Q/GDGZ

广东国准认证服务有限公司企业标准

Q/GDGZ 012-2025

安全风险管理体系 要求

Requirements for the safety risk management system

2025年11月25日发布　　2025年11月25日实施

广东国准认证服务有限公司　发布

前 言

本文件按照GB/T 1.1-2020《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。

本文件由广东国准认证服务有限公司提出。

本文件由广东国准认证服务有限公司归口。

本文件主要起草人：王燕、麦佩莹、银倩、许二红、黄俪等人。

目录

安全风险管理体系 要求

1 范围

本文件规定了建立、实施、保持和持续改进安全风险管理体系的具体要求。为组织建立安全风险管理体系提供参考。

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 1.1 《标准化工作导则标准化文件的结构和起草规则》

GB/T 19001 《质量管理体系 要求》

GB/T 19000-2016 《质量管理体系基础和术语》

GB/T 19025-2023/ISO 10015:2019 《质量管理 能力管理和人员发展指南》

GB/T 23694-2024《风险管理 术语》

3 术语和定义

GB/T23694-2024 界定的以及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。

3.2 目标 objective

要实现的结果。

3.3 不确定性 uncertainty

与理解或知识有关的信息不足(即使只是部分不足)的状态。

3.4 风险管理 risk management

指导和控制组织在风险方面的协调活动。

3.5 风险管理成熟度riskmanagementmaturity

与实现组织目标有关的风险管理能力水平的度量。

3.6 风险管理体系 riskmanagementsystem

风险管理文化、风险管理职责分工、风险偏好、制度流程及管理风险所需的基础和工具等管理要素的有机整体。

4 组织所处的环境

4.1 理解组织及其所处的环境

组织应识别和确定与其目标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各种外部和内部因素。

组织应对这些内部和外部因素的相关信息进行监视和评审。

注 1:这些因素可以包括需要考虑的正面和负面要素或条件。

注 2:外部因素，主要考虑法律、 自然环境、技术、社会、社会责任、竞争与合作等方面。

注 3:内部因素，主要考虑组织的使命、理念、价值观、文化和组织结构。

4.2 理解相关方的需求和期望

组织应确定:

a)与安全风险管理体系有关的相关方;

b)各相关方有关安全风险管理的需求和期望。

4.3 确定安全风险管理体系的范围

4.3.1 组织应界定安全风险管理体系的边界和应用范围，确定该范围时，应考虑:

a)各种内部和外部因素，见4.1;

b)相关方的需求和期望，见4.2;

c)其组织单元和职能边界;

d)其活动、产品和服务;

e)其实施控制与施加影响的权限和能力。

4.3.2 范围一经界定，在该范围内组织的所有活动、产品和服务均须纳入安全风险管理体系管理。

4.3.3 应保持所界定范围的形成文件的信息，并可为相关方所获取。

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内的应用，且应:

a)确定这些过程所需要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)，以确保这些过程的运行和有效控制；

d)确定并确保获得这些过程所需的资源；

e)规定与这些过程相关的主体、责任和权限；

f)应对按照6.1 的要求所确定的风险和机遇；

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 在必要的程度上，组织应:

a)保持安全风险管理体系及其过程的形成文件的信息，以支持过程运行:

b)保持确认其过程按策划进行的形成文件的信息。

5 领导作用

5.1 领导作用和承诺

最高管理者应证实其在安全风险管理体系方面的领导作用和承诺，通过:

a)对安全风险管理体系的有效性负责；

b)确保已制订相应的安全风险管理体系方针及目标，且与组织的战略方向相一致；

c)将安全风险管理体系理念贯彻到组织管理的战略、规划和运营过程中；

d)在战略规划中考虑安全风险管理体系管理；

e)确保安全风险管理体系所需的资源的供给，以实现安全风险管理体系目标；

f)促进安全风险管理体系的持续改进和创新。

5.2 安全风险管理体系方针

最高管理者应制定、实施和保持安全风险管理体系方针，方针应:

