中旌认证（上海）有限公司

Zhongjing certification (Shanghai) Co., Ltd

安全风险管理体系 要求

CTS ZJC/R 1033 :2025

（第2版）

编制	审查	批准
技术部	葛龙歆	章弋
发布日期：2025年09月20日		实施日期：2025年09月21日

目　录

前 言

本标准参考 GB/T 24353—2022/ISO 31000:2018《风险管理 指南》和 GB/T 27921:2023《风险管理 风险评估技术》起草，采用 ISO 制定的管理体系标准框架，以提高与其他管理体系标准的协调一致性。

本标准采用过程方法，该方法结合了"策划-实施-检查-处置"(PDCA)循环和基于风险的思维。

过程方法使组织能够策划过程及其相互作用。

PDCA 循环使组织能够确保其过程得到充分的资源和管理，确定改进机会并采取行动。

基于风险的思维使组织能够确定可能导致其过程和安全风险管理体系偏离策划结果的各种因素，采取预防控制，最大限度地降低不利影响，并最大限度地利用出现的机遇。

---

1 范围

本标准为下列组织规定了安全风险管理体系要求：

a) 需要证实其具有稳定识别、评估和应对安全风险的能力，以满足相关方要求及适用法律法规要求；

b) 通过体系的有效应用，包括体系改进的过程，以及保证符合相关方要求和适用的法律法规要求，旨在保护组织价值并增强相关方满意。

本标准规定的所有要求是通用的，旨在适用于各种类型、不同规模和提供不同产品和服务的组织。

注 1：本标准中的"安全风险"指不确定性对组织安全目标的影响，包括但不限于生产安全、信息安全、环境安全等领域的风险。

注 2：法律法规要求可称作法定要求。

---

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 24353—2022/ISO 31000:2018 风险管理 指南
- GB/T 27921:2023 风险管理 风险评估技术
- GB/T 19011 管理体系审核指南

