众信联诚检验认证（厦门）有限公司

Zhongxin Liancheng Inspection and Certification (Xiamen) Co., Ltd.

风险管理体系要求

文件编号：CTS /F-ZXLC-032-2025

文件版次：A/0 版

编　　制：文件编制小组

审　　核：陈丽芳

批　　准：程洁

受控状态：受控

发布日期：2025 年 8 月 25 日　　实施日期：2025 年 9 月 15 日

目录

地址:福建省厦门火炬高新区软件园三期集美北大道 1108 号 1801-1 室
电话：0592-5921023　　邮箱：bjzxlc2021@163.com

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

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。

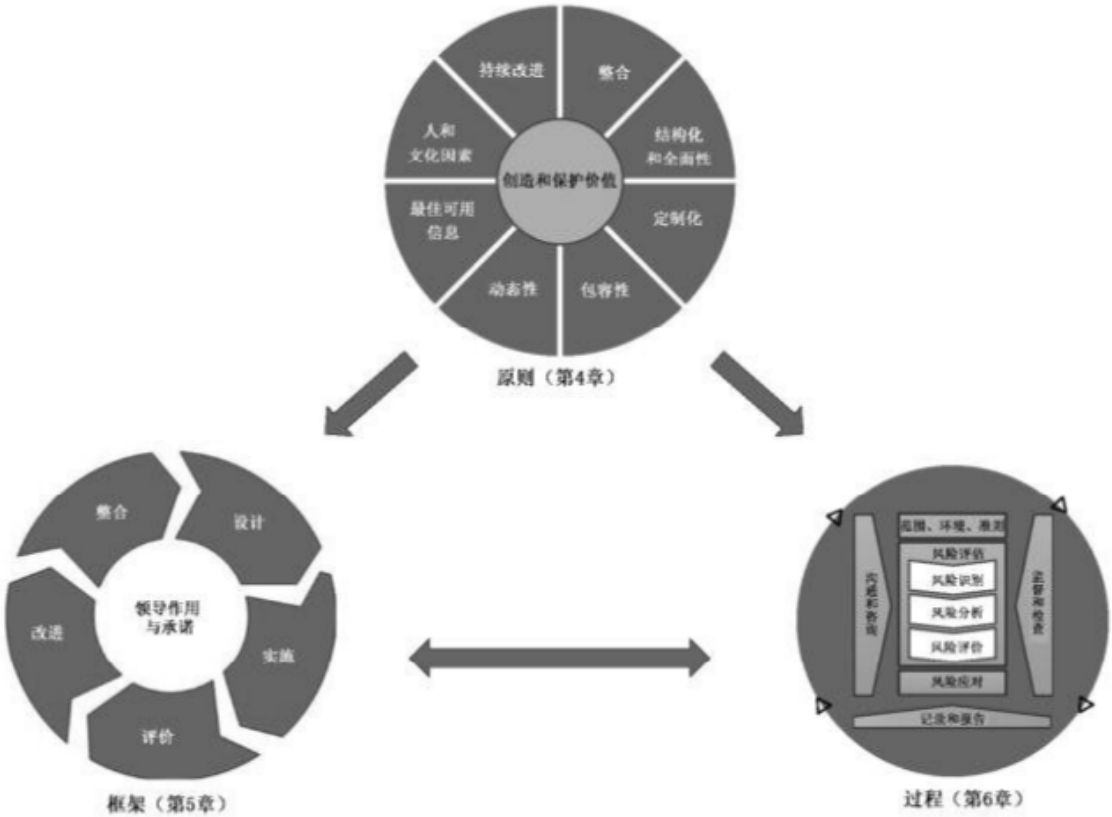

图 1　原则、框架和过程

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

是间接的。

注 2：后果可以定性或定量表述。

注 3：任何后果都可能通过连锁反应和累积效应升级。

3.7

可能性　likelihood

某件事发生的概率。

注 1：在风险管理术语中，无论是以客观的或主观的、定性或定量的方式来定义、度量或确定，还是用一般词汇或数学术语来描述(如概率，或一定时间内的频率)，"可能性"都用来表示某件事发生的概率。

注 2："可能性(likelihood)"这一英语词汇在一些语言中没有直接与之对应的词汇，因此经常用"概率(probability)"这个词代替。不过，在英语中，"概率"常常被狭义地理解为一个数学词汇。因此，在风险管理术语中，"可能性"有着与许多语言中使用的"概率"一词相同的解释，而不局限于英语中"概率"一词的意义。

3.8

控制　control

保持和(或)改变风险(3.1)的措施。

注 1：控制包括但不限于保持和/或改变风险的任何流程、策略、措施、操作或其他行动。

注 2：控制并非总能取得预期的改变效果。

4　原则

风险管理的目的是创造和保护价值。风险管理能够改善绩效、鼓励创新、支持组织目标的实现。

图 2 列出的这些原则，为有效和高效的风险管理提供指导，阐述了风险管理的意图、目的和价值。这些原则是风险管理的基础，可在确立组织风险管理框架和过程时认真考虑。这些原则有助于组织管理不确定性对目标的影响。