a)与组织的使命和发展战略相匹配；

b)为制定安全风险管理体系管理目标提供框架；

c)包括安全风险管理体系的承诺和持续改进管理体系的承诺；

d)保持安全风险管理体系方针的形成文件的信息，在组织内部进行沟通和传达，并付诸实施；

e)适宜时，可向相关方提供。

5.3 组织的岗位、职责及权限

最高管理者应在组织内部分配并沟通相关岗位的职责和权限，以确保:

a)安全风险管理体系符合本标准的要求；

b)各过程获得其预期输出；

c)向最高管理者报告安全风险管理体系的绩效及改进机会；

d)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 应对风险与机遇的措施

6.1.1 策划安全风险管理体系时，组织应从全生命周期的观点，确定需要应对的风险和机遇，应考虑:

a) 4.1 所描述的因素和 4.2 所提及的要求；

b)安全风险管理体系的范围；

c)安全风险管理体系管理的各个环节；

d)环境效益、经济效益与社会效益的平衡。

以确保安全风险管理体系能够实现预期结果，增强有利影响，实现持续改进。

注：安全风险管理体系管理环节可能包括：设计阶段、资源化利用阶段、再生阶段。

6.1.2 组织应策划:

a)应对这些风险和机遇的措施；

b)在安全风险管理体系过程中整合并实施这些措施；

c)评价这些措施的有效性。

6.2 目标及其实现的策划

6.2.1 组织对安全风险管理体系所需的相关职能、主体、层次和过程设定安全风险管理体系管理目标。 目标应:

a)平衡环境效益、经济效益与社会效益；

b)与组织的安全风险管理体系方针一致；

c)考虑到适用的要求；

d)可评价；

e)可实现；

f)予以监视；

g)予以沟通；

h)适时更新。

6.2.2 组织策划如何实现其安全风险管理体系管理目标时，应确定:

a)需要做什么；

b)需要哪些资源；

c)由谁负责；

d)如何将其与组织的管理过程相结合；

e)何时完成及相应的时间表；

f)如何评价结果。

6.2.3 组织应确定变更的需求和机会，以保持和改进安全风险管理体系管理绩效。

6.2.4 组织应有计划、系统地进行变更，识别风险和机遇，并评价变更的潜在。

6.2.5 组织应保持目标的形成文件的信息。

6.3 变更的策划

6.3.1 当下列情祝发生时，组织应对安全风险管理体系进行变更，

a)安全风险管理体系因素发生变化时:

b)法律、法规和其它要求发生变化时，

o)提高安全风险管理体系管理绩效的技术、设备和经验方法适用时。

6.3.2 组织在策划变更时，应考虑:

a)变更目的及潜在后果；

b)安全风险管理体系的完整性；

c)资源的可获得性；

d)责任和权限的分配或再分配。

6.3.3 组织应保持变更策划结果的形成文件的信息并适时更新。

6.4 过程策划

组织应考虑:

a)安全风险管理体系要求；

b)功能要求；

c)经济性要求；

d)法律法规要求；

e)最佳可行技术要求；

f)客户需求。

g)应急响应能力。

7 支持

7.1 资源

7.1.1 总则

组织应确定并提供建立、实施、维护和持续改进安全风险管理体系所需的资源。

组织应考虑:

a)现有内部资源的能力和局限性；

b)需要从外部相关方获得的资源。

7.1.2 人员

组织应确定并提供所需的人员，以有效实施安全风险管理体系并运行和控制其过程。

组织应:

a)确保相关人员知晓安全风险管理体系方针、 目标及对安全风险管理体系有效性的贡献；

b)确定关键岗位人员所需具备的知识和能力；

c)基于适当的教育、安全风险或经历，确保这些人员能够胜任工作；

d)适当时，采取措施以获得所必需的能力，并评价所采取措施的有效性。

7.1.3 设施设备

组织应确定、提供和维护绿色过程运行所需的设施设备，以实现组织的安全风险管理体系管理目标。

7.2 信息交流

7.2.1 总则

7.2.1.1 组织应确定与安全风险管理体系相关的内部和外部信息交流的过程包括:

a)信息交流的内容；

b)信息交流的时机；

c)信息交流的对象；

d)信息交流的方法、工具和方式。

7.2.1.2 组织应当保证其信息交流的质量。适当时，组织应保留信息交流的形成文件的信息，作为其信息交流的证据。

7.2.2 内部信息交流

组织应:

a)在其各职能和层次间就安全风险管理体系的相关信息进行内部信息交流适当时，包括安全风险管理体系变更的交流；

b)确保其信息交流过程能够促使在其控制下工作的人员对持续改进做出贡献。

7.2.3 外部信息交流

组织应:

a)与影响安全风险管理体系管理绩效的相关方进行外部信息交流与共享；

b)以优化安全风险管理体系管理绩效为目标，进行协同决策。

7.3 形成文件的信息

7.3.1 总则

组织的安全风险管理体系应包括:

a)本标准所要求的形成文件的信息；

b)组织确定的安全风险管理体系有效性所需的形成文件的信息。

7.3.2 创建和更新

创建和更新形成文件的信息时，组织应确保适当的:

a)标识和说明(如:标题、 日期、作者、索引编号等）；

b)格式(如:语言、软件版本、图示)和媒介(如:纸质、电子格式）；

c)评审和批准，以确保适宜性和充分性。

7.3.3 形成文件的信息的控制

7.3.3.1 应控制安全风险管理体系和本标准所要求的形成文件的信息，以确保:

a)无论何时何处需要这些信息，均可获得并适用；

b)予以妥善保护(如:防止失密、不当使用或不完整)。

7.3.3.2 为控制形成文件的信息，组织应关注下列活动:

a)分发、访问、检索和使用；

b)存储和防护，包括保持可读性；

c)变更控制(比如版本控制）；

d)保留和处置。

7.3.3.3 对策划和运行安全风险管理体系所必需的来自外部的原始的形成文件的信息，组织应进行适当识别和控制。

7.3.3.4 应对所保存的作为符合性证据的形成文件的信息予以保护，防止非预期的更改。

8 运行

8.1 运行策划和控制

8.1.1 组织应从全生命周期的观点出发，策划、实施、控制和保持满足安全风险管理体系要求所需要的过程(见 4.4)，并实施第 6 章中所确定的措施，通过：

a)制定过程的运行准则；

b)按照运行准则实施过程控制。

8.1.2 组织应对计划内的变更进行控制，并对非预期性变更的后果予以评审，必要时，应采取措施降低对安全风险管理体系管理绩效的有害影响。

8.1.3 组织应确保对外包过程实施控制或施加影响。应在安全风险管理体系内规定对这些过程或组织实施控制或施加影响的类型与程度。

8.1.4 组织应保持必要的形成文件的信息，以确信上述过程已按策划得到实施。

8.2 应急准备和响应

8.2.1 组织应建立、实施和保持对 6.1.1 中识别的对安全风险管理体系管理有影响的潜在紧急情况进行应急准备并做出响应所需的过程。

组织应:

a)通过策划措施做好相应紧急情况的准备，以预防或减轻有害影响；

b)对实际发生的紧急情况做出响应；

c)根据紧急情况和潜在的对绿色绩效的影响程度，采取相适应的措施预防或减轻紧急情况带来的后果；

d)可行时，定期试验所策划的响应措施；

e)定期评审并修订过程过程和策划的响应措施，特别是发生紧急情况后或进行。

f)适用时，向有关的相关方，包括在组织控制下工作的人员提供应急准备和响应相关的信息和安全风险。

8.2.2 组织应保留必要的形成文件的信息，以确信过程按策划得到实施。

9 绩效评价

9.1 监视、测量、分析和评价

9.1.1 总则

9.1.1.1 组织应监视、分析和评价其安全风险管理体系管理绩效。组织应确定

a)需要监视和测量的内容:

b)适用时，监视、测量、分析和评估的方法，以确保有效的结果；

c)组织评价其安全风险管理体系管理绩交责效所信依据的准则和适当的参数；

d)实施监视、价监视、测量结果的时机。

9.1.1.2 组织应确保使用经过校准或验证的监视和测量设备,并对其予以维护。

9.1.1.3 组织应评价其安全风险管理体系管理绩效和安全风险管理体系的有效性。

9.1.1.4 组织应按其建立的信息交流过程的规规定以及法律法规的要，就有关安全风险管理体系管理绩效的信息进行内部和外部信息交流。

9.1.1.5 组织应保留适当的形成文件的信息，作为监规、测量、分析和评价结果的证据。

9.1.2 分析与评价

9.1.2.1 组织应分析和评价通过监视和测量获得的适宜的数据和信息。这应包括适用方法的确定。应利用分析结果评价:

a)确定安全风险管理体系的适宜性、充分性、有效性；

b)确保活动、产品和服务能持续满足利益相关方要求；

c)确保过程的有效运行和控制；

d)识别安全风险管理体系的改进机会。

9.1.2.2 数据分析和评价的结果应作为管理评审的输入。

9.2 内部审核

9.2.1 总则

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:

a)是否符合:

b)组织自身的安全风险管理体系要求；

c)本标准的要求。

b)是否得到了有效地实施和保持。

9.2.2 内部审核方案

9.2.2.1 组织应建立、实施并保持一个或多个内部审核方案，包括实施审核的频次、方法、职责、策划要求和内部审核报告。

9.2.2.2 建立内部审核方案时，组织应考虑相关过程对于绿色绩效的重要性、影响组织的变化以及以往审核的结果。

组织应:

a)规定每次审核的准则和范围；

b)选择审核员并实施审核，确保审核过程的客观性与公正性；

c)确保向相关管理者报告审核结果。

9.2.2.3 组织应保留文件化信息，作为审核方案实施和审核结果的证据。

9.3 管理评审

9.3.1 总则

最高管理者应按计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。

9.3.2 管理评审输入

策划和实施管理评审应考虑下列内容:

a)以往管理评审所采取措施的实施情况；

b)与安全风险管理体系相关的内外部因素的变化；

c)有关安全风险管理体系绩效和有效性的信息，包括下列趋势性信息:

1)相关方的反馈；

2)安全风险管理体系管理目标的实现程度；

3)不符合和纠正措施；

4)监视和测量的结果；

5)适用法律要求；

6)自愿义务；

7)审核结果。

8)资源的充分性；

9)应对风险和机遇所采取措施的有效性；

10)改进的机会。

9.3.3 管理评审的输出

9.3.3.1 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)安全风险管理体系所需的变更；

c)资源需求。

9.3.3.2 组织应保留作为管理评审结果证据的形成文件的信息。

10 持续改进

10.1 总则

组织应确定改进的机会(见 9.1，9.2 和 9.3)，并实施必要的措施实现其安全风险管理体系的预期结果。

10.2 不符合和纠正措施

10.2.1 发生不符合时，组织应:

a)对不符合做出响应，适用时:

1)采取措施控制并纠正不符合；

2)处置产生的后果。

b)通过以下方式评价消除不符合原因的措施需求，以防止不符合再次发生或在其他地方发生:

1)评审不符合；

2)确定不符合的原因；

3)确定是否存在或是否可能发生类似的不符合。

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，更新策划期间确定的风险和机遇；

f)需要时，对安全风险管理体系进行变更。

10.2.2 纠正措施应与所发生的不符合造成影响的重要程度相适应。

10.2.3 组织应保留形成文件的信息作为下列事项的证据:

a)不符合的性质和所采取的任何后续措施；

b)任何纠正措施的结果。

10.3 持续改进

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，以提升安全风险管理体系管理绩效。