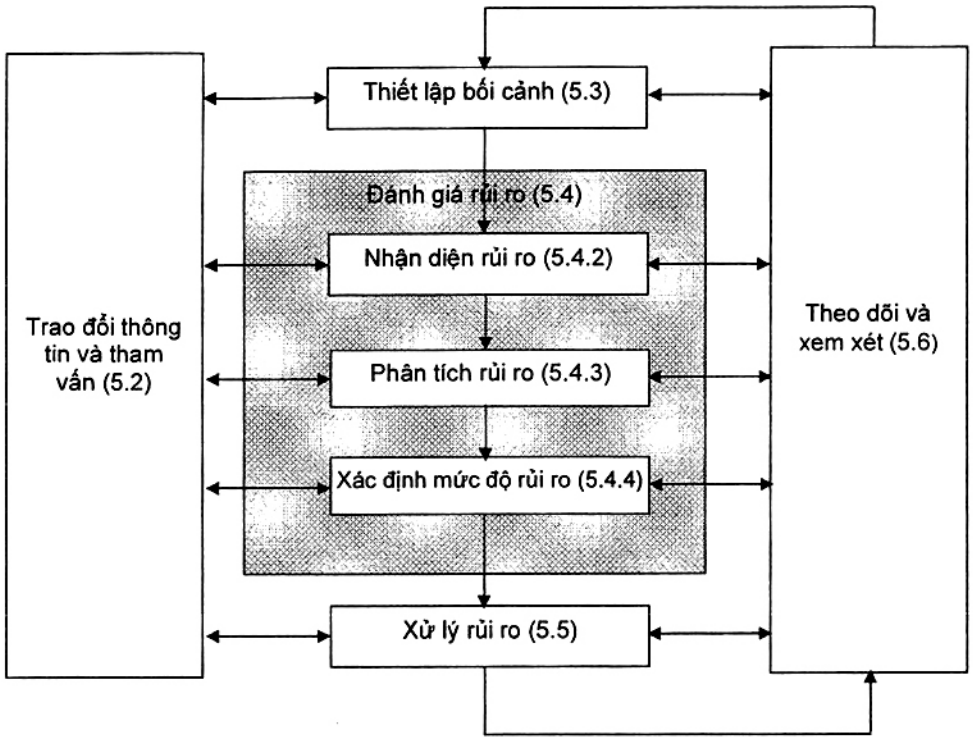
## 5 Quá trình

### 5.1 Khái quát

Quá trình quản lý rủi ro cần:

- là một phần không tách rời của quản lý,
- được gắn vào văn hóa, việc thực hành, và
- phù hợp với các quá trình hoạt động của tổ chức.

Quá trình này bao gồm các hoạt động được mô tả từ 5.2 đến 5.6. Quá trình quản lý rủi ro được thể hiện trên Hình 3.




**Hình 3 – Quá trình quản lý rủi ro**

### 5.2 Trao đổi thông tin và tham vấn

Trao đổi thông tin và tham vấn với các bên liên quan bên ngoài và nội bộ cần diễn ra trong tất cả các giai đoạn của quá trình quản lý rủi ro.

Vì vậy, các kế hoạch trao đổi thông tin và tham vấn cần được xây dựng ở giai đoạn đầu. Những kế hoạch này cần đề cập đến những vấn đề liên quan đến chính rủi ro, nguyên nhân rủi ro, hệ quả của nó (nếu biết), và các biện pháp thực hiện để xử lý rủi ro. Cần thực hiện có hiệu lực việc trao đổi thông tin và tham vấn nội bộ, bên ngoài nhằm đảm bảo rằng những người chịu trách nhiệm về thực hiện quá trình quản lý rủi ro và các bên liên quan đều hiểu được cơ sở đưa ra các quyết định và lý do tại sao lại yêu cầu những hành động cụ thể.