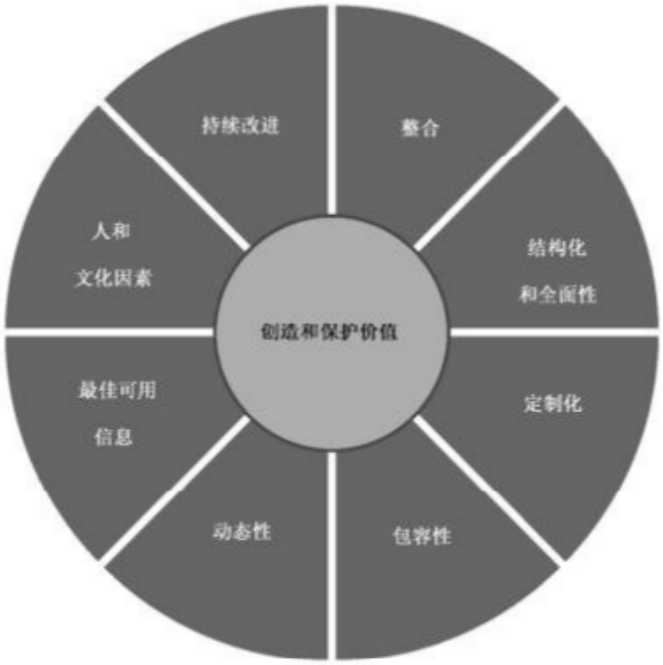

图 2　原则

有效的风险管理需要满足图 2 中列举的原则，其进一步解释如下。

a)　整合

风险管理是组织所有活动的有机组成部分。

注：将风险管理的原则、框架和过程融入组织其他管理活动及其制度办法，有助于推动风险管理的落实。

b) 结构化和全面性

采用结构化和全面性的方法开展风险管理，有助于获得一致的和可比较的结果。

c) 定制化

组织根据自身目标所对应的内外部环境，定制设计风险管理框架和过程。

d) 包容性

利益相关者适当、及时的参与，可以使他们的知识、观点和认知得到充分考虑。这样有助于提高组织的风险意识，并促进风险管理信息的充分沟通。

e) 动态性

随着组织内外部环境的变化，组织面临的风险可能会出现、变化或消失。风险管理以适当、及时的方式预测、发现、确认和应对这些变化和事件。

f) 最佳可用信息

风险管理的信息输入是基于历史信息、当前信息和未来预期的。在风险管理过程中宜明确考虑与这些信息和预期相关的限制条件和不确定性。信息宜及时、清晰，并且是有关的利益相关者可获得的。

g) 人和文化因素

人的行为和文化在各个层级和阶段显著影响着风险管理的各个方面。

h) 持续改进

通过不断学习和实践，持续改进风险管理。

5 框架

5.1 概述

风险管理框架的目的是协助组织将风险管理纳入重要的活动和职能中。风险管理的有效性取决于其与组织治理及决策制定的整合情况。这需要利益相关者尤其是最高管理层的支持。

框架制定包含在整个组织中整合、设计、实施、评价和改进风险管理。图 3 列举了风险管理框架的要素。

图 3 框架

组织宜对其现有的风险管理实践及过程进行评价，并在上述框架内对评价出的差距进行改进优化。框架内各要素及其协同运作的方式宜结合组织需求进行针对性地设计。

5.2 领导作用和承诺

最高管理层和监督机构需确保将风险管理融入所有组织活动中，通过以下活动展现领导作用和承诺：

——针对性地设计和实施框架的所有要素；

——发布风险管理声明或方针，内容包括制定风险管理方法、计划或行动方案；

——确保为管理风险配置必要的资源；

——在组织内的相应层级分配权限、职责和责任。

这样做有助于组织：

——使风险管理与自身目标、战略和文化相协同；

——识别并履行组织的所有义务及自愿承诺；

——确定可承担或不可承担的风险数量和类型，以指导风险准则的制定，确保与组织及利益相关者沟通；

——与组织及利益相关者沟通风险管理的价值；

——促进对风险的系统性监测；

——确保风险管理框架适应组织环境。

最高管理层负责管理风险，监督机构负责监督风险管理。通常对监督机构的要求或预期是：

——确保组织在设定目标时，充分考虑相关风险；

——了解组织在实现组织目标的过程中所面临的风险；

——确保风险管理体系能够高效实施和运作；

——确保这些风险相对于组织目标而言是适当的；

——确保这些风险及其管理的信息得到适当沟通。

5.3 整合

风险管理的整合有赖于对组织结构及内外部环境的理解。组织结构因组织目的、目标和复杂程度而异；在组织结构的每一部分都需要进行风险管理。组织内部的所有人都有管理风险的责任。

组织的治理结构决定组织的运营过程、内外部关系以及实现目标所需的规章制度、程序和实务。组织的管理架构将治理要求转化为战略和相应的目标，以达到可持续发展所需要的绩效水平。确定组织内部的风险管理职责和监督角色是组织治理不可或缺的内容。

