安全风险管理体系认证技术规范

文件编号：CTS TBGL-25-2026

版本号：B/0

受控状态： （ 受控 ）

编写：技术部

审核：张辉根

批准：周春阳

2026-01-08发布 **2026-01-08实施**

江西腾标认证有限公司

目录

1. 范围

1.1. 本技术规范为下列组织规定了 安全风险管理体系 的要求：

1.1.1. 需要证实其具有稳定提供满足顾客要求及适用法律法规要求的产品和服务的能力；

1.1.2. 通过体系的有效应用，包括体系改进的过程，以及保证符合顾客要求和适用的法律法规要求，旨在增加顾客满意。

1.2. 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 本标准中的术语“产品”或“服务”仅适用于预期提供给顾客或顾客所要求的产品和服务。

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 19001-2026/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 27921-2023/IEC 31010:2019风险管理-风险评估技术；
- GB/T 24353-2022/ISO 31000:2018风险管理-指南；
- GB/T 23694-2024风险管理-术语；
- 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

略，可参考2.规则发生性引用文件内术语与定义

4. 组织环境

4.1. 理解组织及其环境

4.1.1. 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。

4.1.2. 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。

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. 组织应监视和评审这些相关方的信息及其相关要求：

1) 与 安全风险管理体系 有关的相关方；
2) 与 安全风险管理体系 有关的相关方的要求。

4.3. 确定 安全风险管理体系 范围

4.3.1. 组织必须确定 安全风险管理体系 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) 组织的产品和服务。

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

4.3.4. 组织的 安全风险管理体系 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 安全风险管理体系 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. 安全风险管理体系 及其过程

4.4.1. 组织应按照 安全风险管理体系 认证技术规范的要求，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 。

4.4.2. 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：

4) 确定这些过程所需的输人和期望的输出；
5) 确定这些过程的顺序和相互作用；
6) 确定和应用所需的准则和方法(包手监视、测量和相关绩效指标),以确保这些过程的有效运行和控制；
7) 确定这些过程所需的资源并确保其可获得；
8) 分配这些过程的职责租权限；
9) 按照6.1条的要求应对风险和机遇；
10) 评价这些过程，实施所雷的变更，以确保实现这些过程的顶期结果；
11) 改进过程和 安全风险管理体系 。

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，证实其对 安全风险管理体系 的领导作用和承诺：

1) 对 安全风险管理体系 的有效性负责；
2) 确保制定 安全风险管理体系 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 安全风险管理体系 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的思维；
5) 确保 安全风险管理体系 所需的资源是可获得的；

6) 沟通有效的培训管理和符合 安全风险管理体系 要求的重要性；
7) 确保 安全风险管理体系 实现其预期结果；
8) 促使人员积极参与，指导和支持他们为 安全风险管理体系 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. 制定培训方针

最高管理者应制定、实施和保持培训方针，培训方针应：

1) 适应组织的宗旨和环境并支持其战略方向；
2) 为建立培训目标提供框架；
3) 包括满足适用 安全风险管理体系 要求的承诺；
4) 包括持续改进 安全风险管理体系 的承诺。

5.2.2. 沟通培训方针应：

1) 可获取 安全风险管理体系 并保持成文信息；
2) 安全风险管理体系 在组织内得到沟通、理解和应用；
3) 适宜时， 安全风险管理体系 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. 最高管理者应确保组织 安全风险管理体系 相关岗位的职责、权限得到分配、沟通和理解。

5.3.2. 最高管理者应分配职责和权限，以确保：

1) 安全风险管理体系 符合本标准的要求；
2) 确保各过程获得其预期输出；
3) 报告 安全风险管理体系 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) 确保在整个组织中推动以顾客为关注焦点；
5) 确保在策划和实施 安全风险管理体系 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 安全风险管理体系 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 安全风险管理体系 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；

4) 实现改进。

6.1.2. 组织应策划：

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

6.1.3. 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. 培训目标及其实现的策划

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

1) 培训目标应：
   ① 与培训方针保持一致；
   ② 可测量；
   ③ 考虑适用的要求；
   ④ 与产品和服务合格以及增强顾客满意相关；
   ⑤ 予以监视；
   ⑥ 予以沟通；
   ⑦ 适时更新。
2) 组织应保持有关培训目标的成文信息。

6.2.2. 策划如何实现培训目标时，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 安全风险管理体系 进行变更时，变更应按所策划的方式实施(见4.4.保密管理体系及其过程)。

6.3.2. 组织应考虑：

1) 变更目的及其潜在后果；
2) 安全风险管理体系 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 安全风险管理体系 。