Phương pháp nhóm tham vấn có thể:

- giúp thiết lập bối cảnh thích hợp;
- đảm bảo rằng lợi ích của các bên liên quan được hiểu và xem xét;
- giúp đảm bảo rằng những rủi ro được xác định đầy đủ;

- tập hợp các lĩnh vực chuyên môn khác nhau lại để phân tích 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 trong xác định mức độ rủi ro;
- đảm bảo việc chấp thuận và hỗ trợ phương án xử lý;
- tăng cường quản lý thay đổi thích hợp trong quá trình quản lý rủi ro; và
- xây dựng một kế hoạch trao đổi thông tin và tham vấn bên ngoài và nội bộ thích hợp.

Trao đổi thông tin và tham vấn với các bên liên quan là rất quan trọng vì họ đánh giá rủi ro dựa trên nhận thức của chính mình về rủi ro. Những nhận thức này có thể khác nhau do các khác biệt về giá trị, nhu cầu, giả định, khái niệm và mối quan tâm của các bên liên quan. Vì quan điểm của họ có thể tác động đáng kể tới việc ra quyết định, nên nhận thức của bên liên quan cần được xác định, ghi lại và xem xét trong quá trình ra quyết định.

Trao đổi thông tin và tham vấn cần thúc đẩy việc trao đổi thông tin một cách trung thực, dễ hiểu và chính xác, có tính đến khía cạnh bảo mật và quyền hợp pháp cá nhân.

### 5.3 Thiết lập bối cảnh

#### 5.3.1 Khái quát

Bằng việc thiết lập bối cảnh, tổ chức làm rõ được các mục tiêu, xác định các tham số bên ngoài và nội bộ được đưa ra xem xét khi quản lý rủi ro, lập ra phạm vi và tiêu chí rủi ro cho quá trình còn lại. Trong khi nhiều tham số cũng tương tự như các tham số được xem xét trong thiết kế khuôn khổ quản lý rủi ro (xem 4.3.1), khi thiết lập bối cảnh cho quá trình quản lý rủi ro, cần phải xem xét các tham số ở mức chi tiết hơn và đặc biệt là các tham số liên quan như thế nào đến phạm vi của quá trình quản lý rủi ro cụ thể.

#### 5.3.2 Thiết lập bối cảnh bên ngoài

Bối cảnh bên ngoài là môi trường bên ngoài, trong đó tổ chức tìm cách để đạt được các mục tiêu của mình.

Hiểu biết về bối cảnh bên ngoài là điều quan trọng để đảm bảo rằng các mục tiêu và mối quan tâm của các bên liên quan bên ngoài đều được xem xét khi xây dựng tiêu chí rủi ro. Nó được dựa trên bối cảnh chung của tổ chức, nhưng với các chi tiết cụ thể của các yêu cầu luật định và chế định, nhận thức của các bên liên quan và các khía cạnh khác của rủi ro cụ thể liên quan tới phạm vi quá trình quản lý rủi ro.

Bối cảnh bên ngoài có thể bao gồm, nhưng không giới hạn ở:

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

### 5.3.3 Thiết lập bối cảnh nội bộ

Bối cảnh nội bộ là môi trường bên trong ở đó tổ chức tìm cách để đạt được các mục tiêu của mình. Quá trình quản lý rủi ro cần phải được liên kết với văn hóa, các quá trình, cơ cấu và chiến lược của tổ chức. Bối cảnh nội bộ là bất cứ điều gì bên trong tổ chức có thể ảnh hưởng đến cách thức quản lý rủi ro của tổ chức. Nó cần được thiết lập, vì:

a) quản lý rủi ro xảy ra trong bối cảnh các mục tiêu của tổ chức;

b) mục tiêu và tiêu chí của một dự án, quá trình hay hoạt động cụ thể cần được xem xét một cách tổng thể theo các mục tiêu của tổ chức; và

c) một số tổ chức không nhận ra cơ hội để đạt được mục tiêu chiến lược, dự án hoặc hoạt động của mình và điều này ảnh hưởng đến cam kết, uy tín, độ tin cậy và giá trị của tổ chức.

Cần hiểu được bối cảnh nội bộ. Điều này có thể bao gồm, nhưng không giới hạn ở:

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

### 5.3.4 Thiết lập bối cảnh của quá trình quản lý rủi ro

Cần thiết lập mục tiêu, chiến lược, phạm vi và tham số về các hoạt động của tổ chức, hoặc những bộ phận trong tổ chức áp dụng quá trình quản lý rủi ro. Cần thực hiện việc quản lý rủi ro với sự xem xét đầy đủ các nhu cầu cần thiết để quyết định nguồn lực được sử dụng trong việc thực hiện quản lý rủi ro. Các nguồn lực cần thiết, trách nhiệm và quyền hạn, và các hồ sơ phải lưu giữ cũng cần được quy định rõ.