风险管理与组织的整合是一个动态、循环提升的过程，宜结合组织需求和文化量身定制。风险管理不是孤立的，而是组织目的、治理、领导作用和承诺、战略、目标和运营的一部分。

5.4 设计

5.4.1 理解组织及其环境

在设计风险管理框架时，组织需审视并了解其内外部环境。

需审视的组织外部环境包括但不限于：

——国际、国内、区域或地方的社会、文化、政治、法律、监管、金融、技术、经济、自然环境；

——对组织目标产生影响的关键驱动因素和趋势；

——与外部利益相关者的关系，以及他们的认知、价值取向、需求和期望；

——合同关系和承诺；

——组织所处关系网络的复杂性及依赖关系。

需审视的组织内部环境包括但不限于：

——愿景、使命和价值观；

——治理方式、组织结构、职能、责任和绩效考核；

——战略、目标和方针；

——组织文化；

——组织采用的标准、指南和模型；

——组织在资源和知识方面所具备的能力(即资本、时间、人力、知识产权、程序、系统和技术等)；

——数据、信息系统和信息流；

——与内部利益相关者的关系，充分考虑其认知和价值取向；

——合同关系和承诺；

——相互依赖性和相互关联性。

5.4.2 明确表达风险管理承诺

最高管理层和监督机构可通过政策、声明或其他形式，表达并展现自身对风险管理的持续承诺，以明确传达组织有关风险管理的目标和承诺。风险管理承诺包括但不限于：

——组织的风险管理目的及其与组织目标和其他方针的联系；

——强化将风险管理融入组织整体文化的要求；

——引导将风险管理融入组织核心业务活动和决策制定过程中；

——明确权限、责任和职责；

——配置必要的资源；

——处理相互冲突目标的方式；

——组织绩效指标的度量和报告；

——回顾和改进。

组织宜在其内部传达风险管理承诺并适时向利益相关者传达。

5.4.3 明确组织角色、权限、职责和责任

最高管理层和监督机构宜明确组织相关角色的风险管理责任、职责和权限，并与组织所有层级沟通，且需要：

——强调风险管理是一项核心职责；

——指定有责任和权限管理风险的个人(风险责任人)。

5.4.4 资源配置

最高管理层和监督机构宜确保为风险管理分配适当的资源，包括但不限于：

——人力、技能、经验和能力；

——组织用于风险管理的程序、方法和工具；

——文件化的过程和程序；

——信息和知识管理系统；

——专业发展和培训需要。

组织需考虑现有资源的能力和局限性。

5.4.5 沟通和咨询

为支持风险管理框架和促进风险管理的有效运用，组织需建立经批准的沟通和咨询方法。沟通主

要是与目标受众分享信息。咨询主要是通过获取参与者的反馈，为制定决策或其他活动提供建议。沟通和咨询的方法和内容宜反映有关利益相关者的期望。

沟通和咨询宜及时，确保相关信息得到适当的收集、整理、汇总和分享，并适时提供反馈和做出改进。

5.5 实施

组织宜通过以下工作实施风险管理框架：

——制定适当的实施计划，包括时间和资源等要素；

——识别组织内各类决策制定的人员、时间、位置和方法；

——必要时，对当前的决策程序进行调整；

——确保组织开展风险管理的工作安排得到清晰的理解和执行。

风险管理框架的成功实施，需要利益相关者的参与和重视。这样能够使组织明确地处理决策中的不确定性；同时还能确保组织在面对新的或后续的不确定性时及时做出反应。

通过恰当地设计和实施风险管理框架，可以确保将风险管理过程融入组织内部所有活动（包括决策制定）之中，并将充分考虑内外部环境的变化。

5.6 评价

评价风险管理框架的有效性，组织宜：

——根据组织设计和实施风险管理框架的目的、实施计划、绩效指标和预期表现效果，定期分析风险管理框架的实施效果；

——确定风险管理框架是否仍适用于支持组织目标的实现。

5.7 改进

5.7.1 调整

组织宜持续监控和更新风险管理框架，以适应内外部环境的变化，这样有助于提升组织价值。

5.7.2 持续改进

组织宜持续改进风险管理框架的适用性、充分性、有效性以及风险管理过程与其他管理活动的整合方式。

当识别出相关差距或改进空间后，组织宜制定改进计划和任务，并分配给相关负责人实施。这些改进计划和任务的实施，有助于加强组织的风险管理。

6 过程

6.1 概述

风险管理过程是将政策、程序和实践系统地应用于沟通和咨询、建立环境、风险评估、风险应对、监督和检查、记录和报告等活动。图4给出了风险管理过程。

风险管理过程是组织管理和决策的有机组成部分，需融入组织的架构、运营和流程中。它可以应用在战略、运营、项目群或单个项目层面。

风险管理过程在组织中的应用可以是多方面的，可根据组织目标定制，并与其所处的内外部环境相适应。

在整个风险管理过程中，需要考虑人的行为因素和文化因素的动态性和多变性。

虽然风险管理过程通常表现为按一定的顺序开展，但在实践中是一个循环提升的过程。

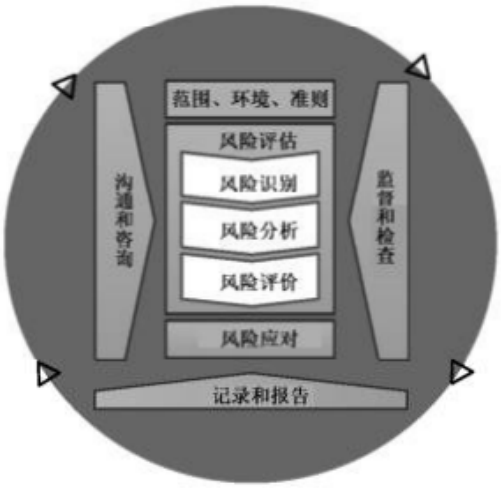

图 4　过程

6.2　沟通和咨询

沟通和咨询的目的是帮助利益相关者理解风险、明确制定决策的依据以及采取特定管理措施的原因。沟通是为了促进对风险的认识和理解，咨询则是为了获取反馈和信息，以支持决策制定。两者的密切协调将促进信息交换的真实性、及时性、相关性、准确性和可理解性，并能兼顾到信息的保密性、完整性和个人隐私保护。