2) 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 安全风险管理体系 ，并运行和控制其过程。

7.1.3. 基础设施

1) 组织应确定、提供并维护所需的基础设施，以运行过程，并获得合格产品和服务。

2) 基础设施可包括：

① 建筑物和相关设施；

② 设备，包括硬件和软件；

③ 运输资源；

④ 信息和通讯技术。

7.1.4. 过程运行环境

1) 组织应确定、提供并维护所需的环境，以运行过程，并获得合格产品和服务。

2) 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：

① 社会因素(如非歧视、安定、非对抗)；

② 心理因素(如减压、预防过度疲劳、稳定情绪)；

③ 物理因素(如温度、热量、湿度、照明、空气流通、卫生、噪声)。

3) 由于所提供的产品和服务不同，这些因素可能存在显著差异。

7.1.5. 监视和测量资源

1) 监视：当利用监视或测量来验证产品和服务符合要求时，组织应确定并提供所需的资源，以确保结果有效和可靠。

① 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。

② 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。

2) 测量溯源

① 当要求测量溯源时，或组织认为测量溯源是信任测量结果有效的基础时，测量设备应：

a. 对照能溯源到国际或国家标准的测量标准，按照规定的时间间隔或在使用前进行校准和(或)检定，当不存在上述标准时，应保留作为校准或验证依据的成文信息；

b. 予以识别，以确定其状态；

c. 予以保护，防止由于调整、损坏或衰减所导致的校准状态和随后的测量结果的失效。当发现测量设备不符合预期用途时，组织应确定以往测量结果的有效性是否受到不利影响，

② 必要时应采取适当的措施。

7.1.6. 组织知识

1) 组织应确定必要的知识，以运行过程，并获得合格产品和服务。

2) 这些知识应予以保持，并能在所需的范围内得到。

3) 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。

① 组织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。

② 组织知识可基于：

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、产品和服务的改进结果)；

b. 外部来源(如标准、学术交流、专业会议、从顾客或外部供方收集的知识)。

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 安全风险管理体系 绩效和有效性；
2) 基于适当的教育、培训或经验，确保这些人员是胜任的；
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。

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

组织必须确保在其控制下工作的人员知晓：

1) 安全风险管理体系 的培训方针
2) 与 安全风险管理体系 相关的培训目标；
3) 其对 安全风险管理体系 有效性的贡献，包括改进绩效的益处；
4) 不符合 安全风险管理体系 认证技术规范要求的后果。

7.4. 沟通

组织应确定与 安全风险管理体系 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。

7.5. 成文信息

7.5.1. 总则

1) 组织的 安全风险管理体系 成文信息必须包括 安全风险管理体系 认证技术规范要求的文件及组织确定的 安全风险管理体系 有效运行所需的文件。
2) 对于不同组织， 安全风险管理体系 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：

1) 标识和说明(如标题、日期、作者、索引编号)；
2) 形式(如语言、软件版本、图表)和载体(如纸质的、电子的)；
3) 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

1) 应控制 安全风险管理体系 和 安全风险管理体系 认证技术规范所要求的成文信息，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 安全风险管理体系 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. 为满足 安全风险管理体系 的要求，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.保密管理体系及其过程）进行策划、实施和控制：

1) 确定产品和服务的要求；
2) 建立下列内容的准则：
① 过程；
② 产品和服务的接收。
3) 确定 安全风险管理体系 所需的资源以使产品和服务符合要求；
4) 按照 安全风险管理体系 准则实施过程控制；
5) 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 证实产品和服务符合要求。

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(见8.4.生产和服务提供)。

8.2. 产品和服务的要求

8.2.1. 顾客沟通

与顾客沟通的内容应包括：

1) 提供有关产品和服务的信息；
2) 处理问询、合同或订单，包括更改；
3) 获取有关产品和服务的顾客反馈，包括顾客投诉；
4) 处置或控制顾客财产；
5) 关系重大时，制定应急措施的特定要求。

