ICS 13.200
CCS

中华人民共和国国家标准

GB/T 43500-2023

安全管理体系 要求

Safety management systems — Requirements

2023-11-27 发布 2024-06-01实施

国家市场监督管理总局
国家标准化管理委员会 发布

目次

1 范围 4
2 规范性引用文件 4
3 术语和定义 4
4 组织及环境 7
4.1 组织及其所处的环境 7
4.2 相关方的需求和期望 7
4.3 安全管理体系的范围 8
4.4 安全管理体系及其过程 8
5 领导作用与全员参与 8
5.1 领导作用 8
5.2 安全方针 10
5.3 组织结构、职责和权限 10
5.4 全员参与 10
6 策划 11
6.1 法律法规要求和其他要求的确定 11
6.2 应对风险的策划 11
6.2.1 总则 11
6.2.2 风险识别 13
6.2.3 风险分析和评价 13
6.2.4 措施的策划 14
6.3 安全目标及其实现的策划 14
6.3.1 安全目标 14
6.3.2 实现安全目标的策划 14
6.4 变更的策划 14
7 支持 15
7.1 总则 15
7.2 资源 15
7.2.1 总则 15
7.2.2 人员 15
7.2.3 资金 15
7.2.4 设备设施与物资 15
7.2.5 知识与技术 16
7.2.6 外部资源 16
7.3 安全文化 16
7.3.1 组织安全文化 16
7.3.2 个体安全文化 16
7.4 沟通 16
7.4.1 总则 16
7.4.2 内部沟通 17
7.4.3 外部沟通 17
7.5 文件化信息 17
7.5.1 总则 17
7.5.2 创建和更新 17
7.5.3 管理和控制 17

8 运行 18
8.1 运行的策划和控制 18
8.1.1 总则 18
8.1.2 安全风险管控 18
8.1.3 隐患排查治理 18
8.2 应急准备和响应 19
9 绩效评价 19
9.1 监视、测量、分析、评价 19
9.1.1 总则 19
9.1.2 合规性评价 20
9.2 内部审核 20
9.2.1 总则 20
9.2.2 内部审核程序 20
9.3 管理评审 20
9.3.1 总则 20
9.3.2 管理评审输入 21
9.3.3 管理评审输出 21
10 改进 21
10.1 事件、不符合和纠正措施 21
10.2 持续改进 22

安全管理体系要求

1 范围

本文件提出了安全管理体系的要求，旨在使组织能够控制风险并改进安全绩效，但是它既不规定具体的安全绩效准则，也不提供详细的安全管理体系设计规范。

本文件适用于有意向建立、实施、保持和改进安全管理体系的所有类型和规模的组织。

本文件适用于生产安全、社区安全、功能区安全、公共场所安全、校园安全、交通安全、防灾减灾安全等领域，但不适用于信息安全、产品安全、公安等行业领域。

本文件提供了一种整体和通用的方法，而不是行业或领域特有的要求。

本文件可以在组织的整个生命周期中使用，并可以应用于所有级别的任何活动，包括内部和外部活动。

本文件能够全部或部分地用于组织改进和优化安全管理。然而，只有当本文件的所有要求均被包含在了组织的安全管理体系中并全部得到满足，有关符合本文件的声明才能被认可。

2 规范性引用文件

本文件没有规范性引用文件。

3 术语和定义

下列术语和定义适用于本文件。

3.1

组织 organization

为实现目标(3.12)，由职责、权限和相互关系构成自身功能的一个人或一组人。

注：组织包括但不限于企事业单位、政府机构、社团、个体工商户，或者上述组织的某部分或其组合，无论其是否为法人组织、公有或私有。

3.2

相关方 interested party

可影响或者受到决策或活动所影响，或者自认为受决策或活动影响的个人或组织(3.1)。

示例：相关方可包括顾客、游客、居民、社区、供方、监管部门、非政府组织、投资方和工作人员。

3.3

工作人员 staff

在组织(3.1)管理下开展工作或与工作相关的活动的人员。

注1：在不同安排下，人员有偿或无偿地开展工作或与工作相关的活动，如定期的或临时的、间歇性的或季节性的、偶然的或兼职的等。

注2：工作人员包括最高管理者(3.8)、管理类人员和非管理类人员。

注3：根据组织所处的环境，在组织控制下所开展的工作或与工作相关的活动可由组织雇佣的工作人员、外部供方的工作人员、承包方、个人、外部派遣工作人员，以及其工作或与工作相关的活动在一定程度上受组织共同控制的其他人员来完成。