Bối cảnh của quá trình quản lý rủi ro sẽ thay đổi theo nhu cầu của tổ chức. Nó có thể bao gồm, nhưng không giới hạn ở việc:

- xác định mục đích và mục tiêu của hoạt động quản lý rủi ro;
- xác định trách nhiệm đối với và trong phạm vi quá trình quản lý rủi ro;

- xác định phạm vi cũng như mức độ và tầm ảnh hưởng của các hoạt động quản lý rủi ro được thực hiện, bao gồm cả những nội dung cụ thể được đưa vào và loại trừ;
- xác định các hoạt động, quá trình, chức năng, dự án, sản phẩm, dịch vụ hoặc tài sản theo thời gian và địa điểm;
- xác định các mối quan hệ giữa một dự án, quá trình hay hoạt động cụ thể với các dự án, quá trình hay hoạt động khác của tổ chức;
- xác định các phương pháp luận về đánh giá rủi ro;
- xác định cách thức đánh giá việc thực hiện và hiệu lực trong quản lý rủi ro;
- xác định và quy định rõ về những quyết định phải được đưa ra; và
- xác định, lập phạm vi hoặc khuôn khổ các nghiên cứu cần thiết, mức độ và mục tiêu nghiên cứu, các nguồn lực cần thiết cho những nghiên cứu này.

Việc quan tâm đến những điều này và các yếu tố liên quan khác cần giúp đảm bảo rằng phương pháp tiếp cận quản lý rủi ro được chấp nhận là phù hợp với hoàn cảnh, với tổ chức và với những rủi ro ảnh hưởng đến việc đạt được các mục tiêu của tổ chức.

### 5.3.5 Xác định tiêu chí rủi ro

Tổ chức cần xác định tiêu chí sử dụng để xác định mức độ nghiêm trọng của rủi ro. Tiêu chí cần phản ánh các giá trị, mục tiêu và nguồn lực của tổ chức. Một số tiêu chí có thể sử dụng hoặc bắt nguồn từ các yêu cầu luật định và chế định và các yêu cầu khác mà tổ chức quy định. Tiêu chí rủi ro cần nhất quán với chính sách quản lý rủi ro của tổ chức (xem 4.3.2), được xác định khi bắt đầu bất kỳ quá trình quản lý rủi ro nào và được xem xét liên tục.

Khi xác định tiêu chí rủi ro, các yếu tố được xem xét cần bao gồm:

- bản chất, loại nguyên nhân và hệ quả có thể xảy ra và cách thức đo lường chúng;
- cách thức xác định khả năng xảy ra rủi ro;
- khuôn khổ thời gian của khả năng xảy ra rủi ro và/hoặc hệ quả;
- cách thức xác định mức độ rủi ro;
- quan điểm của các bên liên quan;
- mức độ nào rủi ro có thể chấp nhận hoặc chịu được; và
- có cần xem xét sự kết hợp của nhiều rủi ro với nhau không, và nếu cần thì sự kết hợp nào và kết hợp ra sao cần được xem xét.

### 5.4 Đánh giá rủi ro

#### 5.4.1 Khái quát

Đánh giá rủi ro là quá trình tổng thể của việc xác định rủi ro, phân tích rủi ro và xác định mức độ rủi ro.

CHÚ THÍCH: Tiêu chuẩn ISO/IEC 31010 đưa ra hướng dẫn về kỹ thuật đánh giá rủi ro.