8.2.2. 产品和服务要求的确定

在确定向顾客提供的产品和服务的要求时，组织应确保：

1) 产品和服务的要求得到规定，包括：
① 适用的法律法规要求；
② 组织认为的必要要求。

2) 提供的产品和服务能够满足所声明的要求。

8.2.3. 产品和服务要求的评审

1) 组织应确保有能力向顾客提供满足要求的产品和服务。

2) 在承诺向顾客提供产品和服务之前，组织应对如下各项要求进行评审：

① 顾客规定的要求，包括对交付及交付后活动的要求；

② 顾客虽然没有明示，但规定的用途或已知的预期用途所必需的要求；

③ 组织规定的要求；

④ 适用于产品和服务的法律法规要求；

⑤ 与以前表述不一致的合同或订单要求。

3) 组织应确保与以前规定不一致的合同或订单要求已得到解决。

4) 若顾客没有提供成文的要求，组织在接受顾客要求前应对顾客要求进行确认。

注：在某些情况下，如网上销售，对每一个订单进行正式的评审可能是不实际的，作为替代方法，可评审有关的产品 信息，如产品目录。

5) 适用时，组织应保留与下列方面有关的成文信息：

① 评审结果；

② 产品和服务的新要求。

8.2.4. 产品和服务要求的更改

若产品和服务要求发生更改，组织应确保相关的成文信息得到修改，并确保相关人员知道已更改的要求 。

8.3. 外部提供的过程、产品和服务的控制

8.3.1. 总则

1) 组织应确保外部提供的过程、产品和服务符合要求。

2) 在下列情况下，组织应确定对外部提供的过程、产品和服务实施的控制：

① 外部供方的产品和服务将构成组织自身的产品和服务的一部分；

② 外部供方代表组织直接将产品和服务提供给顾客；

③ 组织决定由外部供方提供过程或部分过程。

3) 组织应基于外部供方按照要求提供过程、产品和服务的能力，确定并实施对外部供方的评价、选择、绩效监视以及再评价的准则。对于这些活动和由评价引发的任何必要的措施，组织应保留成文信息。

8.3.2. 控制类型和程度

1) 组织应确保外部提供的过程、产品和服务不会对组织稳定地向顾客交付合格产品和服务的能力产生不利影响。

2) 组织应：

① 确保外部提供的过程保持在其 安全风险管理体系 的控制之中；

② 规定对外部供方的控制及其输出结果的控制；

③ 还应考虑：

a. 外部提供的过程、产品和服务对组织稳定地满足顾客要求和适用的法律法规要求的能力的潜在影响 ；

b. 由外部供方实施控制的有效性；

④ 确定必要的验证或其他活动，以确保外部提供的过程、产品和服务满足要求。

8.3.3. 提供给外部供方的信息

1) 组织应确保在与外部供方沟通之前所确定的要求是充分和适宜的。

2) 组织应与外部供方沟通以下要求：

① 需提供的过程、产品和服务；

② 对下列内容的批准：

a. 产品和服务；

b. 方法、过程和设备；

c. 产品和服务的放行；

③ 能力，包括所要求的人员资格；

④ 外部供方与组织的互动；

⑤ 组织使用的对外部供方绩效的控制和监视；

⑥ 组织或其顾客拟在外部供方现场实施的验证或确认活动。

8.4. 生产和服务提供

8.4.1. 生产和服务提供的控制

1) 组织应在受控条件下进行生产和服务提供。

2) 适用时，受控条件应包括：

① 可获得成文信息，以规定以下内容：

d. 拟生产的产品、提供的服务或进行的活动的特性；

e. 拟获得的结果。

② 可获得和使用适宜的监视和测量资源；

③ 在适当阶段实施监视和测量活动，以验证是否符合过程或输出的控制准则以及产品和服务的接收准则；

④ 为过程的运行使用适宜的基础设施，并保持适宜的环境；

⑤ 配备胜任的人员，包括所要求的资格；

⑥ 若输出结果不能由后续的监视或测量加以验证，应对生产和服务提供过程实现策划结果的能力进行确认，并定期再确认；

⑦ 采取措施防止人为错误；

⑧ 实施放行、交付和交付后的活动。

8.4.2. 标识和可追溯性

1) 需要时，组织应采用适当的方法识别输出，以确保产品和服务合格。

2) 组织应在生产和服务提供的整个过程中按照监视和测量要求识别输出状态。

3) 当有可追溯要求时，组织应控制输出的唯一性标识，并应保留所需的成文信息以实现可追溯。

8.4.3. 顾客或外部供方的财产

1) 组织应爱护在组织控制下或红织使用的顾客或外部供方的财产

2) 对组织使用的或构成产品和服务一部分的顾客和外部供方财产，组织应予以识别、验证、保护和防护。

3) 若顾客或外部供方的财产发小王失、损坏或发现不适用情况，组织应向顾客或外部供方报告，并保留所发生情况的成文信息。

注：顾客或外部供方的财产可能包括材料零部件、工具和设备以及场所、年产权和个人资料

8.4.4. 防护

1) 组织应在生产和服务提供期间对输出进行必要的防护，以确保符合要求。

2) 注：防护可包括标识、处置、污染控制、包装、储存、传输或运输以及保护。

8.4.5. 交付后活动

1) 组织应满足与产品和服务相关的交付后活动的要求。

2) 在确定所要求的交付后活动的覆盖范围和程度时，组织应考虑：
   ① 法律法规要求；
   ② 与产品和服务相关的潜在不良的后果；
   ③ 产品和服务的性质、使用和预期寿命；
   ④ 顾客要求；
   ⑤ 顾客反馈。