---

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 安全风险 safety risk

不确定性对组织安全目标的影响。

注：安全目标可包括人员安全、资产安全、环境安全、信息安全等方面。

3.3 风险管理 risk management

指导和控制组织与风险相关的协调活动。

3.4 安全风险管理体系 safety risk management system

组织建立方针、目标以及实现这些目标的过程的相互关联或相互作用的一组要素，用于管理安全风险。

3.5 利益相关方 stakeholder

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。

3.6 风险源 risk source

可能单独或共同引发风险的要素。

3.7 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。

3.8 后果 consequence

某事件对目标影响的结果。

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。

3.9 可能性 likelihood

某件事发生的概率。

3.10 控制 control

保持和(或)改变风险的措施。

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。

3.11 风险评估 risk assessment

风险识别、风险分析和风险评价的整个过程。

3.12 风险识别 risk identification

发现、确认和描述可能有助于或妨碍组织实现目标的风险的过程。

3.13 风险分析 risk analysis

了解风险性质及其特征，必要时包括风险等级的过程。

3.14 风险评价 risk evaluation

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的过程。

3.15 风险应对 risk treatment

选择和实施风险处理方案的过程。

---

4 组织环境

4.1 理解组织及其环境

组织应确定与其宗旨和战略方向相关并影响其实现安全风险管理体系预期结果的能力的各种外部和内部因素。

组织应对这些外部和内部因素的相关信息进行监视和评审。

注 1：这些因素可能包括需要考虑的正面和负面要素或条件。

注 2：考虑来自于国际、国内、地区或当地的各种法律法规、技术、竞争、市场、文化、社会和经济环境的因素，有助于理解外部环境。

注 3：考虑与组织的价值观、文化、知识和绩效等有关的因素，有助于理解内部环境。

4.2 理解相关方的需求和期望

由于相关方对组织识别、评估和应对安全风险的能力具有影响或潜在影响，因此，组织应确定：

a) 与安全风险管理体系有关的相关方；
b) 与安全风险管理体系有关的相关方的要求。

组织应监视和评审这些相关方的信息及其相关要求。

4.3 确定安全管理体系的范围

组织应确定安全管理体系的边界和适用性，以确定其范围。

在确定范围时，组织应考虑：

a) 4.1 中提及的各种外部和内部因素；
b) 4.2 中提及的相关方的要求；
c) 组织的安全风险类型和特点。

如果本标准的全部要求适用于组织确定的安全管理体系范围，组织应实施本标准的全部要求。

组织的安全管理体系范围应作为成文信息，可获得并得到保持。该范围应描述所覆盖的安全风险类型，如果组织确定本标准的某些要求不适用于其安全管理体系范围，应说明理由。

只有当所确定的不适用的要求不影响组织确保其安全风险管理的能力或责任，对保护组织价值也不会产生影响时，方可声称符合本标准的要求。

4.4 安全风险管理体系及其过程

4.4.1

组织应按照本标准的要求，建立、实施、保持和持续改进安全风险管理体系，包括所需过程及其相互作用。

组织应确定安全风险管理体系所需的过程及其在整个组织中的应用，且应：

a) 确定这些过程所需的输入和期望的输出；
b) 确定这些过程的顺序和相互作用；
c) 确定和应用所需的准则和方法(包括监视、测量和相关绩效指标)，以确保这些过程的有效运行和控制；
d) 确定这些过程所需的资源并确保其可获得；
e) 分配这些过程的职责和权限；
f) 按照 6.1 的要求应对风险和机遇；
g) 评价这些过程，实施所需的变更，以确保实现这些过程的预期结果；
h) 改进过程和安全风险管理体系。

4.4.2

在必要的范围和程度上，组织应：

a) 保持成文信息以支持过程运行；
b) 保留成文信息以确信其过程按策划进行。

---

5 领导作用

5.1 领导作用和承诺

5.1.1 总则

最高管理者应通过以下方面，证实其对安全管理体系的领导作用和承诺：

a) 对安全管理体系的有效性负责；
b) 确制定安全管理体系的安全方针和安全目标，并与组织环境相适应，与战略方向相一致；
c) 确保安全管理体系要求融入组织的业务过程；
d) 促进使用过程方法和基于风险的思维；
e) 确保安全管理体系所需的资源是可获得的；
f) 沟通有效的安全风险管理和符合安全管理体系要求的重要性；
g) 确保安全管理体系实现其预期结果；
h) 促使人员积极参与，指导和支持他们为安全管理体系的有效性作出贡献；
i) 推动改进；
j) 支持其他相关管理者在其职责范围内发挥领导作用。

注：本标准使用的"业务"一词可广义地理解为涉及组织存在目的的核心活动，无论是公有、私有、营利或非营利组织。

5.1.2 以相关方为关注焦点

最高管理者应通过确保以下方面，证实其以相关方为关注焦点的领导作用和承诺：

a) 确定、理解并持续地满足相关方要求以及适用的法律法规要求；
b) 确定和应对风险和机遇，这些风险和机遇可能影响安全风险管理的能力以及保护组织价值的能力；
c) 始终致力于通过风险管理创造和保护价值。

5.2 方针

5.2.1 制定安全方针

最高管理者应制定、实施和保持安全方针，安全方针应：

a) 适应组织的宗旨和环境并支持其战略方向；
b) 为建立安全目标提供框架；
c) 包括满足适用要求的承诺；
d) 包括持续改进安全管理体系的承诺；
e) 包括创造和保护价值的承诺。

5.2.2 沟通安全方针

安全方针应：

a) 可获取并保持成文信息；
b) 在组织内得到沟通、理解和应用；
c) 适宜时，可为有关相关方所获取。

5.3 组织的岗位、职责和权限

最高管理者应确保组织相关岗位的职责、权限得到分配、沟通和理解。

最高管理者应分配职责和权限，以：

a) 确保安全管理体系符合本标准的要求；
b) 确保各过程获得其预期输出；
c) 报告安全管理体系的绩效以及改进机会，特别是向最高管理者报告；
d) 确保在整个组织中推动风险管理；

