ICS 03.100.01
CCS A 02

中华人民共和国国家标准

GB/T 24353—2022/ISO 31000:2018
代替 GB/T 24353—2009

风险管理　指南

Risk management—Guidelines

（ISO 31000:2018,IDT）

2022-10-12 发布　　2022-10-12 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前言 …… Ⅲ
引言 …… Ⅳ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　原则 …… 2
5　框架 …… 3
5.1　概述 …… 3
5.2　领导作用和承诺 …… 4
5.3　整合 …… 4
5.4　设计 …… 4
5.5　实施 …… 6
5.6　评价 …… 6
5.7　改进 …… 6
6　过程 …… 6
6.1　概述 …… 6
6.2　沟通和咨询 …… 7
6.3　范围、环境、准则 …… 7
6.4　风险评估 …… 8
6.5　风险应对 …… 10
6.6　监督和检查 …… 11
6.7　记录和报告 …… 11
参考文献 …… 12

前　言

本文件按照GB/T1.1—2020《标准化工作导则　第1部分:标准化文件的结构和起草规则》的规定起草。

本文件代替GB/T 24353—2009《风险管理　原则与实施指南》。与GB/T 24353—2009相比,除了编辑性改动外,主要技术变化如下:

——增加了第3章的八个术语(见3.1～3.8);

——更改了第4章的内容,调整了原则的数量(见第4章,2009年版的第4章)、补充了原则的内容、增加了原则的示意图(见第4章)。

——第5章由“风险管理过程”改为“框架”;第6章由“风险管理的实施”改为“过程”(见第5章、第6章,2009版的第5章、第6章)。

本文件等同采用ISO 31000:2018《风险管理　指南》。

本文件做了下列最小限度的编辑性改动:

增加了4a)条款说明“注”。

本文件由全国风险管理标准化技术委员会(SAC/TC 310)提出并归口。

本文件起草单位:中国标准化研究院、蒙娜丽莎集团股份有限公司、三门核电有限公司、三只松鼠股份有限公司、北京大学、中共中央党校(国家行政学院)、中国核能电力股份有限公司、第一会达(北京)数据技术有限公司、达信评(北京)风险管理咨询有限公司、国家科技风险开发事业中心、国务院国有资产监督管理委员会研究中心、中国矿业大学(北京)。

本文件主要起草人:高晓红、陆小伟、孙保均、徐涵、孙友文、吕多加、刘剑、施颖、支东生、游志斌、刘新立、张杰军、吴昕、郭小娟、项京锋、张旗康、顾千辉。

本文件及其所代替文件的历次版本发布情况为:

——2009年首次发布为GB/T 24353—2009;

——本次为第一次修订。

引　言

任何类型和规模的组织都受到各种内外部因素的影响，导致其目标的实现存在不确定性。这些目标关系到组织中从战略决策到运营的各种活动，表现在战略、运营、财务、环境、社会、声誉等各个方面。

风险管理通过考虑不确定性及其对目标的影响，采取相应的措施，为组织的决策和运营以及有效应对各类突发事件提供支持。风险管理旨在保证组织恰当地应对风险，提高风险应对的效率和效果，增强决策和行动的合理性，有效地配置资源。

管理风险是一个循环提升的过程，有助于组织制定战略、实现目标和做出合理的决策。管理风险是组织治理和领导作用的一部分，为组织所有层级的管理提供基础，有助于管理体系的改善。管理风险是组织所有相关活动的有机组成部分，包括与利益相关者的沟通。

管理风险时要考虑组织的内、外部环境，包括人的行为和文化因素。

图 1 列出了管理风险所依据的原则、框架和过程。这些原则、框架和过程可能已全部或部分地存在于组织内，但可根据需要进行调整或改善，从而使管理风险的效果好、效率高，并且具有一致性。