3.4

要求 requirement

明示的、通常隐含的或必须满足的需求或期望。

注1: “通常隐含的”是指，对组织(3.1)和相关方(3.2)而言，按惯例或常见做法，对这些需求或期望加以考虑是不言而喻的。

注2:规定的要求是指经明示的要求，如文件化信息中所阐明的要求。

3.5

法律法规要求和其他要求 legal requirements and other requirements

组织(3.1)必须遵守的法律法规要求，以及组织必须遵守或选择遵守的其他要求(3.4)。

注1:对本文件而言，法律法规要求和其他要求是与安全管理体系(3.7)相关的要求。

注2: “法律法规要求和其他要求”包括集体协议的规定，例如：组织的和行业的标准、合同规定、与社团或非政府组织间的协议。

3.6

管理体系 management system

组织(3.1)用于建立方针(3.10)和目标(3.12)以及实现这些目标的过程的一组相互关联或相互作用的要素。

注1: 一个管理体系可针对单个或多个领域。

注2: 体系要素包括组织的结构、角色和职责、策划、运行、绩效评价和改进。

注3: 管理体系的范围可包括：整个组织，组织中具体且可识别的职能或部门，或者跨组织的一个或多个职能。

3.7

安全管理体系 safety management system

用于建立和实现安全方针(3.10)和目标的管理体系或管理体系的一部分。

3.8

最高管理者 top management

在最高层指挥和控制组织(3.1)的一个人或一组人。

注1:在保留对安全管理体系(3.7)承担最终责任的前提下，最高管理者有权在组织内授权和提供资源。

注2:若管理体系的范围仅覆盖组织的一部分，则最高管理者是指那些指挥和控制该部分的人员。

3.9

领导作用 Leadership

确立战略方针目标，建立管理体系，并运用人力、物力、财力等资源确保有效实施，达到目标的能力。

3.10

方针 policy

由组织最高管理者(3.8)正式表述的组织(3.1)的意图和方向。

3.11

安全方针

由组织最高管理者(3.8)发布的安全宗旨，体现内部的安全追求和行为准则，以及对外部的安全承诺。

注：安全方针，是组织防止人员伤害和健康损害、财产损失、并提供健康安全的环境的总体意图和方向的表述。

3.12

目标 objective

要实现的结果。

注1:目标可以是战略性的、战术性的或运行层面的。

注2: 目标可涉及不同领域(如财务的、健康安全的和环境的目标),并可应用于不同层面(如战略层面、组织整体层面、项目层面、产品和过程层面)。

注3:目标可按其他方式来表述，例如：按预期结果、意图、追求、目的、运行准则来表述目标。

注4: 安全目标，是由组织设定的，与安全方针一致的，与安全相关的目标。

3.13

安全目标 Safety objective

组织(3．1)为实现与安全方针(3．11)相一致的特定结果而制定的目标(3．12)。

3.14

安全文化 safety culture

组织(3．1)运行或管理过程形成的对安全的态度、理念、意识、行为方式，以及安全制度的总和。

注：安全文化是存在于组织(3.1)和个人中的种种素质和态度的总和。

3.15

危险源 hazard

可能导致人员伤害、健康损害、财产损失或环境破坏的源头。

3.16

风险 risk

不确定因素对目标(3．12)的影响。

注1: 影响是指对预期的偏离——正面的或负面的。

注2: 不确定性是指对事件及其后果或可能性缺乏甚至部分缺乏相关信息、理解或知识的状态。

注3: 通常，风险以潜在事件(3.24)和后果，或两者的组合来描述其特性。

注4: 通常，风险以某事件(3.24) (包括情况的变化)的后果及其发生的可能性的组合来表述。

注5:本文件中风险指安全风险(3.17)

