



风险管理体系 认证技术规范

文件编号：CTS TBGL135-2026

版本号：B/2

受控状态： ()

编写：技术部

审核：张辉根 

批准：周春阳 

首次发布：2022-12-20发布

首次实施：2022-12-20

修订实施日期：20260423

江西腾标认证有限公司

目录

1. 范围	3
2. 规范性引用文件	3
3. 术语和定义	3
4. 组织环境	3
4.1. 理解组织及其环境	3
4.2. 理解相关方的需求和期望	4
4.3. 确定 风险管理体系 范围	4
4.4. 风险管理体系 及其过程	4
5. 领导作用	5
5.1. 领导作用和承诺	5
5.2. 方针	5
5.3. 组织的岗位、职责和权限	6
6. 策划	6
6.1. 应对风险和机遇的措施	6
6.2. 风险管理体系 目标及其实现的策划	6
6.3. 变更的策划	7
7. 支持	7
7.1. 资源	7
7.2. 能力	7
7.3. 意识	8
7.4. 沟通	8
7.5. 成文信息	8
8. 运行	9
8.1. 运行策划和控制	9
8.2. 危险源辨识与风险评估	9
8.3. 风险控制	10
8.4. 变更管理	10
8.5. 应急准备与响应	11
8.6. 安全教育培训与意识提升	11
8.7. 外部提供的过程、产品和服务的控制	11
9. 绩效评价	11
9.1. 监视、测量、分析和评价	11
9.2. 内部审核	12
9.3. 管理评审	12
10. 改进	13
10.1. 不合格与纠正措施	13
10.2. 持续改进	13
11. 其他	13

1. 范围

本文件规定了组织建立、实施、保持和持续改进 风险管理体系 的要求。本文件适用于：

- 1) 组织建立、实施、保持和改进 风险管理体系 ；
- 2) 认证机构对组织进行 风险管理体系 认证。

2. 规范性引用文件

下列文件对于本文件的应用必不可少。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/ISO 9001:2015 质量管理体系 要求
- GB/T 19000-2016/ISO 9000:2015 质量管理体系 基础和术语
- GB/T 33000-2016 企业安全生产标准化基本规范
- GB/T 24353-2022/ISO 31000:2018 风险管理 指南

注：认证审核时引用文件的有效性以审核实施时现行有效的最新版本为准。

3. 术语和定义

GB/T 19000-2016以及下列术语和定义适用于本文件。

3.1. 安全风险

发生安全事故的可能性与事故后果严重性的组合。

3.2. 危险源

可能导致人身伤害和（或）健康损害的根源、状态或行为，或其组合。

3.3. 风险评估

对危险源导致的安全风险进行分析、评价和分级的过程。

3.4. 风险控制

为消除或降低安全风险而采取的措施。

3.5. 重大危险源

长期地或临时地生产、搬运、使用或储存危险物质，且危险物质的数量等于或超过临界量的单元。

3.6. 变更管理

对人员、工艺、技术、设备、设施、材料、环境、管理等方面的永久性 or 临时性变更进行系统化控制的过程。

3.7. 应急准备

为有效应对突发事件而采取的各种措施的总称。

3.8. 最高管理者

在最高层指挥和控制组织的一个人或一组人。

4. 组织环境

4.1. 理解组织及其环境

组织应建立并保持程序，以确定与其宗旨和战略方向相关并影响其实现 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，并保留成文信息。

- 1) 外部因素：法律法规要求（如《安全生产法》、《消防法》等）、监管机构要求（如应急管理部门、行业主管部门）、行业标准与规范、市场竞争环境、技术发展趋势、社会文化环境等。
- 2) 内部因素：组织的价值观、文化、知识、规模、活动类型、产品和服务、生产流程、设施设备状况、资源状况（人力、财力、技术）、以往安全事故记录等。

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。
- 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。
- 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

4.2.1. 由于相关方对组织稳定提供符合顾客要求及适用法律法规要求的产品和服务的能力具有影响或潜在影响。

4.2.2. 组织应监视和评审 风险管理体系 相关方的信息及其相关要求：

4.2.3. 相关方包括但不限于：

- 1) 内部相关方：员工、管理层、股东、工会。
- 2) 外部相关方：政府及监管机构（应急管理、市场监管、消防、卫健等）、顾客、供方和承包商、周边社区、行业协会、认证机构、媒体、保险公司。