e) 确保在策划和实施安全管理体系变更时保持其完整性；
f) 指定有责任和权限管理风险的个人(风险责任人)。

---

6 策划

6.1 应对风险和机遇的措施

6.1.1

在策划安全管理体系时，组织应考虑到 4.1 所提及的因素和 4.2 所提及的要求，并确定需要应对的风险和机遇，以：

a) 确保安全管理体系能够实现其预期结果；
b) 增强有利影响；
c) 预防或减少不利影响；
d) 实现改进；
e) 创造和保护价值。

6.1.2

组织应策划：

a) 应对这些风险和机遇的措施；
b) 如何：
   1) 在安全管理体系过程中整合并实施这些措施；
   2) 评价这些措施的有效性。

应对措施应与风险和机遇对组织安全目标的潜在影响相适应。

注 1：应对风险可选择规避风险，为寻求机遇承担风险，消除风险源，改变风险的可能性或后果，分担风险，或通过信息充分的决策而保留风险。

注 2：机遇可能导致采用新实践、推出新措施、开辟新领域、赢得新相关方、建立合作伙伴关系、利用新技术和其他可行之处，以应对组织或其相关方的需求。

6.2 安全目标及其实现的策划

6.2.1

组织应针对相关职能、层次和安全管理体系所需的过程建立安全目标。

安全目标应：

a) 与安全方针保持一致；
b) 可测量；
c) 考虑适用的要求；
d) 与风险管理相关；
e) 予以监视；
f) 予以沟通；
g) 适时更新。

组织应保持有关安全目标的成文信息。

6.2.2

策划如何实现安全目标时，组织应确定：

a) 要做什么；
b) 需要什么资源；
c) 由谁负责；
d) 何时完成；
e) 如何评价结果。

6.3 变更的策划

当组织确定需要对安全管理体系进行变更时，变更应按所策划的方式实施。

组织应考虑：

a) 变更目的及其潜在后果；
b) 安全管理体系的完整性；
c) 资源的可获得性；
d) 职责和权限的分配或再分配。

---

7 支持

7.1 资源

7.1.1 总则

组织应确定并提供所需的资源，以建立、实施、保持和持续改进安全风险管理体系。

组织应考虑：

a) 现有内部资源的能力和局限；
b) 需要从外部供方获得的资源。

7.1.2 人员

组织应确定并配备所需的人员，以有效实施安全风险管理体系，并运行和控制其过程。

7.1.3 基础设施

组织应确定、提供并维护所需的基础设施，以运行过程，并有效管理安全风险。

注：基础设施可包括：
a) 建筑物和相关设施；
b) 设备，包括硬件和软件；
c) 运输资源；
d) 信息和通讯技术；

e) 风险管理工具和技术。

7.1.4 过程运行环境

组织应确定、提供并维护所需的环境，以运行过程，并有效管理安全风险。

注：适宜的过程运行环境可能是人为因素与物理因素的结合，例如：
a) 社会因素(如非歧视、安定、非对抗)；
b) 心理因素(如减压、预防过度疲劳、稳定情绪)；
c) 物理因素(如温度、热量、湿度、照明、空气流通、卫生、噪声)。

7.1.5 监视和测量资源

当利用监视或测量来验证风险管理符合要求时，组织应确定并提供所需的资源，以确保结果有效和可靠。

组织应确保所提供的资源：

a) 适合所开展的监视和测量活动的特定类型；
b) 得到维护，以确保持续适合其用途。

组织应保留适当的成文信息，作为监视和测量资源适合其用途的证据。

7.1.6 组织的知识

组织应确定必要的知识，以运行过程，并有效管理安全风险。

这些知识应予以保持，并能在所需的范围内得到。

为应对不断变化的需求和发展趋势，组织应审视现有的知识，确定如何获取或接触更多必要的知识和知识更新。

注 1：组织的知识是组织特有的知识，通常从其经验中获得，是为实现组织目标所使用和共享的信息。

注 2：组织的知识可基于：
a) 内部来源(如知识产权、从经验获得的知识、从失败和成功项目汲取的经验和教训、获取和分享未成文的知识和经验，以及过程和风险管理改进结果)；
b) 外部来源(如标准、学术交流、专业会议、从相关方或外部供方收集的知识)。

7.2 能力

组织应：

a) 确定在其控制下工作的人员所需具备的能力，这些人员从事的工作影响安全管理体系绩效和有效性；
b) 基于适当的教育、培训或经验，确保这些人员是胜任的；
c) 适用时，采取措施以获得所需的能力，并评价措施的有效性；
d) 保留适当的成文信息，作为人员能力的证据。