3.17

安全风险 Safety risk

发生人员伤害和健康损害、财产损失、环境破坏的可能性与其后果严重性的组合。

3.18

隐患 Hidden peril

可导致安全事件(3.24)发生的人的不安全行为、物的不安全状态、管理的缺陷，或其中一种或几种的组合。

3.19

监视 monitoring

确定体系、过程或活动的手段和过程。

注：为了确定状态，可能需要检查、监督或批判地观察。

3.20

审核 audit

为获得审核证据并对其进行客观评价，以确定满足审核准则的程度所进行的系统的、独立的和文件化的过程。

注1:审核可以是内部(第一方)审核或外部(第二方或第三方)审核，也可以是一种结合(结合两个或多个领域)的审核。

注2:内部审核由**组织** (3.1)自行实施或由外部方代表其实施。

注3: “审核证据”和“审核准则”的定义见GB/T 19011。

3.21

绩效 performance

可量化的结果。

注1: 绩效可能涉及定量或定性的发现。结果可由定量或定性的方法来确定或评价。

注2:绩效可能涉及活动、过程、产品、服务、体系或组织(3.1)的管理。

3.22

符合 conformity

满足要求(3.4)。

3.23

不符合 **nonconformity**

未满足要求(3.4)。

注：不符合与本标准的要求和组织(3.1)自己确定的安全管理体系(3.7)附加的要求有关。

3.24

事件incident

可能或已经导致人员伤害、健康损害、财产损失或环境破坏的情况。

注1:发生伤害、损失或破坏的事件有时被称为“事故”。

注2:未发生但有可能发生伤害、损失和破坏的事件在英文中称为 “near-miss″、″near-hit″或″close call”，在中文中也可称为“未遂事件” 、“未遂事故”或“事故隐患”等。