4.2.4. 组织应建立、实施并保持程序，以识别相关方，并促其参与到与 风险管理体系 相关的已识别的议题中。组织应保留促进相关方参与所产生的输出作为成文信息。与相关方的沟通应为一个持续的过程，而组织应保留沟通记录。

4.3. 确定 风险管理体系 范围

4.3.1. 组织应确定 风险管理体系 的边界和适用性，以确定其范围。

4.3.2. 在确定范围时，组织应考虑：

- 1) 在4.1.理解组织及其环境中提及的各种外部和内部因素；
- 2) 在4.2理解相关方的需求和期望中提及的相关方的要求；
- 3) 组织的活动、产品、服务、场所和部门。

4.3.3. 如果本标准的全部要求适用于组织确定的 风险管理体系 范围，组织应实施本标准的全部要求。

4.3.4. 组织应编制并保持 风险管理体系 范围的成文信息。该范围应明确界定管理体系覆盖的边界和适用性，经最高管理者批准后生效。该范围应描述所覆盖的产品和服务类型，如果组织确定本标准的某些要求不适用于其 风险管理体系 范围，应说明理由。

4.3.5. 只有当所确定的不适用的要求不影响组织确保其产品和服务合格的能力或责任，对增强顾客满意也不会产生影响时，方可声称符合本标准的要求。

4.4. 风险管理体系 及其过程

4.4.1. 组织应按照本技术规范的要求，建立、形成文件、实施、保持和持续改进 风险管理体系 ，包括所需过程及其相互作用。组织应保留管理体系成文信息（如管理手册）。

4.4.2. 组织应确定 风险管理体系 所需的过程及其在整个组织中的应用，且应：

- 1) 确定这些过程所需的输入和期望的输出；

- 2) 确定这些过程的顺序和相互作用；
 - 3) 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；
 - 4) 确定这些过程所需的资源并确保其可获得；
 - 5) 分配这些过程的职责和权限；
 - 6) 按照6.1条款的要求应对风险和机遇；
 - 7) 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；
 - 8) 改进过程和 风险管理体系 。
- 4.4.3. 在必要的范围和程度上,组织应:**
- 1) 保持成文信息以支持过程运行；
 - 2) 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,提供证据以证实其对 风险管理体系 的领导作用和承诺。最高管理者应保留履行上述职责的记录(如会议纪要、批准文件等):

- 1) 对 风险管理体系 的有效性负责；
- 2) 确保制定 风险管理体系 的方针和目标,并与组织环境相适应,与战略方向相一致；
- 3) 确保 风险管理体系 要求融入组织的业务过程；
- 4) 促进使用过程方法和基于 风险管理体系 的思维；
- 5) 确保 风险管理体系 所需的资源是可获得的；
- 6) 沟通有效的培训管理和符合 风险管理体系 要求的重要性；
- 7) 确保 风险管理体系 实现其预期结果；
- 8) 促使人员积极参与,指导和支持他们为 风险管理体系 的有效性作出贡献；
- 9) 推动改进；
- 10) 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. 以顾客为关注焦点

最高管理者应通过确保以下方面,证实其以顾客为关注焦点的领导作用和承诺:

- 1) 确定、理解并持续地满足顾客要求以及适用的法律法规要求；
- 2) 确定和应对风险和机遇,这些风险和机遇可能影响产品和服务合格以及增强顾客满意的能力；
- 3) 始终致力于增强顾客满意。

5.2. 方针

5.2.1. 制定 风险管理体系 方针

最高管理者应制定、形成文件、实施和保持 风险管理体系 方针, 风险管理体系 方针应经最高管理者批准,并保留批准记录:

- 1) 适应组织的宗旨和环境并支持其战略方向；
- 2) 为建立 风险管理体系 目标提供框架；
- 3) 包括满足适用 风险管理体系 要求(如法律法规、监管要求、相关方要求)的承诺；

- 4) 包括持续改进 风险管理体系 的承诺；
- 5) 包括预防 安全事故、保护人员安全和健康的承诺。

5.2.2. 沟通 风险管理体系 方针应：

- 1) 可获取 风险管理体系 并保持成文信息；
- 2) 风险管理体系 在组织内得到沟通、理解和应用；
- 3) 适宜时， 风险管理体系 可为有关相关方所获取。