#### 5.4.2 Nhận diện rủi ro

Tổ chức cần xác định các nguồn rủi ro, lĩnh vực chịu tác động, sự kiện (bao gồm cả những thay đổi về hoàn cảnh), nguyên nhân, hệ quả tiềm ẩn của sự kiện. Mục đích của bước này là tạo ra một danh mục đầy đủ các rủi ro dựa trên những sự kiện có thể tạo ra, tăng cường, ngăn ngừa, giảm nhẹ, đẩy nhanh hoặc làm chậm việc đạt được các mục tiêu. Quan trọng là phải xác định các rủi ro gắn với việc không theo đuổi một cơ hội. Việc xác định một cách toàn diện là rất quan trọng, bởi vì một rủi ro không được xác định trong giai đoạn này cũng sẽ không có trong các phân tích sau đó.

Việc xác định cần bao gồm cả những rủi ro mà nguồn gốc của chúng có hoặc không thuộc sự kiểm soát của tổ chức, cho dù nguồn hay nguyên nhân gây ra rủi ro có thể không rõ ràng. Xác định rủi ro cần bao gồm kiểm tra tác động của hệ quả cụ thể, bao gồm ảnh hưởng theo đợt và tích lũy. Cũng cần phải xem xét một loạt các hệ quả ngay cả khi các nguồn hay nguyên nhân gây ra rủi ro không rõ ràng. Bên cạnh việc xác định những gì có thể xảy ra, cũng cần phải xem xét nguyên nhân và kịch bản có khả năng chỉ ra những hệ quả có thể có. Tất cả các nguyên nhân và hệ quả nghiêm trọng đều cần được xem xét.

Tổ chức cần áp dụng các công cụ và kỹ thuật nhận dạng rủi ro, phù hợp với các mục tiêu và khả năng của mình cũng như với các rủi ro phải đối mặt. Thông tin liên quan và cập nhật rất quan trọng trong việc xác định rủi ro. Khi có thể, điều này cần bao gồm thông tin cơ bản thích hợp. Những người có kiến thức phù hợp cần tham gia vào việc xác định rủi ro.

#### 5.4.3 Phân tích rủi ro

Phân tích rủi ro đòi hỏi phải xây dựng hiểu biết về rủi ro. Phân tích rủi ro cung cấp đầu vào để xác định mức độ rủi ro và quyết định xem có cần xử lý rủi ro hay không, quyết định về chiến lược, phương pháp xử lý rủi ro thích hợp nhất. Phân tích rủi ro cũng có thể cung cấp đầu vào cho việc ra quyết định khi nào phải thực hiện các phương án và giải pháp liên quan đến các loại hình, mức độ rủi ro khác nhau.

Phân tích rủi ro đòi hỏi phải xem xét nguyên nhân và nguồn rủi ro, hệ quả tích cực và tiêu cực của chúng, khả năng những hệ quả này có thể xảy ra. Cần xác định các yếu tố ảnh hưởng đến hệ quả và khả năng xảy ra. Rủi ro được phân tích bằng cách xác định hệ quả, khả năng xảy ra và các thuộc tính khác của rủi ro. Một sự kiện có thể có nhiều hệ quả và có thể ảnh hưởng đến nhiều mục tiêu. Cũng cần xem xét các kiểm soát hiện có, hiệu quả và hiệu lực của những kiểm soát này.

Cách thức thể hiện hệ quả và khả năng xảy ra và cách chúng được kết hợp để xác định mức độ rủi ro cần phản ánh loại hình rủi ro, thông tin sẵn có và mục đích theo đó kết quả của đánh giá rủi ro được sử dụng. Tất cả phải nhất quán với tiêu chí rủi ro. Việc xem xét sự phụ thuộc lẫn nhau của các rủi ro và

nguồn rủi ro khác nhau cũng rất quan trọng.

Tính tin cậy trong việc xác định mức độ rủi ro và tính nhạy cảm của nó đối với điều kiện tiên quyết và các giả định cần được xem xét trong phân tích và được truyền đạt có hiệu lực đến những người ra quyết định và đến các bên liên quan khác khi thích hợp. Các yếu tố như sự bất đồng ý kiến giữa các chuyên gia, sự không chắc chắn, tính sẵn có, chất lượng, số lượng, sự phù hợp liên tục của thông tin, hoặc những hạn chế về mô hình cần được nêu ra và có thể được nhấn mạnh.