在风险管理过程的所有阶段，均需与相关的内外部利益相关者沟通并咨询其意见。

沟通和咨询的目标是：

——为风险管理过程的每个步骤汇集不同领域的专业知识；

——确保在界定风险准则和评价风险时适当考虑不同观点；

——提供充分信息，以促进对风险的全面了解和决策制定；

——使受风险影响的群体形成包容意识和责任意识。

6.3　范围、环境、准则

6.3.1　概述

确定范围、环境和准则的目的，在于有针对性地设计风险管理过程，以实现有效的风险评估和恰当的风险应对。范围、环境和准则包括界定过程范围、理解内外部环境和界定评定准则。

6.3.2　界定范围

组织宜界定其风险管理活动的范围。

由于风险管理过程可应用于不同层面(如战略、运营、项目群、单个项目或其他活动)，所以明确风险管理过程的范围、目标及其与组织目标的一致性十分重要。

规划风险管理实施路径时，所考虑的事项包括：

——目标和需要做的决策；

——过程中各个步骤的预期结果；

——时间、地点、具体包含和排除的事项；

——适当的风险评估工具和技术；

——所需的资源、责任和需要保留的记录；

——与其他项目、过程和活动的关系。

6.3.3 内外部环境

内外部环境是指组织设定并实现自身目标所依赖的环境。

风险管理环境的确定，宜建立在对组织运营所处的内外部环境的理解上，并反映出实施风险管理活动的具体场景。理解环境之所以重要，是因为：

——风险管理是在组织目标和活动的环境下进行的；

——组织方面的因素可能是一种风险源；

——风险管理过程的目的和范围宜与整个组织的目标相互关联。

组织可在考虑 5.4.1 所述因素的基础上，建立风险管理过程的内外部环境。

6.3.4 界定风险准则

组织宜基于其目标，确定其所能承受的风险数量和类型，组织还需界定评价风险重要性的准则并支持决策过程。风险准则宜与风险管理框架相一致，并根据相关活动的具体目的和范围进行针对性的设计。风险准则宜反映组织的价值观、目标和资源，并与组织的风险管理方针和声明相一致。在界定风险准则时宜考虑组织的义务和利益相关者的意见。

虽然风险准则可在风险评估过程之初确定，但它是动态变化的，因此宜持续审视并于必要时进行修改。

在设定风险准则时，以下方面宜加以考虑：

——可能影响结果和目标的不确定因素的性质和类型(包括有形的和无形的)；

——如何界定和度量后果(包括正面的和负面的)和可能性；

——时间相关因素；

——采用度量标准的一致性；

——如何确定风险等级；

——如何考虑多项风险的组合及顺序；

——组织的风险容量。

6.4 风险评估

6.4.1 概述

风险评估是风险识别、风险分析和风险评价的整个过程。

风险评估宜系统地、循环地、协作性地开展，并充分考虑利益相关者的观点。风险评估宜使用最佳可用信息，在必要时可通过进一步调查加以补充。

6.4.2 风险识别

风险识别的目的是发现、确认和描述可能有助于或妨碍组织实现目标的风险。采用相关、适当、最新的信息对于识别风险非常重要。

组织可使用一系列技术来识别可能影响一个或多个目标的不确定性。识别风险宜考虑以下因素及相互之间的关系：

——有形和无形的风险源；

——原因和事件；

——威胁和机遇；

——脆弱性和应对能力；
——内外部环境变化；
——新兴风险；
——资产和资源的性质和价值；
——后果及其对目标的影响；
——知识的局限性和信息的可靠性；
——与时间有关的因素；
——识别风险所涉及人员的偏见、假设和看法。

不管风险源是否在组织控制范围内，都宜对风险进行识别。需考虑风险带来的多于一种的结果，这些结果可能导致各种有形或无形的后果。

6.4.3 风险分析

风险分析的目的是了解风险性质及其特征，必要时包括风险等级。风险分析包括对不确定性、风险源、后果、可能性、事件、情境、控制措施及其有效性进行详尽考虑。一个事件可能有多种原因和后果，可能影响多个目标。

开展风险分析的细致和复杂程度可有所不同，具体取决于分析目的、信息的可获得性和可靠性以及可用的资源。分析技术可以是定性的、定量的或者定量和定性相结合的，具体视情况和预期用途而定。

风险分析可考虑以下因素：
——事件的可能性及后果；
——后果的性质及影响程度；
——复杂性和关联性；
——时间相关因素及波动性；
——现有控制措施的有效性；
——敏感性和置信水平。

风险分析受观点分歧、偏见、风险认知及判断的影响。其他影响包括所使用信息的质量、所做的假设和排除情形、所使用技术的局限性以及开展分析的方式。这些影响均宜考虑、记录，并与决策者沟通。

高度不确定的事件可能难以量化。这在分析具有严重影响的事件时可能是一个问题。在此情况下，综合使用多种分析技术通常能提供更合理的观点。

风险分析可为风险评价提供信息输入，也可为是否需要和如何应对风险，及采取最适宜的策略和方法提供信息支撑。当面对不同类别和不同等级的风险需要做出抉择时，风险分析结果可为决策提供深刻见解。

6.4.4 风险评价

风险评价的目的是支持决策。风险评价是将风险分析结果和既定风险准则相比较，以确定是否需要采取进一步行动。风险评价可促成以下决定：
——不采取进一步行动；
——考虑风险应对方案；
——开展进一步分析，以更全面地了解风险；
——维持现有的控制措施；
——重新考虑目标。