5.3. 组织的岗位、职责和权限

5.3.1. 最高管理者应以文件形式明确并分配 风险管理体系 相关岗位的职责、权限。组织应保留岗位职责分配表，并确保相关人员知晓。

5.3.2. 最高管理者应指定一名或多名管理者，不论其是否负有其他职责，应使其具有以下方面的岗位、职责和权限，以确保：

- 1) 风险管理体系 符合本技术规范的要求；
- 2) 协调与 风险管理体系 有关的内部和外部沟通，确保各过程获得其预期输出；
- 3) 报告 风险管理体系 的绩效以及改进机会(见9.1. 监视、测量、分析和评价),特别是向最高管理者报告；
- 4) 确保在整个组织中提高对 风险管理体系 重要性的意识；
- 5) 确保在策划和实施 风险管理体系 变更时保持其完整性。

6. 策划

6.1. 应对风险和机遇的措施

6.1.1. 在策划 风险管理体系 时，组织应考虑到4.1. 理解组织及其环境所提及的因素和4.2理解相关方的需求和期望所提及的要求，并确定需要应对的风险和机遇，以：

- 1) 确保 风险管理体系 能够实现其预期结果；
- 2) 增强有利影响；
- 3) 预防或减少不利影响（如安全事故、财产损失、法律风险）；
- 4) 实现持续改进。

6.1.2. 组织应建立并保持合规义务登记册，以识别和跟踪与 风险管理体系 相关的法律法规、标准及其他要求；

6.1.3. 组织应策划：

- 1) 应对这些风险和机遇的措施；
- 2) 在 风险管理体系 过程中整合并实施这些措施(见4.4. 条款)；
- 3) 评价这些措施的有效性。

6.1.4. 应对措施应与风险和机遇对产品和服务符合性的潜在影响相适应。

- 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。
- 2) 机遇可能导致采用新实践、推出新产品、开辟新市场、赢得新顾客，建立合作伙伴关系、利用新技术和其他可行之处，以应对组织或其顾客的需求。

6.2. 风险管理体系 目标及其实现的策划

6.2.1. 组织应针对相关职能、层次和 风险管理体系 所需的过程建立 风险管理 目标。

- 1) 风险管理体系 目标应：

- ① 与 风险管理体系 方针保持一致；
- ② 可测量（如何可行，如事故发生率、隐患整改率、培训覆盖率）；
- ③ 考虑适用的要求；
- ④ 予以监视；
- ⑤ 予以沟通；
- ⑥ 视情况予以适时更新。

2) 组织应保持有关 风险管理体系 目标的成文信息。

6.2.2. 策划如何实现 风险管理体系 目标时，组织应确定：

- 1) 要做什么；
- 2) 需要什么资源；
- 3) 由谁负责；
- 4) 何时完成；
- 5) 如何评价结果。

6.3. 变更的策划

6.3.1. 当组织确定需要对 风险管理体系 进行变更时，变更应按所策划的方式实施(见4.4.条款)。

6.3.2. 组织应考虑：

- 1) 变更目的及其潜在后果；
- 2) 风险管理体系 的完整性；
- 3) 资源的可获得性；
- 4) 职责和权限的分配或再分配。

7. 支持

7.1. 资源

7.1.1. 总则

- 1) 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 风险管理体系 。组织应保留资源评估与配置的记录。
- 2) 组织资源包括：人力资源、基础设施（如安全防护设施、监控系统、应急设备等）、过程运行环境、监视和测量资源、财务资源、技术资源、信息等。
- 3) 组织应考虑：
 - ① 现有内部资源的能力和局限；
 - ② 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 风险管理体系 ，并运行和控制其过程。关键岗位应明确任职要求并保留人员资质证明。

7.2. 能力

7.2.1. 组织必须：

- 1) 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 风险管理体系 绩效和有效性；
- 2) 基于适当的教育、培训或经验，确保这些人员是具备所需的能力；
- 3) 适用时，采取措施以获得所需的能力，并评价措施的有效性；

- 4) 保留适当的成文信息作为人员能力的证据；
 - 5) 每年至少一次对能力需求进行评审。
- 7.2.2. 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