注：适用措施可包括对在职人员进行培训、辅导或重新分配工作，或者聘用、外包胜任的人员。

7.3 意识

组织应确保在其控制下工作的人员知晓：

a) 安全方针；
b) 相关的安全目标；
c) 他们对安全管理体系有效性的贡献，包括改进绩效的益处；
d) 不符合安全管理体系要求的后果；
e) 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。

7.4 沟通

组织应确定与安全管理体系相关的内部和外部沟通，包括：

a) 沟通什么；
b) 何时沟通；
c) 与谁沟通；
d) 如何沟通；
e) 谁来沟通。

沟通和咨询的目的是帮助利益相关方理解风险、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。

7.5 成文信息

7.5.1 总则

组织的安全管理体系应包括：

a) 本标准要求的成文信息；
b) 组织所确定的、为确保安全管理体系有效性所需的成文信息。

注：对于不同组织，安全管理体系成文信息的多少与详略程度可以不同，取决于：
——组织的规模，以及活动、过程和风险的类型；
——过程及其相互作用的复杂程度；
——人员的能力。

7.5.2 创建和更新

在创建和更新成文信息时，组织应确保适当的：

a) 标识和说明(如标题、日期、作者、索引编号)；
b) 形式(如语言、软件版本、图表)和载体(如纸质的、电子的)；
c) 评审和批准，以保持适宜性和充分性。

7.5.3 成文信息的控制

7.5.3.1

应控制安全管理体系和本标准所要求的成文信息，以确保：

a) 在需要的场合和时机，均可获得并适用；
b) 予以妥善保护(如防止泄密、不当使用或缺失)。

7.5.3.2

为控制成文信息，适用时，组织应进行下列活动：

a) 分发、访问、检索和使用；
b) 存储和防护，包括保持可读性；
c) 更改控制(如版本控制)；
d) 保留和处置。

对于组织确定的策划和运行安全管理体系所必需的来自外部的成文信息，组织应进行适当识别，并予以控制。

对所保留的、作为符合性证据的成文信息应予以保护，防止非预期的更改。

注：对成文信息的"访问"可能意味着仅允许查阅，或者意味着允许查阅并授权修改。

---

8 运行

8.1 运行的策划和控制

为满足安全风险管理的要求，并实施第 6 章所确定的措施，组织应通过以下措施对所需的过程进行策划、实施和控制：

a) 确定安全风险管理的要求；
b) 建立下列内容的准则：
   1) 过程；
   2) 风险管理的接收。
c) 确定所需的资源以有效管理安全风险；
d) 按照准则实施过程控制；
e) 在必要的范围和程度上，确定并保持、保留成文信息，以：
   1) 确信过程已经按策划进行；
   2) 证实风险管理符合要求。

策划的输出应适合于组织的运行。

组织应控制策划的变更，评审非预期变更的后果，必要时，采取措施减轻不利影响。

组织应确保外包过程受控。

8.2 沟通和咨询

沟通和咨询的目的是帮助利益相关方理解风险、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方沟通并咨询其意见。

沟通和咨询的目标是：

a) 为风险管理过程的每个步骤汇集不同领域的专业知识；
b) 确保在界定风险准则和评价风险时适当考虑不同观点；
c) 提供充分信息，以促进对风险的全面了解和决策制定；

d) 使受风险影响的群体形成包容意识和责任意识。

8.3 范围、环境、准则

8.3.1 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。

8.3.2 界定范围

组织应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：

a) 目标和需要做的决策；
b) 过程中各个步骤的预期结果；
c) 时间、地点、具体包含和排除的事项；
d) 适当的风险评估工具和技术；
e) 所需的资源、责任和需要保留的记录；
f) 与其他项目、过程和活动的关系。

8.3.3 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，应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：

a) 风险管理是在组织目标和活动的环境下进行的；
b) 组织方面的因素可能是一种风险源；
c) 风险管理过程的目的和范围应与整个组织的目标相互关联。

组织应在考虑 4.1 所述因素的基础上，建立风险管理过程的内外部环境。

8.3.4 界定风险准则

组织应基于其目标，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。风险准则应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。风险准则应反映组织的价值观、目标和资源，并与组织的风险管理方针和声明相一致。在界定风险准则时应考虑组织的义务和利益相关方的意见。