注3:尽管事件可能涉及一个或多个不符合(3.22),但在没有不符合(3.23)时也可能会发生。

3.25

持续改进 continual improvement

提高绩效(3.21)的循环活动。

注1: 提高绩效涉及使用安全管理体系(3.7)以实现与安全方针(3.11)和安全目标(3.13)相一致的整体安全绩效的改进。

注2:持续并不意味着不间断，因此活动不必同时在所有领域发生。

4 组织及环境

4.1 组织及其所处的环境

组织应确定与其宗旨相关并影响其实现安全管理体系预期结果的内部和外部因素，包括受组织影响的或能够影响组织的因素。

组织应对这些内部和外部因素的相关信息进行监视和评价。

注1:内部和外部因素可能是正面的或负面的，包括能影响组织安全管理体系的条件、特性或变化情况。

注2: 为利于理解外部环境，可考虑来自于国际、国内、地区或当地的政治、法律法规、文化、社会、经济或金融、技术、市场竞争、自然环境等有关的因素。

注3:为利于理解内部环境，可考虑与组织的属性、特征、价值观和文化等有关的因素。

4.2 相关方的需求和期望

组织应确定：

a) 与安全管理体系有关的相关方；

b) 相关方与安全管理体系有关的需求和期望；

c) 这些需求和期望中哪些是或将可能成为法律法规要求和其他要求；

d) 这些需求中哪些将通过安全管理体系来解决。

4.3 安全管理体系的范围

组织应明确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) 内部和外部因素(见4.1)；

b) 相关方的需求和期望(见4.2)；

c) 所计划或实施的活动。

安全管理体系应包括在组织控制下或在其影响范围内可能影响组织安全绩效的活动、产品和服务。

组织应将范围形成文件化信息。

4.4 安全管理体系及其过程

组织应按照本文件的要求建立、实施、保持和持续改进安全管理体系，包括所需的过程及其相互作用。安全管理体系应与组织的其他管理体系相融合。

组织应确定安全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获得；

e) 分配这些过程的职责和权限；

f) 按照策划(见6)实施过程保留文件化信息以支持过程运行，确信其过程按策划进行；

g) 有效评价过程，及时整改变更，以确保实现这些过程的预期结果；

h) 改进过程和安全管理体系。

5 领导作用与全员参与

5.1 领导作用

最高管理者应通过以下方式证实其在安全管理体系方面的领导作用并承诺：

a) 对安全管理体系及其绩效全面负责并承担责任；

b) 明确建立安全方针和安全目标，并与组织战略方向相一致；

c) 确保安全管理体系要求融入组织业务过程之中；

d) 确保建立、实施、保持和改进安全管理体系所需的资源；

e) 就有效的安全管理和符合安全管理体系要求的重要性进行沟通；

f) 确保安全管理体系实现其预期结果；

g) 指导并支持保持和增强安全管理体系的有效性行为；

h) 确保并促进安全绩效和安全管理体系的持续改进；

i) 支持和监督其他相关管理者在其职责范围内发挥领导作用；

j) 在组织内建立、引导和促进安全文化；

k) 保护各种有利于安全保障的做法和行动，保护相关方不因报告隐患、违规行为、事件等而遭受报复；

l) 强化对重大危险源、重大安全风险、重大事故隐患以及新型风险的关注和控制；

m) 确保充分考虑相关方的安全需求和期望，必要时，建立、实施其协商和参与的过程；

n) 必要时，支持在组织内建立和运行安全管理委员会或工作组。

注：本文件中的“业务”可从广义上理解为涉及组织存续发展的活动。

5.2 安全方针

最高管理者应结合组织的愿景、战略、宗旨、规模、业务以及组织所处环境(见4.1),建立、实施和保持安全方针。

安全方针应：

a) 适合于组织，以及组织的安全风险的特性；

b) 为制定安全目标提供框架；

c) 明确安全管理融入组织的相关业务和活动；

d) 包括以下承诺：

——为防止人员伤亡、健康损害、财产损失、环境破坏而提供安全保障；

——满足法律法规要求和其他要求；

——消除隐患和降低安全风险；

——持续改进安全管理体系；

——鼓励相关方协商和参与。

安全方针应：

——作为文件化信息而可被获取；

——在组织内予以沟通；

——在适当时可为相关方所获取；

——保持相关和适宜。

5.3 组织结构、职责和权限

最高管理者应确保将安全管理体系内相关角色及其职责、权限分配到组织内各层次并予以沟通，且作为文件化信息予以保持。组织内每一层次的工作人员均应承担其所控制部分安全管理职责。

必要时，最高管理者应确保建立、健全组织内全员安全责任制，并确保将安全职责和权限传递到组织内各层次。

最高管理者应对下列事项分配职责和权限：

a) 确保安全管理体系符合本文件的要求；

b) 向最高管理者报告安全管理体系的绩效。

5.4 全员参与

组织应按照本文件的要求建立、实施、保持和持续改进安全管理体系，包括所需的过程，用于所有相关人员在安全管理体系的开发、策划、实施、绩效评价和改进措施中的协商和参与。

组织应：

a) 为协商和参与提供必要的机制、时间、培训和资源；

注1:工作人员代表可视为一种协商和参与机制。

b) 及时提供组织安全管理相关信息的沟通渠道；

c) 确定和尽可能消除妨碍参与的障碍或壁垒，并尽可能减少那些难以消除的障碍或壁垒；

注2:障碍和壁垒可包括未回应的意见和建议，语言或读写障碍，报复或威胁报复，以及不鼓励或惩罚内部人员参与的政策或惯例等。

d) 强调与非管理类人员在如下方面的协商：

1) 确定相关方的需求和期望(见4.2) ；

2) 建立安全方针(见5.2)；

3） 适用时，分配组织的职责和权限(见5.3) ；
4） 确定如何满足法律法规要求和其他要求(见6.1)；
5） 制定安全目标并为其实现进行策划(见6.3)；
6） 制定安全相关的管理规定；
7） 确定对外包、采购和承包方适用的控制措施；
8） 确定所需监视、测量和评价的内容(见9.1) ；
9） 策划、建立、实施和保持审核方案(见9.2.2)；
10)确保持续改进(见10.2)。