Phân tích rủi ro có thể được thực hiện với mức độ chi tiết khác nhau, tùy thuộc vào rủi ro, mục đích của phân tích, thông tin, dữ liệu và nguồn lực sẵn có. Phân tích có thể là định tính, bán định lượng hay định lượng, hoặc kết hợp của các dạng này, tùy từng hoàn cảnh.

Hệ quả và khả năng xảy ra có thể được xác định bằng việc mô hình hóa các kết quả của một sự kiện hoặc một loạt các sự kiện, hoặc bằng cách ngoại suy từ những nghiên cứu thực nghiệm hay từ dữ liệu có sẵn. Hệ quả có thể được thể hiện theo các tác động hữu hình và vô hình. Trong một số trường hợp, có thể cần một số giá trị bằng số hoặc ký hiệu mô tả để xác định hệ quả và khả năng xảy ra của nó tại những thời điểm, địa điểm, các nhóm hoặc tình huống khác nhau.

### 5.4.4 Xác định mức độ rủi ro

Mục đích của xác định mức độ rủi ro là hỗ trợ việc ra quyết định về những rủi ro cần được xử lý và ưu tiên thực hiện xử lý, dựa trên kết quả phân tích rủi ro.

Xác định mức độ rủi ro đòi hỏi phải so sánh mức độ rủi ro thấy được trong quá trình phân tích với tiêu chí rủi ro được thiết lập khi xem xét bối cảnh. Dựa vào so sánh này, có thể xem xét nhu cầu xử lý.

Quyết định cần tính đến bối cảnh rủi ro rộng hơn và bao gồm việc xem xét khả năng chịu đựng rủi ro của các bên không phải là tổ chức được hưởng lợi từ rủi ro. Các quyết định phải được đưa ra phù hợp với các yêu cầu pháp lý, quản lý và yêu cầu khác.

Trong một số trường hợp, việc xác định mức độ rủi ro có thể dẫn đến quyết định thực hiện phân tích kỹ hơn. Việc xác định mức độ rủi ro cũng có thể dẫn đến một quyết định không xử lý rủi ro theo bất kỳ cách nào khác ngoài việc duy trì các kiểm soát hiện có. Quyết định này sẽ bị ảnh hưởng bởi thái độ của tổ chức đối với rủi ro và tiêu chí rủi ro đã được thiết lập.

## 5.5 Xử lý rủi ro

### 5.5.1 Khái quát

Xử lý rủi ro liên quan đến việc chọn một hoặc nhiều phương án để thay đổi rủi ro và thực hiện những phương án này. Khi được thực hiện, các xử lý sẽ cung cấp hoặc thay đổi các kiểm soát. Xử lý rủi ro liên quan đến một quá trình theo chu kỳ gồm:

- đánh giá việc xử lý rủi ro;
- quyết định mức độ rủi ro tồn đọng có chấp nhận được hay không;
- nếu không chấp nhận được, tạo ra một xử lý rủi ro mới; và

– đánh giá hiệu lực của việc xử lý đó.

Các phương án xử lý rủi ro không nhất thiết phải loại trừ lẫn nhau hoặc thích hợp trong mọi tình huống. Các phương án có thể bao gồm:

a) tránh rủi ro bằng cách quyết định không bắt đầu hoặc tiếp tục hoạt động làm phát sinh rủi ro;

b) tiếp nhận hoặc làm tăng rủi ro để theo đuổi một cơ hội;

c) loại bỏ nguồn rủi ro;

d) thay đổi khả năng xảy ra;

e) thay đổi hệ quả;

f) chia sẻ rủi ro với một hoặc nhiều bên khác (bao gồm cả hợp đồng và tài trợ rủi ro); và

g) kiềm chế rủi ro bằng quyết định sáng suốt.

### 5.5.2 Lựa chọn các phương án xử lý rủi ro

Lựa chọn một phương án xử lý rủi ro thích hợp nhất liên quan đến việc cân đối giữa chi phí và nỗ lực thực hiện với các lợi ích thu được về các yêu cầu luật định, chế định và các yêu cầu khác như trách nhiệm xã hội và bảo vệ môi trường tự nhiên. Các quyết định cũng cần phải tính đến các rủi ro có thể đảm bảo việc xử lý nhưng không thuyết phục về mặt kinh tế, ví dụ rủi ro có hệ quả nghiêm trọng nhưng khó xảy ra.