组织应通过培训、宣传、会议等方式，确保在其控制下工作的人员知晓以下内容。组织应保留培训记录和培训签到表。

- 1) 风险管理体系 的培训方针
- 2) 与 风险管理体系 相关的培训目标；
- 3) 组织对 风险管理体系 有效性的贡献，包括改进绩效的益处；
- 4) 不符合 风险管理体系 认证技术规范要求的后果；
- 5) 在 风险管理体系 过程中个人的角色和职责；
- 6) 报告 风险管理体系 和潜在危险相关的程序。

7.4. 沟通

7.4.1. 组织应确定与 风险管理体系 相关的内部和外部沟通，包括但不限于：

- 1) 沟通什么；
- 2) 何时沟通；
- 3) 与谁沟通；
- 4) 如何沟通；
- 5) 谁来沟通。

7.4.2. 组织应建立、实施和保持程序，以确保在安全事故或紧急情况期间与内外部相关方（如员工、监管机构、周边社区、媒体）进行有效沟通。组织应保留沟通记录（如通知、报告、会议纪要）。

7.5. 成文信息

7.5.1. 总则

- 1) 组织的管理体系成文信息必须包括 风险管理体系 认证技术规范要求的文件及组织确定的 风险管理体系 有效运行所需的文件。
- 2) 对于不同组织， 风险管理体系 成文信息的多少与详略程度可以不同，取决于：
 - ① 组织的规模，以及活动、过程、产品和服务的类型；
 - ② 过程及其相互作用的复杂程度；
 - ③ 人员的能力。

7.5.2. 创建和更新

在创建和更新成文信息时，组织应确保适当的标识和说明(如标题、日期、作者、索引编号)、格式(如语言、软件版本、图表)、载体(如纸质的、电子的)以及评审和批准，以保持适宜性和充分性。

7.5.3. 成文信息的控制

组织应建立并保持成文信息控制程序，以确保：在需要的场合和时机，均可获得并适用；予以妥善保护。组织应保留成文信息分发、变更、处置的记录。

- 1) 应控制 风险管理体系 所要求的成文信息，以确保：
 - ① 在需要的场合和时机，均可获得并适用；
 - ② 予以妥善保护(如防止泄密、不当使用或缺失)。

- 2) 为控制成文信息，适用时，组织应进行下列活动：
 - ① 分发、访问、检索和使用；
 - ② 存储和防护，包括保持可读性；
 - ③ 更改控制(如版本控制)；
 - ④ 保留和处置。
 - 3) 对于组织确定的策划和运行 风险管理体系 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。
 - 4) 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. 运行策划和控制

- 8.1.1. 组织应策划、实施和控制满足 风险管理体系 所需的全过程，并实施第6章所确定的措施，组织必须通过以下措施对所需的过程（见4.4.条款）进行策划、实施和控制。组织应保留运行策划的输出（如风险控制计划、作业指导书）。
 - 1) 确定 风险管理体系 的工作要求，建立下列内容的准则：
 - ① 过程准则（如危险源辨识方法、风险评估准则、风险控制措施要求）；
 - ② 安全工作的接收准则（如安全验收标准、隐患整改标准）；
 - a. 确定 风险管理体系 所需的资源；
 - b. 按照 风险管理体系 准则实施过程控制；
 - ③ 在必要的范围和程度上，确定并保持、保留成文信息
 - ④ 确信过程已经按策划进行；
 - ⑤ 证实 风险管理体系 工作符合要求。
 - 8.1.2. 策划的输出应适合于组织的运行。
 - 8.1.3. 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. 危险源辨识与风险评估

8.2.1. 危险源辨识

组织应建立、实施和保持文件化的程序，以系统化地辨识与组织活动、产品和服务相关的危险源。组织应保留危险源辨识记录，并至少每年更新一次。

- 1) 常规和非常规的活动；
- 2) 所有进入工作场所的人员（包括员工、承包商、访客等）的活动；
- 3) 人的行为、能力和其他人为因素；
- 4) 已识别的源于工作场所外，能够对工作场所内组织控制下的人员造成不利影响的危险源；
- 5) 在工作场所附近，由组织控制下的工作活动所产生的危险源；
- 6) 由组织或外界所提供的基础设施、设备和材料；
- 7) 组织所进行的变更，或外部变更（如法律法规变更）；
- 8) 辨识由变更（工艺、设备、人员、材料等）产生的新危险源；
- 9) 危险源的分类（如物理、化学、生物、人机工程、心理等）。