e） 强调非管理类人员在如下方面的参与：
1） 确定其协商和参与的机制；
2） 辨识危险源、隐患，并评价安全相关的风险(见6.2) ；
3） 确定能力要求、培训需求，并参与培训效果评价(见7.2.2)；
4） 组织安全文化建设(见7.3)；
5） 确定沟通的内容和方式(见7.4)；
6） 确定风险控制措施及其有效的实施和应用(见8.1.2) ；
7） 确定消除隐患的措施(8.1.3)；
8） 调查事件和不符合并确定纠正措施(见10.1)；
9） 寻求改进安全管理体系的机会(见10.2)。

注3:强调非管理类工作人员的协商和参与，旨在适用于执行工作活动的人员，但无意排除其他人员，如受组织内工作活动或其他因素影响的管理者。

注4:需认识到，若可行，向工作人员免费提供培训以及在工作时间内提供培训，可以消除工作人员参与的重大障碍。

6 策划

6.1 法律法规要求和其他要求的确定

组织应建立、实施和保持过程，以：

a） 确定最新的适用于组织安全管理相关的法律法规要求和其他要求；

b） 确定如何将这些法律法规要求和其他要求应用于组织，以及所需沟通的范围和内容；

c） 在建立、实施、保持和持续改进其安全管理体系时，必须考虑这些法律法规要求和其他要求；

组织应保持和保留有关法律法规要求和其他要求的文件化信息，并确保及时更新以反映任何变化。

注：法律法规要求和其他要求可能会给组织带来风险和机遇。

6.2 应对风险的策划

6.2.1 总则

在对安全管理体系进行策划时，组织应考虑所处的环境(见4.1)、相关方所提及的要求(见4.2)和安全管理体系的范围(见4.3),基于风险管理的原理，识别分析和评价安全相关风险，并策划应对措施，以