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，因此应持续审视并于必要时进行修改。

在设定风险准则时，以下方面应加以考虑：

a) 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)；
b) 如何界定和度量后果(包括正面的和负面的)和可能性；
c) 时间相关因素；

d) 采用度量标准的一致性；
e) 如何确定风险等级；
f) 如何考虑多项风险的组合及顺序；
g) 组织的风险容量。

8.4 风险评估

8.4.1 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。

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

8.4.2 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。识别风险应考虑以下因素及相互之间的关系：

a) 有形和无形的风险源；
b) 原因和事件；
c) 威胁和机遇；
d) 脆弱性和应对能力；
e) 内外部环境变化；
f) 新兴风险；
g) 资产和资源的性质和价值；
h) 后果及其对目标的影响；
i) 知识的局限性和信息的可靠性；
j) 与时间有关的因素；
k) 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，都应对风险进行识别。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。

8.4.3 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：

a) 事件的可能性及后果；
b) 后果的性质及影响程度；
c) 复杂性和关联性；
d) 时间相关因素及波动性；

e）现有控制措施的有效性；
f）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。这些影响均应考虑、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。

8.4.4 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：

a）不采取进一步行动；
b）考虑风险应对方案；
c）开展进一步分析，以更全面地了解风险；
d）维持现有的控制措施；
e）重新考虑目标。

决策应考虑到更广泛的环境，以及对内外部利益相关方的实际和预期影响。

风险评价的结果应予以记录、沟通，然后在组织适当层级予以确认。

8.5 风险应对

8.5.1 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：

a）制定和选择风险应对方案；
b）计划和实施风险应对措施；
c）评估风险应对措施的成效；
d）确定剩余风险是否可接受；
e）若不可接受，采取进一步应对措施。

8.5.2 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：

a）决定不开始或退出会导致风险的活动，来规避风险；
b）承担或增加风险，以寻求机会；
c）消除风险源；
d）改变可能性；

e) 改变后果；
f) 分担风险(如通过签订合同，购买保险)；
g) 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，还应考虑所有的组织义务、自愿性承诺和利益相关方的观点。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，组织应考虑利益相关方的价值观、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方接受。

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。监督和检查应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方应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。

8.5.3 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。应对计划应明确指明实施风险应对的顺序。

应对计划应纳入管理计划和组织运营过程中，并征询利益相关方意见。

应对计划中提供的信息应包括：

a) 选择应对方案的理由，包括可获得的预期收益；
b) 批准和实施计划的责任人；
c) 拟采取的措施行动，包括应急预案；
d) 所需要的资源，包括风险准备；
e) 绩效考核的标准和方法；
f) 限制因素；
g) 必要的报告和监测；
h) 行动预期开展和完成的时间。

8.6 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。应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。

监督和检查应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。

监督和检查的结果应纳入组织绩效管理、考核和报告活动中。

8.7 记录和报告

应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：

a) 在组织各层级通报风险管理活动及结果；
b) 为决策制定提供信息；
c) 改进风险管理活动；
d) 促进与利益相关方的互动，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，应考虑(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，可提升与利益相关方的沟通质量，并为最高管理者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：

a) 区分利益相关方及其具体信息需求和要求；
b) 报告成本、频率和及时性；
c) 报告方式；
d) 信息与组织目标和决策的相关性。

---

9 绩效评价

9.1 监视、测量、分析和评价

9.1.1 总则

组织应确定：

a) 需要监视和测量什么；
b) 需要用什么方法进行监视、测量、分析和评价，以确保结果有效；
c) 何时实施监视和测量；
d) 何时对监视和测量的结果进行分析和评价。