决策宜考虑到更广泛的环境，以及对内外部利益相关者的实际和预期影响。

风险评价的结果宜予以记录、沟通，然后在组织适当层级予以确认。

6.5 风险应对

6.5.1 概述

风险应对的目的是选择和实施风险处理方案。

风险应对是一个循环提升的过程，包括：

——制定和选择风险应对方案；

——计划和实施风险应对措施；

——评估风险应对措施的成效；

——确定剩余风险是否可接受；

——若不可接受，采取进一步应对措施。

6.5.2 选择风险应对方案

选择最合适的风险应对方案，可在实现目标获得的潜在收益和付出的成本、耗费的精力或由此引发的不利后果之间进行权衡。

风险应对方案之间不一定是相互排斥的，也不一定适用于所有情形。风险应对方案涉及以下一个或多个方面：

——决定不开始或退出会导致风险的活动，来规避风险；

——承担或增加风险，以寻求机会；

——消除风险源；

——改变可能性；

——改变后果；

——分担风险（如通过签订合同，购买保险）；

——慎重考虑后决定保留风险。

采取风险应对的理由不仅考虑经济因素，还宜考虑所有的组织义务、自愿性承诺和利益相关者的观点。可依据组织目标、风险准则和可用资源选择风险应对方案。

选择风险应对方案时，组织宜考虑利益相关者的价值观、认知和潜在参与程度以及与其沟通和协商的最佳方式。虽然效果相同，但某些风险应对方案相比其他方案更能被某些利益相关者接受。

虽然经过谨慎的设计和实施，但风险应对不一定产生预期结果，甚至可能产生意外的后果。监督和检查宜作为风险应对实施的一部分，以确保不同形式的风险应对持续有效。

风险应对还可能产生需要加以管理的新风险。

如果没有可用的应对方案或者应对方案不足以改变风险，组织可将这些风险记录下来，并持续跟踪。

决策者和其他利益相关者宜了解经风险应对后剩余风险的性质和程度。组织可记录剩余风险，对其进行监督和检查，并适时采取进一步应对措施。

6.5.3 编制和实施风险应对计划

风险应对计划的目的是明确如何实施所选定的应对方案，以便相关人员了解应对计划，并监测计划实施进度。应对计划宜明确指明实施风险应对的顺序。

应对计划宜纳入管理计划和组织运营过程中，并征询利益相关者意见。

应对计划中提供的信息应包括：

——选择应对方案的理由，包括可获得的预期收益；

——批准和实施计划的责任人；

——拟采取的措施行动，包括应急预案；
——所需要的资源，包括风险准备；
——绩效考核的标准和方法；
——限制因素；
——必要的报告和监测；
——行动预期开展和完成的时间。

6.6 监督和检查

监督和检查的目的是确保和提升风险管理过程设计、实施和结果的质量和成效。宜将对风险管理过程的持续监督和定期检查及其结果作为风险管理过程内计划性工作的组成部分，并明确界定责任。

监督和检查宜贯穿于风险管理过程的所有阶段。监督和检查包括计划、收集和分析信息、记录结果和提供反馈。

监督和检查的结果宜纳入组织绩效管理、考核和报告活动中。

6.7 记录和报告

宜通过适当的工作机制，记录和报告风险管理过程及其结果。记录和报告旨在：
——在组织各层级通报风险管理活动及结果；
——为决策制定提供信息；
——改进风险管理活动；
——促进与利益相关者的互动，包括各层级的风险责任人。

在决定创建、留存和处理所记录信息时，宜考虑(但不限于)信息的用途、敏感性及内外部环境。

报告是组织治理不可或缺的一部分，可提升与利益相关者的沟通质量，并为最高管理层和监督机构履行职责提供支持。报告的考虑因素包括但不限于：
——区分利益相关者及其具体信息需求和要求；
——报告成本、频率和及时性；
——报告方式；
——信息与组织目标和决策的相关性。

参 考 文 献

[1] IEC 31010 Risk management—Risk assessment techniques

华信金泰检验认证有限公司

Huaxin Jintai Inspection and Certification Co., Ltd.

风险管理体系要求

文件编号：CTS HXJT/YQMS-08-2026

文件版次：A/0

编　　制：文件编制小组

审　　核：

批　　准：

受控状态：受控

发布日期：2026 年 03 月 18 日　　实施日期：2026 年 03 月 18 日

文件修改记录

修订说明	修订页数	修订日期	批准

目录

地址： 河北省石家庄市长安区广安街 91 号世纪方舟 B-26-2203,2206

电话：0311-68008520 邮箱：hxjttc@hxjttc.com

风险管理体系 要求

1 范围

1.1 本文件规定了组织建立、实施、保持和改进风险管理体系的要求，旨在帮助组织通过系统管理不确定性对目标的影响，创造和保护价值，支持组织战略实现与绩效提升。

1.2 本文件适用于所有类型和规模的组织（如企业、事业单位、政府机构等），可应用于组织全生命周期的各类活动，包括战略规划、运营管理、项目实施、服务提供等不同层级的决策与实践。

1.3 本文件不强制规定具体的风险管理技术方法，组织可根据自身内外部环境、目标特性及风险类型，定制化选择适用的工具与流程，确保与 GB/T 24353-2022/ISO 31000:2018 的原则和框架保持一致。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件；凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 19001-2016 质量管理体系 要求

