CTS

广东中嘉认证有限公司企业标准

风险管理体系
认证技术规范

2025-08-17发布　　2025-08-17实施

广东中嘉认证有限公司　　发布

目录

前言

本标准按照GB/T 24353-2022/ISO 31000:2018 给出的规则起草。

本标准由广东中嘉认证有限公司起草。

本标准主要起草人：彭一康、邱可为、丁飞、吴峰、罗延君、麦永洪、陈燕。

1、范围

本规范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。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。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、术语和定义

下列术语和定文适用于本文件。

2.1风险

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，潜在事件及后果和可能性来描述。

2.2风险管理

指导和控制组织与风险（2.1）相关的协调活动。

2.3利益相关者

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。

2.4风险源

可能单独或共同应发风险（2.1）的要素。

2.5事件

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。

2.6后果

某事件（2.5）对目标影响的结果。

注1：后果可以使确定的，也可以使不确定的；对目标的影响可以是正面的，也可以使负面的，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。

2.7可能性

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。

2.8控制

保持和（或）改变风险（2.1）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。

3、认证模式

初次认证+监督审核+再认证+非例行监督（必要时）

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。

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。

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：

——针对性设计和实施框架的所有要素；

——发生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检测；

——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欧高效实施和运作；

——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；

——强化将风险管理融人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。

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。

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，咨询则是为不获取反馈相信息，以支持决策制定，两者的密切协调将促进信息交换的真实生、及时性、相关性，准确性可理解性：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存阶段，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不解和决策制定；

——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执择时，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。