Một số phương án xử lý có thể được xem xét và áp dụng riêng lẻ hoặc kết hợp. Bình thường, tổ chức có thể được lợi từ việc chấp nhận một kết hợp các phương án xử lý.

Khi chọn lựa các phương án xử lý rủi ro, tổ chức nên xem xét các giá trị và nhận thức của các bên liên quan và những cách thích hợp nhất để trao đổi thông tin với họ. Khi phương án xử lý rủi ro có thể tác động đến rủi ro ở nơi nào khác trong tổ chức hoặc với các bên liên quan, thì những phương án này cần được tính đến trong quyết định. Mặc dù hiệu lực như nhau, nhưng một số xử lý rủi ro có thể được một số bên liên quan chấp nhận hơn so với các xử lý khác.

Phương án xử lý cần xác định rõ thứ tự ưu tiên, trong đó các xử lý rủi ro riêng lẻ cần được thực hiện.

Bản thân xử lý rủi ro cũng có thể gây ra rủi ro. Một rủi ro đáng kể có thể là sự thất bại hoặc không hiệu quả của các biện pháp xử lý rủi ro. Theo dõi cần là một phần không thể thiếu của phương án xử lý rủi ro để đảm bảo duy trì hiệu lực của các biện pháp này.

Xử lý rủi ro cũng có thể gây ra những rủi ro thứ phát cần phải được đánh giá, xử lý, theo dõi và xem xét. Những rủi ro thứ phát này cần được đưa vào cùng phương án xử lý như rủi ro ban đầu chứ không xử lý như một rủi ro mới. Cần phải xác định và duy trì mối liên hệ giữa hai rủi ro này.

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

Mục đích của kế hoạch xử lý rủi ro là văn bản hóa cách thức thực thi các phương án xử lý được chọn.

Các thông tin cung cấp trong kế hoạch xử lý cần bao gồm:

- lý do lựa chọn các phương án xử lý, bao gồm cả lợi ích mong muốn sẽ đạt được;
- những người có trách nhiệm giải trình đối với việc phê duyệt kế hoạch và những người chịu trách nhiệm thực hiện kế hoạch;
- các hành động đề xuất;
- các yêu cầu nguồn lực bao gồm cả dự phòng;
- các biện pháp thực hiện và ràng buộc;
- các yêu cầu đối với việc báo cáo và theo dõi; và
- thời gian và lịch trình.

Kế hoạch xử lý cần được tích hợp với các quá trình quản lý của tổ chức và được thảo luận với các bên liên quan thích hợp.

Người ra quyết định và các bên liên quan khác cần được biết về bản chất và mức độ rủi ro tồn đọng sau khi xử lý. Rủi ro tồn đọng cần được lập thành văn bản và chịu sự theo dõi, xem xét và khi thích hợp, sẽ có xử lý thêm.

### 5.6 Theo dõi và xem xét

Cả theo dõi và xem xét phải là một phần được hoạch định của quá trình quản lý rủi ro và bao gồm hoạt động kiểm tra hoặc giám sát thường xuyên. Nó có thể mang tính định kỳ hoặc đột xuất.

Trách nhiệm theo dõi và xem xét cần được xác định rõ ràng.

Các quá trình theo dõi và xem xét của tổ chức cần bao gồm tất cả các khía cạnh của quá trình quản lý rủi ro với mục đích:

- đảm bảo rằng hoạt động kiểm soát có hiệu quả và hiệu lực trong cả thiết kế và vận hành;
- có thêm thông tin để cải tiến việc đánh giá rủi ro;
- phân tích và rút ra bài học từ các sự kiện (bao gồm cả những lần thoát nạn), những thay đổi, các xu hướng, thành công và thất bại;
- phát hiện những thay đổi trong bối cảnh bên ngoài và nội bộ, bao gồm cả thay đổi về tiêu chí rủi ro và bản thân rủi ro có thể yêu cầu xem xét lại việc xử lý rủi ro và thứ tự ưu tiên; và
- xác định những rủi ro đang hình thành.