8.2.2. 风险评估

组织应建立、实施和保持文件化的程序，以对已辨识的危险源进行风险评估。组织应保留风险评估报告，确定风险等级和可接受风险准则。风险评估应：

- 1) 考虑现有控制措施的有效性；
- 2) 确定风险等级，进行分级管理；
- 3) 识别重大安全风险和重大危险源；
- 4) 确定风险是否可接受。

8.3. 风险控制

8.3.1. 风险控制措施策划

- 1) 组织应根据风险评估结果，策划并实施风险控制措施。组织应保留风险控制措施策划与实施的记录，明确责任人、措施内容和完成时限。
- 2) 控制措施的选择应遵循以下层级原则：
 - ① 消除危险源；
 - ② 替代（用低风险物质或工艺替代高风险物质或工艺）；
 - ③ 工程控制（如隔离、防护、通风、联锁等）；
 - ④ 管理控制（如安全操作规程、培训、作业许可、轮班等）；
 - ⑤ 个体防护装备。

8.3.2. 风险控制措施实施

组织应：

- 1) 实施所策划的风险控制措施；
- 2) 将风险控制措施纳入相关过程或作业文件；
- 3) 确保风险控制措施的有效性。

8.3.3. 安全风险分级管控

组织应根据安全风险评估结果及生产经营状况等，确定相应的安全风险等级，对其进行分级分类管理，实施安全风险差异化动态管理，制定并落实相应的安全风险控制措施。

8.3.4. 重大危险源管理

- 1) 组织应建立文件化的重大危险源管理制度，全面辨识重大危险源。
- 2) 组织应保留重大危险源清单，并向所在地安全监管部门备案（适用时）。
- 3) 对确认的重大危险源制定安全管理技术措施和应急预案。
- 4) 组织应对重大危险源进行登记建档，设置重大危险源监控系统，进行日常监控，并按照有关规定向所在地安全监管部门备案。

8.4. 变更管理

- 1) 组织应制定文件化的变更管理制度。变更实施前应经授权人批准，变更完成后应保留验收记录。
- 2) 变更前应对变更过程及变更后可能产生的安全风险进行分析，制定控制措施，履行审批及验收程序，并告知和培训相关从业人员。变更类型包括但不限于：
 - ① 工艺、技术变更；
 - ② 设备、设施变更；
 - ③ 材料、化学品变更；
 - ④ 人员、组织机构变更；
 - ⑤ 法律法规、标准变更。

8.5. 应急准备与响应

- 1) 组织应建立、实施和保持文件化的应急准备与响应程序；
 - ① 识别潜在的紧急情况（如火灾、爆炸、泄漏、自然灾害等）；
 - ② 制定应急预案，明确应急组织、职责、程序和资源；
 - ③ 提供应急设备、设施和物资，并定期检查和维护；
 - ④ 定期进行应急演练，评估演练效果，并改进应急预案；
 - ⑤ 在紧急情况发生后，及时进行响应和处置，并评估响应效果。
- 2) 组织应制定应急预案，并经最高管理者批准；
- 3) 应至少每年组织一次应急演练，并保留演练评估报告。

8.6. 安全教育培训与意识提升

- 1) 组织应建立、实施和保持安全教育培训程序，确保：
 - ① 所有员工接受必要的安全教育培训，了解其岗位的 风险管理体系 相关的范畴与工作职责；
 - ② 新员工、转岗员工、承包商和访客接受相应的安全培训；
 - ③ 特种作业人员持证上岗；
 - ④ 定期开展安全意识和技能提升活动。
- 2) 组织应制定年度安全培训计划，并保留培训记录和考核结果。

8.7. 外部提供的过程、产品和服务的控制

- 1) 组织应确保外部提供的过程、产品和服务（如外包工程、设备采购、化学品供应、物流服务）符合 风险管理体系 的要求。组织应：
 - ① 向外部供方明确安全要求（如安全资质、安全操作规程、 风险管理体系 控制措施、危险作业审批要求）；
 - ② 评价和选择外部供方，确保其具备满足安全要求的能力；
 - ③ 对外部供方的安全绩效进行监视和评价；
 - ④ 对涉及高风险的外包活动（如动火、高处、受限空间作业），明确控制要求和责任划分。
- 2) 组织应与外部供方签订协议或合同，明确安全要求；应保留对供方的评价和选择记录。