本文件旨在帮助组织在制定决策、设定和实现目标以及提升绩效的过程中管理风险，创造和保护价值。

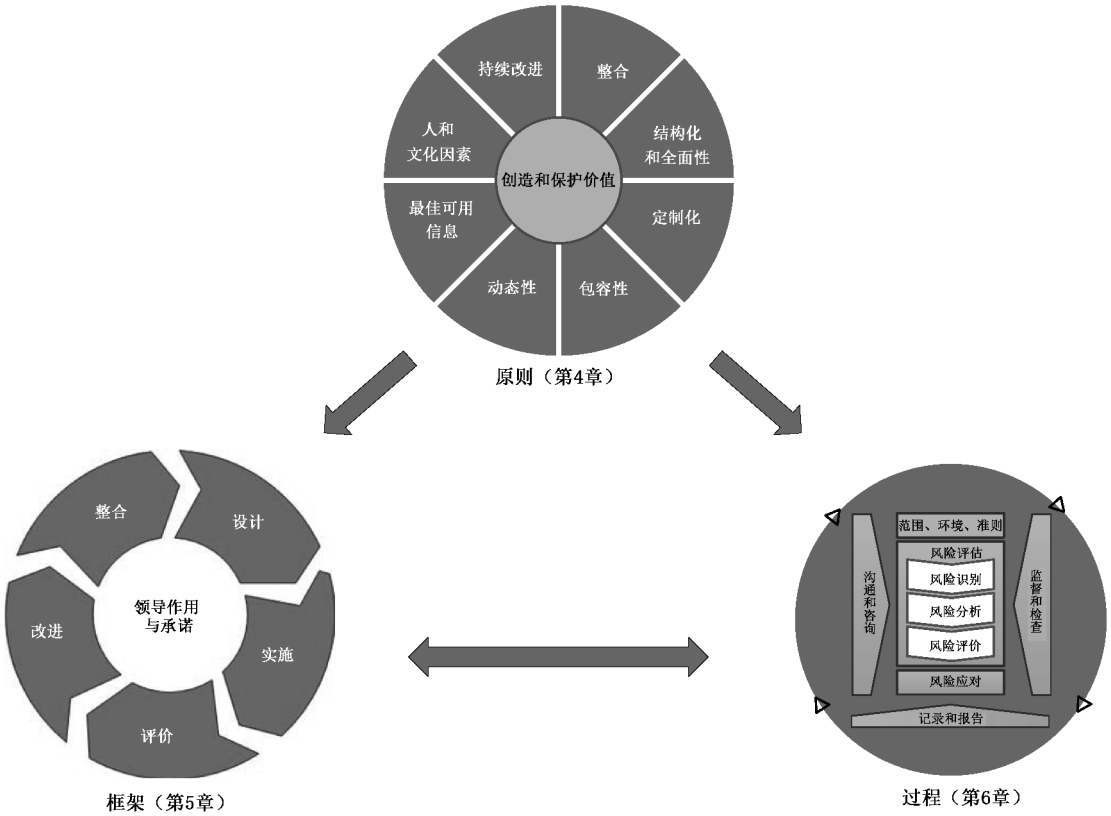

图 1　原则、框架和过程

风险管理　指南

1　范围

本文件为组织管理其所面临的风险提供指南，组织可根据其具体环境，有针对性地应用。

本文件为管理各种类型的风险提供了一种通用方法，而非仅针对某些特定行业或领域。

本文件适用于组织全生命周期的任何活动，包括所有层级的决策制定。

2　规范性引用文件

本文件没有规范性引用文件。

3　术语和定义

下列术语和定义适用于本文件。

3.1

风险　risk

不确定性对目标的影响。

注 1：影响是指偏离预期，偏离可以是正面的和/或负面的，可能带来机会和威胁。

注 2：目标可有不同维度和类型，可应用在不同层级。

注 3：通常风险可以用风险源、潜在事件及其后果和可能性来描述。

3.2

风险管理　risk management

指导和控制组织与风险(3.1)相关的协调活动。

3.3

利益相关者　stakeholder；interested party

可以影响、被影响或自认为会被某一决策或活动影响的个人或组织。

注："interested party"可用来替代英文对应词"stakeholder"。

3.4

风险源　risk source

可能单独或共同引发风险(3.1)的要素。

3.5

事件　event

某些特定情形的产生或变化。

注 1：一个事件可包括一个或多个情形，并且可由多个原因导致。

注 2：事件可能是预期会发生但没发生的事情，也可能是预期不会发生但却发生的事情。

注 3：某事件有可能是风险源。

3.6

后果　consequence

某事件(3.5)对目标影响的结果。

注 1：后果可以是确定的，也可以是不确定的；对目标的影响可以是正面的，也可以是负面的；可以是直接的，也可以