Tiến trình thực hiện các phương án xử lý rủi ro cung cấp thước đo việc thực hiện. Các kết quả có thể được đưa vào quản lý, đo lường tổng thể việc thực hiện của tổ chức và hoạt động báo cáo bên ngoài, nội bộ.

Kết quả của theo dõi và xem xét cần được ghi lại và báo cáo bên ngoài, nội bộ khi thích hợp, và cũng

cần được sử dụng làm đầu vào cho việc xem xét khuôn khổ quản lý rủi ro (xem 4.5).

### 5.7 Lập hồ sơ quá trình quản lý rủi ro

Các hoạt động quản lý rủi ro cần có khả năng truy tìm nguồn gốc. Trong quá trình quản lý rủi ro, hồ sơ cung cấp nền tảng cho việc cải tiến các phương pháp và công cụ, cũng như trong quá trình tổng thể.

Các quyết định liên quan đến việc lập hồ sơ cần tính đến:

- nhu cầu học hỏi liên tục của tổ chức;
- lợi ích của việc tái sử dụng thông tin cho các mục đích quản lý;
- chi phí và nỗ lực liên quan tới việc lập và duy trì hồ sơ;
- nhu cầu đối với hồ sơ theo luật định, chế định và hoạt động;
- phương pháp truy cập, dễ dàng khôi phục và phương tiện bảo quản;
- thời gian lưu trữ, và
- tính nhạy cảm của thông tin.

# Phụ lục A

(tham khảo)

# Các thuộc tính của quản lý rủi ro nâng cao

## A.1 Khái quát

Mọi tổ chức cần hướng tới một mức độ thực hiện khuôn khổ quản lý rủi ro phù hợp với tầm quan trọng của quyết định đã được đưa ra. Danh mục các thuộc tính dưới đây thể hiện mức độ thực hiện cao trong quản lý rủi ro. Để hỗ trợ tổ chức trong việc đo lường việc thực hiện của mình theo các tiêu chí này, một số chỉ số hữu hình được đưa ra cho mỗi thuộc tính.

## A.2 Các kết quả chính

**A.2.1** Tổ chức có hiểu biết chính xác, toàn diện và thực tế về những rủi ro của mình.

**A.2.2** Các rủi ro của tổ chức nằm trong phạm vi tiêu chí rủi ro.

## A.3 Các thuộc tính

### A.3.1 Cải tiến liên tục

Trọng tâm được đặt vào cải tiến liên tục việc quản lý rủi ro thông qua việc thiết lập các mục đích, đo lường, xem xét việc thực hiện và thay đổi sau đó các quá trình, hệ thống, nguồn lực, khả năng và kỹ năng của tổ chức.

Điều này có thể được chỉ ra bởi sự tồn tại của các mục đích thực hiện rõ ràng theo đó đo lường việc thực hiện của tổ chức và nhà quản lý riêng lẻ. Có thể công bố và trao đổi thông tin về việc thực hiện của tổ chức. Thông thường, sẽ có ít nhất một xem xét hàng năm về việc thực hiện và sau đó là sửa đổi các quá trình và thiết lập các mục tiêu thực hiện sửa đổi cho giai đoạn tiếp theo.

Đánh giá việc thực hiện quản lý rủi ro là một phần không thể thiếu của đánh giá việc thực hiện tổng thể của tổ chức và hệ thống đo lường cho các phòng ban và cá nhân.

### A.3.2 Trách nhiệm đầy đủ đối với rủi ro

Quản lý rủi ro nâng cao bao gồm trách nhiệm toàn diện được xác định và chấp nhận đầy đủ đối với rủi ro, kiểm soát, nhiệm vụ xử lý rủi ro. Cá nhân được chỉ định chấp nhận hoàn toàn trách nhiệm, có kỹ năng phù hợp và có đủ nguồn lực để kiểm tra việc kiểm soát, theo dõi rủi ro, cải tiến việc kiểm soát và trao đổi thông tin về rủi ro và việc quản lý rủi ro một cách hiệu quả với các bên liên quan bên ngoài và nội bộ.