组织应评价安全管理体系的绩效和有效性。

组织应保留适当的成文信息，以作为结果的证据。

9.1.2 利益相关方满意

组织应监视利益相关方对其需求和期望已得到满足的程度的感受。组织应确定获取、监视和评审该信息的方法。

注：监视利益相关方感受的例子可包括调查、反馈、座谈、担保索赔和相关方报告。

9.1.3 分析与评价

组织应分析和评价通过监视和测量获得的适当的数据和信息。

应利用分析结果评价：

a) 风险管理的符合性；
b) 利益相关方满意程度；
c) 安全管理体系的绩效和有效性；
d) 策划是否得到有效实施；
e) 应对风险和机遇所采取措施的有效性；

f）外部供方的绩效；
g）安全管理体系改进的需求。

注：数据分析方法可包括统计技术。

9.2 内部审核

9.2.1

组织应按照策划的时间间隔进行内部审核，以提供有关安全管理体系的下列信息：

a）是否符合：
　1）组织自身的安全管理体系要求；
　2）本标准的要求；
b）是否得到有效的实施和保持。

9.2.2

组织应：

a）依据有关过程的重要性、对组织产生影响的变化和以往的审核结果，策划、制定、实施和保持审核方案，审核方案包括频次、方法、职责、策划要求和报告；
b）规定每次审核的审核准则和范围；
c）选择审核员并实施审核，以确保审核过程客观公正；
d）确保将审核结果报告给相关管理者；
e）及时采取适当的纠正和纠正措施；
f）保留成文信息，作为实施审核方案以及审核结果的证据。

注：相关指南参见 GB/T 19011。

9.3 管理评审

9.3.1 总则

最高管理者应按照策划的时间间隔对组织的安全管理体系进行评审，以确保其持续的适宜性、充分性和有效性，并与组织的战略方向保持一致。

9.3.2 管理评审输入

策划和实施管理评审时应考虑下列内容：

a）以往管理评审所采取措施的情况；
b）与安全管理体系相关的内外部因素的变化；
c）下列有关安全管理体系绩效和有效性的信息，包括其趋势：
　1）利益相关方满意和有关相关方的反馈；
　2）安全目标的实现程度；
　3）过程绩效以及风险管理的合格情况；
　4）不合格及纠正措施；
　5）监视和测量结果；
　6）审核结果；
　7）外部供方的绩效。
d）资源的充分性；

e) 应对风险和机遇所采取措施的有效性；
f) 改进的机会。

9.3.3 管理评审输出

管理评审的输出应包括与下列事项相关的决定和措施：

a) 改进的机会；
b) 安全管理体系所需的变更；
c) 资源需求。

组织应保留成文信息，作为管理评审结果的证据。

---

10 改进

10.1 总则

组织应确定和选择改进机会，并采取必要措施，以满足相关方要求和保护组织价值。

这应包括：

a) 改进风险管理能力，以满足要求并应对未来的需求和期望；
b) 纠正、预防或减少不利影响；
c) 改进安全管理体系的绩效和有效性。

注：改进的例子可包括纠正、纠正措施、持续改进、突破性变革、创新和重组。

10.2 不合格和纠正措施

10.2.1

当出现不合格时，包括来自投诉的不合格，组织应：

a) 对不合格做出应对，并在适用时：
    1) 采取措施以控制和纠正不合格；
    2) 处置后果。
b) 通过下列活动，评价是否需要采取措施，以消除产生不合格的原因，避免其再次发生或者在其它场合发生：
    1) 评审和分析不合格；
    2) 确定不合格的原因；
    3) 确定是否存在或可能发生类似的不合格。
c) 实施所需的措施；
d) 评审所采取的纠正措施的有效性；
e) 需要时，更新在策划期间确定的风险和机遇；
f) 需要时，变更安全管理体系。

纠正措施应与不合格所产生的影响相适应。

10.2.2

组织应保留成文信息，作为下列事项的证据：

a) 不合格的性质以及随后所采取的措施；
b) 纠正措施的结果。

10.3 持续改进

组织应持续改进安全管理体系的适宜性、充分性和有效性。

组织应考虑分析和评价的结果以及管理评审的输出，以确定是否存在需求或机遇，这些需求或机遇应作为持续改进的一部分加以应对。

附录 A（资料性附录）

风险管理原则说明

本标准中风险管理原则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。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。

有效的风险管理需要满足以下原则：

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

利益相关方适当、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。在风险管理过程中应明确考虑与这些信息和预期相关的限制条件和不确定性。信息应及时、清晰，并且是有关的利益相关方可获得的。

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。

参考文献

[1] GB/T 24353—2022/ISO 31000:2018 风险管理 指南
[2] GB/T 27921:2023 风险管理 风险评估技术
[3] GB/T 19000 质量管理体系 基础和术语
[4] GB/T 19001 质量管理体系 要求
[5] GB/T 19011 管理体系审核指南
[6] ISO 31010 Risk management—Risk assessment techniques