GB/T 24353-2022/ISO 31000:2018 风险管理 指南

3 术语和定义

3.1 风险（risk）：不确定性对目标的影响（注：影响可正面（机遇）或负面（威胁），可通过风险源、潜在事件、后果及可能性描述）。

3.2 风险管理（risk management）：指导和控制组织与风险相关的协调活动。

3.3 利益相关者（stakeholder）：可影响、被影响或自认为会被组织决策或活动影响的个人或组织。

3.4 风险源（risk source）：可能单独或共同引发风险的要素）。

3.5 事件（event）：某些特定情形的产生或变化（注：可由多原因导致，可能是 “预期发生未发生” 或 “预期未发生却发生”，也可能成为风险源）。

3.6 后果（consequence）：事件对目标影响的结果（注：可直接 / 间接、正面 / 负面，可定性或定量表述，可能通过连锁反应升级）。

3.7 可能性（likelihood）：某事件发生的概率（注：可定性 / 定量描述，含频率、概率等表述方式）。

3.8 控制（control）：保持和 / 或改变风险的措施（注：包括流程、策略、操作等，未必总能实现预期效果）。

3.9 组织（organization）：为实现目标而具有职责、权限和相互关系的个人或群体。

4 组织环境

4.1 理解组织及其环境

4.1.1 组织应系统识别并分析影响风险管理体系有效性的内外部环境因素，确保风险管理与组织目标适配：

外部环境：包括国际 / 国内 / 区域的社会文化、政治法律、监管要求、金融经济、技术发展、自然环境，以及关键驱动趋势、外部利益相关者关系、合同承诺、供应链依赖等；

内部环境：包括组织愿景、使命、价值观，治理结构、组织结构与职责分工，战略目标与方针，组织文化，资源能力（人力、资本、技术、知识产权等），信息系统与信息流，内部利益相关者关系等。

4.1.2 组织应定期评审内外部环境因素的变化，更新分析结果，并作为风险管理体系策划与调整的输入。

4.2 理解利益相关者的需求和期望

4.2.1 组织应识别与风险管理相关的利益相关者（如客户、员工、股东、监管机构、供应商、社区等），明确其对风险的认知、需求及期望（如监管合规要求、客户对风险的容忍度、员工安全诉求等）。

4.2.2 组织应将利益相关者的合理需求与期望转化为风险管理的具体要求（如风险准则、应对目标），并在体系运行中持续沟通。

4.3 确定风险管理体系的范围

4.3.1 组织应基于自身目标、内外部环境及利益相关者需求，界定风险管理体系的应用范围，明确：

a） 适用的活动层级（如战略层、运营层、项目层）；

b） 覆盖的业务领域（如生产、研发、采购、销售）；

c） 时间边界（如短期运营、长期战略周期）；

d） 排除的活动（若有，需说明理由并记录）。

4.3.2 体系范围应形成文件化信息，确保组织内部及相关利益相关者理解一致。

4.4 风险管理体系及其过程

4.4.1 组织应建立结构化的风险管理体系，将风险管理的原则（整合、结构化、定制化等）、框架（领导作用、整合、设计等）及过程（沟通咨询、风险评估、应对等）融入组织现有管理活动（如质量管理、安全管理），避免体系孤立。