注：交付后活动可包括保证条款所规定的措施、合同义务(如维护服务等)、附加服务(如回收或最终处置等)。

8.4.6. 更改控制

1) 组织应对生产或服务提供的更改进行必要的评审和控制，以确保持续地符合要求。
2) 组织应保留成文信息，包括有关更改评审的结果、授权进行更改的人员以及根据评审所采取的必要措施。

8.5. 安全风险管理体系 评价

8.5.1. 产品和服务的放行

1) 组织应在适当阶段实施策划的安排，以验证产品和服务的要求已得到满足。
2) 除非得到有关授权人员的批准，适用时得到顾客的批准，否则在策划的安排已圆满完成之前，不应向顾客放行产品和交付服务。
3) 组织应保留有关产品和服务放行的成文信息。成文信息应包括：
   ① 符合接收准则的证据；
   ② 可追溯到授权放行人员的信息。

8.5.2. 安全风险管理体系 评价

1) 组织开展 安全风险管理体系 应符合 T/PPAC 701—2021 《企业商业秘密管理规范》中相关要求。
2) 详见 T/PPAC 701—2021 《企业商业秘密管理规范》。

8.6. 不合格输出的控制

8.6.1. 组织应确保对不符合要求的输出进行识别和控制，以防止非预期的使用或交付。组织应根据不合格的性质及其对产品和服务符合性的影响采取适当措施。也适用于在产品交付之后，以及在服务提供期间或之后发现的不合格产品和服务。

8.6.2. 组织应通过下列一种或几种途径处置不合格输出，对不合格输出进行纠正之后应验证其是否符合要求：

1) 纠正；
2) 隔离、限制、退货或暂停对产品和服务的提供；
3) 告知顾客；
4) 获得让步接收的授权。

8.6.3. 组织应保留下列成文信息：

1) 描述不合格；
2) 描述所采取的措施；
3) 描述获得的让步。
4) 识别处置不合格的授权。

9. 绩效评价

9.1. 监视、测量、分析和评价

9.1.1. 总则

1) 组织应确定：
   ① 需要监视和测量什么；
   ② 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；
   ③ 何时实施监视和测量；
   ④ 何时对监视和测量的结果进行分析和评价。
2) 组织应评价 安全风险管理体系 的绩效和有效性。
3) 组织应保留适当的成文信息，以作为结果的证据。

9.1.2. 顾客满意

1) 组织应监视顾客对其需求和期望已得到满足的程度的感受。
2) 组织应确定获取、监视和评审该信息的方法。

注：监视顾客感受的例子可包括顾客调查、顾客对交付产品或服务的反馈、顾客座谈、市场占有率分析、顾客赞扬、 担保索赔和经销商报告。

9.1.3. 分析与评价

1) 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。
2) 应利用分析结果评价：
   ① 产品和服务的符合性；
   ② 顾客满意程度；
   ③ 安全风险管理体系 的绩效和有效性；
   ④ 策划是否得到有效实施；
   ⑤ 应对风险和机遇所采取措施的有效性；
   ⑥ 外部供方的绩效；
   ⑦ 安全风险管理体系 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 安全风险管理体系 的下列信息：

1) 审核是否符合：
   ① 组织自身的 安全风险管理体系 要求；
   ② 本标准的要求；
2) 是否得到有效的实施和保持。

9.2.2. 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

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。

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：

1) 以往管理评审所采取措施的情况；
2) 与 安全风险管理体系 相关的内外部因素的变化；
3) 下列有关 安全风险管理体系 绩效和有效性的信息，包括其趋势：
   ① 顾客满意和有关相关方的反馈；
   ② 培训目标的实现程度；
   ③ 过程绩效以及产品和服务的合格情况；
   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。
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。

9.3.3. 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 安全风险管理体系 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. 总则

10.1.1. 组织应确定和选择改进机会，并采取必要措施，以满足顾客要求和增强顾客满意。

10.1.2. 改进措施包括：

1) 改进产品和服务，以满足要求并应对未来的需求和期望；
2) 纠正、预防或减少不利影响；
3) 改进 安全风险管理体系 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. 不符合与纠正措施

10.2.1. 当出现不符合项时，包括来自投诉的不符合项，组织应：

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 安全风险管理体系 。

10.2.2. 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。

10.3. 持续改进

10.3.1. 组织应持续改进 安全风险管理体系 的适宜性、充分性和有效性。

10.3.2. 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。

————————————————