Điều này có thể được chỉ ra bởi tất cả các thành viên của một tổ chức nhận thức đầy đủ về rủi ro, kiểm soát và những nhiệm vụ mà họ có trách nhiệm. Thông thường, điều này sẽ được ghi lại trong bản mô tả công việc/vị trí, cơ sở dữ liệu hoặc hệ thống thông tin. Định nghĩa về vai trò, trách nhiệm giải trình,

trách nhiệm quản lý rủi ro cần là một phần của tất cả các chương trình giới thiệu ban đầu của tổ chức.

Tổ chức đảm bảo rằng những người chịu trách nhiệm được trang bị để thực hiện vai trò đó thông qua việc giao cho họ quyền hạn, thời gian, đào tạo, nguồn lực và kỹ năng đầy đủ để đảm nhận trách nhiệm của mình.

### A.3.3 Áp dụng quản lý rủi ro trong các lần ra quyết định

Tất cả các quyết định được đưa ra trong tổ chức, bất kể mức độ quan trọng và ý nghĩa đều liên quan đến việc xem xét các rủi ro và áp dụng quản lý rủi ro ở mức độ thích hợp nào đó.

Điều này có thể được thể hiện trong hồ sơ các cuộc họp và quyết định để cho thấy rằng đã có các cuộc thảo luận cụ thể về những rủi ro. Ngoài ra, có thể thấy rằng tất cả các thành phần của quản lý rủi ro đều được thể hiện trong các quá trình chính của việc ra quyết định trong tổ chức, ví dụ như các quyết định về việc phân bổ vốn, về các dự án quan trọng, về việc tái cấu trúc và những thay đổi trong tổ chức. Vì những lý do này, quản lý rủi ro trên cơ sở vững chắc được nhìn nhận trong phạm vi tổ chức, là tạo cơ sở cho việc quản trị có hiệu quả.

### A.3.4 Trao đổi thông tin liên tục

Quản lý rủi ro nâng cao bao gồm trao đổi thông tin liên tục với các bên liên quan nội bộ và bên ngoài, bao gồm việc báo cáo thường xuyên và toàn diện về thực hiện quản lý rủi ro, như một phần của quản trị tốt.

Điều này có thể được thể hiện qua việc trao đổi thông tin với các bên liên quan như là một phần thiết yếu và không thể thiếu của quản lý rủi ro. Trao đổi thông tin thực sự được xem là một quá trình hai chiều sao cho có thể ra các quyết định đúng đắn một cách phù hợp về mức độ rủi ro và nhu cầu xử lý rủi ro theo tiêu chí rủi ro được thiết lập phù hợp và toàn diện.

Lập báo cáo bên ngoài và nội bộ thường xuyên và toàn diện về cả rủi ro nghiêm trọng và việc thực hiện quản lý rủi ro góp phần đáng kể vào quản trị có hiệu lực trong tổ chức.

### A.3.5 Tích hợp đầy đủ trong cơ cấu quản trị của tổ chức

Quản lý rủi ro được xem như là trung tâm của các quá trình quản lý của tổ chức, sao cho những rủi ro sẽ được xem xét về ảnh hưởng của sự không chắc chắn tới các mục tiêu. Cơ cấu và các quá trình quản trị được dựa trên việc quản lý rủi ro. Quản lý rủi ro hiệu có hiệu lực được nhà quản lý xem là thiết yếu cho việc đạt được các mục tiêu của tổ chức.

Điều này được thể hiện bằng ngôn ngữ của nhà quản lý và các văn bản tài liệu quan trọng trong tổ chức sử dụng thuật ngữ "sự không chắc chắn" liên quan đến rủi ro. Thuộc tính này cũng thường được phản ánh trong tuyên bố về chính sách của tổ chức, đặc biệt là những tuyên bố liên quan đến quản lý rủi ro. Thông thường, thuộc tính này sẽ được xác nhận qua phỏng vấn nhà quản lý và thông qua bằng chứng về hành động và tuyên bố của họ.

## Thư mục tài liệu tham khảo

[1] ISO Guide 73:2009, *Risks management – Vocabulary* (Quản lý rủi ro – Từ vựng)

[2] ISO/IEC 31010, *Risks management – Risks assessment techniques* (Quản lý rủi ro – Kỹ thuật đánh giá rủi ro)