4.4.2 组织应明确风险管理体系的过程交互关系（如 “风险评估” 为 “风险应对” 提供输入，“监督检查” 为 “改进” 提供依据），形成闭环管理机制。

5 领导作用

5.1 领导作用和承诺

最高管理层应通过以下活动展现对风险管理体系的领导作用和承诺：

a) 确保风险管理融入组织所有活动（如战略制定、运营决策），而非独立流程；

b) 发布风险管理方针，明确组织风险管理的目的、方法及与目标的关联；

c) 为风险管理配置必要资源（人力、技术、资金等），确保体系有效运行；

d) 明确各层级风险管理的职责与权限（如指定 “风险责任人”），并在组织内传达；

e) 定期参与风险管理评审，监督体系有效性，解决体系运行中的重大问题。

5.2 风险管理方针

5.2.1 最高管理层应批准并发布风险管理方针，方针应：

a) 与组织愿景、使命及战略目标一致；

b) 体现风险管理的核心原则；

c) 明确组织的风险容量（可承受的风险类型与等级）及合规义务；

d) 为风险管理目标的制定提供框架。

5.2.2 风险管理方针应形成文件化信息，在组织内全员传达，并适时向利益相关者公开（如通过官网、年报）。

5.3 组织的岗位、职责和权限

5.3.1 组织应在各层级明确风险管理的岗位、职责与权限，确保：

a) 最高管理层：对风险管理体系有效性负总责，审批重大风险应对方案；

b) 风险责任人：负责特定领域 / 活动的风险识别、评估、应对实施与监控；

c) 全体员工：参与所在岗位的风险识别，执行既定的风险控制措施；

d) 监督机构：监督风险管理体系的实施与合规性。

5.3.2 职责与权限应形成文件（如岗位说明书、风险管理职责矩阵），并在组织内公示。

6 策划

6.1 应对风险和机遇的措施

6.1.1 组织应基于对自身环境及利益相关者需求的理解，识别与风险管理体系相关的风险和机遇。

6.1.2 组织应策划应对这些风险和机遇的措施，确保：

a) 风险得到控制，避免体系失效；

b) 机遇得以利用，提升体系有效性；

c) 措施与组织目标及风险容量匹配，并形成文件化的应对计划。

6.2 风险管理目标及其实现的策划

6.2.1 组织应在风险管理方针框架下，制定可测量、可实现、相关联、有时限（SMART）

的风险管理目标，覆盖战略、运营、项目等不同层级，例如：

a） 战略层：“三年内将供应链中断风险发生率降低 30%”；

b） 运营层：“季度内完成关键设备故障风险的全流程评估”。

6.2.2 组织应策划目标实现的路径，明确：

a） 责任部门 / 人员；

b） 所需资源（如培训、工具）；

c） 实施时间表；

d） 监控与评价方法。

6.2.3 风险管理目标应定期评审，并根据内外部环境变化（如法规更新、市场波动）调整。

6.3 变更的策划

6.3.1 当组织内外部环境发生重大变化（如并购重组、法规修订、技术迭代）时，应评估变化对风险管理体系的影响（如风险源新增、风险准则失效）。

6.3.2 组织应策划体系变更的方案，明确变更范围、步骤、责任及验证方法，确保变更后体系仍符合本文件要求及 GB/T 24353-2022/ISO 31000:2018 的框架，避免变更引发新的风险。