9. 绩效评价

9.1. 监视、测量、分析和评价

9.1.1. 总则

- 1) 组织应建立并保持监视、测量、分析和评价的程序，明确：
 - ① 需要监视和测量什么（如故发生率、隐患整改率、培训完成率、风险控制措施有效性）；
 - ② 需要什么方法进行监视、测量、分析和评价的方法，以确保结果有效；
 - ③ 确保用于监视与测量的资源（如检测设备、监控系统）的准确性；
 - ④ 何时实施监视和测量；
 - ⑤ 何时对监视和测量的结果进行分析和评价。
- 2) 组织应保留监视和测量记录。
- 3) 组织应评价 风险管理体系 的绩效和有效性，并保留适当的成文信息，以作为结果的证据。

9.1.2. 合规性评价

- 1) 组织应根据法规要求（如《安全生产法》、《消防法》等）和相关方对安全的要求，建立、实施并保持程序，以定期评价组织对适用法律法规、标准及其他要求的遵守情况。
- 2) 合规性评价应至少每年进行一次，并保留合规性评价报告作为成文信息。
- 3) 合规性评价应由指定部门或人员组织实施，评价结果应报告最高管理者。

9.2. 内部审核

9.2.1. 组织应按照策划的时间间隔（至少每年一次）进行内部审核。

9.2.2. 组织应建立并保持内部审核方案，审核员应具备相应能力且不得审核自己的工作。以提供有关 风险管理体系 是否符合本技术规范的要求，以及是否得到有效实施和保持的信息：

9.2.3. 在进行内部审核时，组织应：

- 1) 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；
- 2) 规定每次审核的审核准则和范围；
- 3) 选择审核员并实施审核，以确保审核过程客观公正；
- 4) 确保将审核结果报告给相关管理者；
- 5) 及时采取适当的纠正和纠正措施；
- 6) 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

最高管理者应按照策划的时间间隔（至少每年一次）对组织的 风险管理体系 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。组织应保留管理评审会议纪要和输出的决定。

9.3.1. 管理评审输入

策划和实施管理评审时应考虑下列内容：

- 1) 以往管理评审所采取措施的情况；
- 2) 与 风险管理体系 相关的内外部因素的变化；
- 3) 有关 风险管理体系 绩效和有效性的信息，包括其趋势：
 - ① 安全事故和事件情况；
 - ② 隐患整改和风险控制情况；
 - ③ 应急演练和响应情况；
 - ④ 外部供方的安全绩效；
 - ⑤ 审核结果；
 - ⑥ 目标的实现程度；
 - ⑦ 不合格及纠正措施；
 - ⑧ 合规性评价的结果。
- 4) 资源的充分性；
- 5) 应对风险和机遇所采取措施的有效性（见6.1.应对风险和机遇的措施）；
- 6) 改进的机会。

9.3.2. 管理评审输出

- 1) 管理评审的输出应包括与下列事项相关的决定和措施：
 - ① 改进的机会；

- ② 风险管理体系 所需的变更；
 - ③ 资源需求。
- 2) 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. 不合格与纠正措施

10.1.1. 当发生不合格项时（如安全事故、隐患未整改、违规操作），组织应在规定时限内：

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

10.1.2. 组织应基于管理评审输出、内审结果、合规性评价等，制定改进计划并跟踪落实。

10.1.3. 纠正措施应与不符合项所产生的影响相适应，组织应保留成文信息，作为下列事项的证据：

- 1) 不符合项的性质以及随后所采取的措施；
- 2) 纠正措施的结果。

10.2. 持续改进

10.2.1. 组织应持续改进 风险管理体系 的适宜性、充分性和有效性。

10.2.2. 组织应考虑分析和评价的结果以及管理评审的输出，确定是否存在持续改进的需求或机遇，并将其作为持续改进变更管理的一部分加以实施。

11. 其他

11.1. 建立并保持程序

组织应形成文件化的程序文件，明确活动的目的、范围、职责、流程和要求。

11.2. 保留成文信息

组织应保存记录（如纸质或电子），以证明活动已按策划实施。记录应清晰、可追溯、便于检索。

11.3. 指定责任人

组织应在相关文件中明确具体岗位或人员的职责，并确保其知晓。

11.4. 时限要求

本文件中“定期”如无特别说明，默认为“至少每年一次”；“及时”指在合理可行的情况下尽快处理，最长不超过30日。