6.3.3 变更实施后，应验证效果并记录，确保体系持续有效运行。

7 支持

7.1 资源

组织应确定并提供建立、实施、保持和改进风险管理体系所需的资源，包括：

a） 人力资源：配备具备风险管理知识、技能和经验的人员（如风险分析师、内审员），必要时引入外部专家；

b） 基础设施：提供风险评估工具（如风险矩阵、数据分析软件）、信息系统（如风险数据库、监控平台）及办公环境；

c） 过程运行环境：营造重视风险的组织文化（如定期开展风险意识培训），建立开放的沟通机制；

d） 监视和测量资源：确保风险监测工具（如设备传感器、数据采集系统）的准确性和适用性。

7.2 能力

7.2.1 组织应识别与风险管理相关的岗位能力要求（如风险评估技能、法规解读能力），确保相关人员具备满足要求的能力。

7.2.2 组织应通过培训、在职辅导、外部认证等方式提升人员能力，例如：

a） 对全员开展 “风险识别基础” 培训；

b） 对风险责任人开展 “定量风险分析方法” 专项培训。

7.2.3 组织应定期评价能力提升效果，并保留培训及评价记录。

7.3 意识

组织应确保全体员工理解：

a) 风险管理方针的内容及重要性；

b) 自身岗位的风险管理职责；

c) 风险对组织目标实现的影响；

d) 不当风险管理可能导致的后果（如合规处罚、经济损失）。

意识提升可通过内部宣传、案例分享、定期会议等方式实现。

7.4 沟通

7.4.1 组织应建立内外部风险管理沟通机制，明确沟通的内容、时机、方式及责任人：

内部沟通：如部门间风险信息共享、重大风险上报；

外部沟通：如向监管机构提交风险报告、向供应商传达风险控制要求。

7.4.2 沟通应确保信息真实、及时、准确、可理解，并考虑信息的敏感性（如商业秘密），必要时采取保密措施。

7.4.3 组织应收集沟通对象的反馈（如利益相关者对风险应对的意见），并用于体系改进。

7.5 文件化信息

7.5.1 组织应确定风险管理体系所需的文件化信息，包括：

a) 必要的文件：风险管理方针、目标、体系范围、风险准则、风险评估程序、应对计划模板等；

b) 必要的记录：风险识别清单、风险分析报告、应对措施实施记录、监督检查结果、管理评审报告等。

7.5.2 组织应控制文件化信息的创建、审批、发放、更改、保存及销毁，确保：

a) 文件化信息清晰、易获取、版本有效；

b) 记录保存期限符合法规要求及组织需求。

8 运行

8.1 运行策划和控制

组织应策划并控制与风险管理相关的运行过程，确保：

a) 运行过程符合风险管理方针、目标及风险准则；

b) 明确各运行环节的输入、输出及责任人；

c) 对运行过程中的变更进行控制，避免非预期后果；

d) 保留运行过程的记录。

8.2 沟通和咨询

8.2.1 沟通和咨询应贯穿风险管理运行的全流程，组织应：

a） 在风险评估前，咨询利益相关者以获取风险识别的输入；

b） 在风险应对中，向相关方（如供应商、客户）沟通应对措施的要求及影响；

c） 在风险监控后，向最高管理层及利益相关者通报风险变化及应对效果。

8.2.2 沟通和咨询应采用适配的方式（如会议、问卷、访谈），确保不同利益相关者的知识、观点被充分考虑。

8.3 范围、环境与准则界定

8.3.1 组织应在每次具体风险管理活动（如某项目风险评估、某季度运营风险审核）前，重新确认或调整范围、环境与准则：

a） 范围界定：明确本次活动覆盖的业务环节、时间周期；

b） 环境分析：结合最新内外部信息，更新环境因素；

c） 准则界定：基于组织目标及风险容量，明确风险评价的标准。

8.3.2 范围、环境与准则应形成文件（如《XX 风险评估任务书》），经相关方审批后执行。

8.4 风险评估实施

风险评估是风险识别、风险分析、风险评价的系统性过程，组织应按以下要求实施：

8.4.1 风险识别

8.4.1.1 组织应采用结构化方法（如头脑风暴、检查表、SWOT 分析、故障树分析）识别可能影响目标实现的风险（威胁与机遇），覆盖：

a） 有形 / 无形风险源；

b） 潜在事件及原因；

c） 事件的直接 / 间接后果；

d） 内外部环境变化带来的新兴风险。

8.4.1.2 风险识别结果应记录为《风险清单》，包含风险名称、风险源、潜在事件、后果描述等信息。

8.4.2 风险分析

8.4.2.1 组织应基于 “最佳可用信息”（历史数据、行业案例、专家判断），分析已识别风险的性质与特征，包括：

a） 可能性分析：定性或定量评估事件发生的概率；

b） 后果分析：定性或定量评估事件对目标的影响；

c） 现有控制措施有效性分析：评估当前措施对降低风险的作用。

8.4.2.2 风险分析结果应形成分析报告，为风险评价提供依据；对高度不确定的风险，应采用多种分析方法交叉验证。

8.4.3 风险评价

8.4.3.1 组织应将风险分析结果与既定风险准则对比，确定风险等级（如 “低、中、高、重大”），并决策：

a） 风险等级低于准则：不采取进一步行动，持续监控；

b） 风险等级符合 / 超过准则：考虑风险应对方案；

c） 信息不足：开展补充分析。

8.4.3.2 风险评价结果应经相关层级审批（如重大风险报最高管理层审批），并更新至《风险清单》。

8.5 风险应对策划与实施

8.5.1 风险应对方案选择

组织应基于风险评价结果，结合成本 - 收益分析、利益相关者期望及组织资源，选择适宜的风险应对方案：

a） 规避风险：退出或不开展引发风险的活动；

b） 利用机遇：增加风险发生概率或扩大正面后果；

c） 消除风险源：移除引发风险的要素；

d） 改变可能性：降低或提高事件发生概率；

e） 改变后果：减轻或放大事件影响；

f） 分担风险：通过合同、保险等方式转移部分风险；

g） 保留风险：经评估后接受风险（。

8.5.2 风险应对计划编制

8.5.2.1 组织应将选定的应对方案转化为可执行的风险应对计划，明确：

a） 应对措施；

b） 责任部门 / 责任人；

c） 所需资源；

d） 实施时间表；

e） 应急预案；

f） 效果评价标准。

8.5.2.2 风险应对计划应与组织的运营计划整合，确保资源同步配置。

8.5.3 风险应对实施与监控

8.5.3.1 责任部门应按风险应对计划实施措施，定期向风险责任人汇报进展；对实施中的问题，应及时上报并调整计划。

8.5.3.2 组织应监控应对措施的有效性，评估：

a） 措施是否按计划执行；

b） 风险等级是否降至预期水平；

c） 是否产生新的风险。

8.5.3.3 应对措施实施完成后，应验证效果并记录；对未达预期的，应重新开展风险评估并制定新的应对方案。

8.6 运行过程监控

8.6.1 组织应建立持续的风险监控机制，对运行过程中的风险及应对措施进行跟踪，包括：

a） 日常监控：通过巡检、数据监测实时捕捉风险变化；

b） 定期检查：按计划开展风险审核，评估风险等级、应对措施有效性及体系符合性。

8.6.2 监控过程中发现风险等级超出准则或应对措施失效时，应启动应急程序（如触发应急预案、上报最高管理层），并及时调整应对方案。

8.6.3 监控结果应记录为《风险监控报告》，作为绩效评价和体系改进的输入。

9 绩效评价

9.1 监视、测量、分析和评价

9.1.1 组织应确定监视和测量的内容，包括：

a） 风险管理体系的有效性；

b） 风险管理目标的实现情况；

c） 风险水平的变化；

d） 利益相关者的满意度。

9.1.2 组织应选择适宜的监视测量方法，确保数据真实可靠；至少每年开展一次综合分析，评估体系绩效，并形成风险管理绩效分析报告。

9.1.3 分析结果应用于识别体系改进机会。

9.2 内部审核

9.2.1 组织应按计划开展风险管理体系内部审核，至少每年一次，审核内容包括：

a） 体系是否符合本文件要求及组织自身规定；

b） 体系是否得到有效实施和保持；

c） 风险评估、应对、监控等过程的有效性。

9.2.2 组织应制定《内部审核方案》，明确审核范围、频次、准则及审核员资质（审核员应独立于被审核部门）；审核结果应形成《内部审核报告》，包含不符合项及改进建议。

9.2.3 责任部门应针对不符合项制定纠正措施，审核员应验证措施的实施效果。

9.3 管理评审

9.3.1 最高管理层应至少每年一次主持风险管理体系管理评审，输入包括：

a） 内部审核结果；

b） 风险管理绩效分析报告；

c） 风险水平变化；

d） 利益相关者反馈；

e） 体系变更需求。

9.3.2 管理评审应重点评价：

a） 风险管理方针、目标的适宜性；

b） 风险管理体系的有效性、充分性及持续适宜性；

c） 资源配置的合理性。

9.3.3 评审结果应形成《管理评审报告》，明确改进决议，并跟踪决议的落实。

10 改进

10.1 不符合和纠正措施

10.1.1 组织应识别风险管理体系运行中的不符合，分析不符合的原因。

10.1.2 组织应针对原因制定并实施纠正措施，确保：

a） 消除不符合本身；

b） 防止不符合再次发生（如 “培训不足” 需补充专项培训并考核）。

10.1.3 组织应验证纠正措施的效果，记录验证结果；对效果不佳的，应重新分析原因并调整措施。

10.2 持续改进

10.2.1 组织应基于监视测量、内部审核、管理评审及纠正措施的结果，识别风险管理体系的改进机会。

10.2.2 组织应制定持续改进计划，明确改进项目、责任部门、时间表及预期效果；定期评审改进进展，确保改进落地。

10.2.3 组织应鼓励全员参与改进，通过持续改进提升风险管理体系的有效性，更好地支持组织目标实现。