——满足法律法规要求和其他要求；
——保证安全管理体系能够实现预期的结果；
——防止或减少不期望的影响；

_____对紧急情况做出准备和响应；

_____提升组织安全文化：

——实现持续改进。

6.2.2 风险识别

组织应识别与安全相关的风险，并进行评估，可考虑如下方面：其中应考虑的包括但不限于：

a) 常态和非常态的状况和活动，包括由以下方面所产生的危险源：

1) 基础设施、设备、原料、材料和工作场所的物理环境及其失效模式；

2) 全生命周期中的活动、产品和服务；

b) 组织内部或外部以往发生的相关事件(包括紧急情况)及其原因；

c) 环境、人、文化以及其他内部或外部因素，包括组织控制之外的但能影响组织安全的因素；

d) 组织的管理架构、责任体系；

e) 人员的安全意识和能力，人员的范围包括组织工作人员及可能受到组织影响的其他人员；

f) 组织的运行、过程、活动和安全管理体系中实际的或拟定的变更；

g) 涉及到的信息、数据、知识的变更；

h) 安全威胁、隐患及潜在紧急情况；

i) 新出现的风险征兆；

j) 相关方之间的相互依赖关系。

注：风险识别的过程包括对危险源、影响范围、事件及其原因和潜在后果的识别。

组织应将风险识别的记录和信息应作为文件化信息予以保留。

6.2.3 风险分析和评价

组织应及时对已识别出的风险(见6.2.2)进行分析和评价，确定所需应对的风险(必要时，进行分级)，以快速确定合理精准的风险管控措施。

组织应确定风险分析评估人员与负责人，必要时，应由最高管理者组织管理层自行评价或聘请专业第三方安全风险评价机构分析评价。

a) 风险分析

风险分析的目的是理解包括风险水平在内的风险性质和特征，风险分析应考虑：

——风险转化为事件的可能性；

——风险造成后果的严重性以及可接受性；

——风险的复杂性、关联性和敏感性；

——风险随时间因素的波动性；

——现有控制措施的有效性。

注1:可接受性应考虑组织自身、相关方及社会的可接受程度。

b) 风险评价

风险评价可以通过将风险分析的结果与既定的风险准则进行比较，确定风险等级，以做出风险应对的决策。决策可能是：

——不采取风险管控措施；

——维持现有管控措施；

——采取新的风险管控措施；

——重新考虑安全管理目标。

组织决策应考虑内外部相关方的实际需求及预期后果，并记录、传递和验证风险评估的结果。

注2:组织应建立、保持、更新和完善有效的风险评价方法和准则，这些方法和准则的文件化信息应予以保持和保留。

注3:组织在建立风险准则、风险等级时，应依据法律法规、标准，并参照其他通用规范。

6.2.4 措施的策划

组织应策划应对风险的措施，并：

a) 在其安全管理体系过程中或其他业务过程中融入并实施这些措施；

b) 评价这些措施的有效性。

在策划措施时，组织应考虑：

——控制的层级(见8.1.2)和安全管理体系的输出；

——组织可以承受或不可承受的风险的数量和类型；

——在策划措施时，组织还应考虑最佳实践、可选技术方案以及财务、运行和经营等要求。

6.3 安全目标及其实现的策划

6.3.1 安全目标

组织应在相关职能和层次上制定安全目标，以保持和持续改进安全管理体系和安全绩效。安全目标应：

a) 与安全方针一致；

b) 可量化(如果可行)、可绩效评价；

c) 考虑适用的要求；

d) 适当考虑来自相关方的要求；

e) 被监督；

f) 可沟通；

g) 持续改进；

h) 形成文件化信息。

6.3.2 实现安全目标的策划

在策划如何实现安全目标时，组织应确定：

a) 要做的内容；

b) 所需的资源；

c) 负责的人员；

d) 完成的时间；

e) 评价的标准；

f) 实现安全目标的措施融入其业务过程的方式方法。

组织应保持和保留安全目标和实现安全目标的策划的文件化信息。

6.4 变更的策划

当组织确定安全管理体系需要变更时，包括因第10章的变更，应有计划的进行。无论是永久性的还是临时性的变更，应在变更前进行评价。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重新分配。

组织应结合实施过程评审变更的效果，必要时重新进行变更策划。

7 支持

7.1 总则

组织应基于法律法规要求和其他要求，结合发展战略与自身条件，积极建设和发展安全能力，以支持安全管理体系的建立、实施、保持和持续改进。

安全能力包括安全技术、安全管理、安全文化等保障能力，以及应急物资、应急响应、应急救援等事故应对处理能力。

7.2 资源

7.2.1 总则

组织在建立、实施、保持和持续改进安全管理体系时，应考虑：

a) 现有内部资源的能力和局限；

b) 需要从外部获得的资源。

7.2.2 人员

组织应：

a) 确定影响或可能影响安全绩效的人员所必需具备的能力；

b) 确保这些人员在适当的教育、培训和经验的基础上胜任工作，必要时获得适当的安全许可；

c) 在适用时，采取适当措施以获得必需的能力，并评估所采取措施的有效性；

d) 保留适当的文件化信息作为能力证据。

注1:此处人员可包括组织的工作人员和为组织活动提供支持或服务的人员，例如，承包方人员、劳务派遣人员、志愿者等。

注2:适当措施包括：向现有人员提供培训、指导、重新分配工作；聘用有能力的人员或将工作承包给能胜任工作的人员等。

组织的工作人员应意识到：

a) 安全方针和安全目标；

b) 其对安全管理体系有效性的贡献作用，包括提升安全绩效的益处；

c) 不符合安全管理体系要求的影响和潜在后果；

d) 与其相关的事件和调查结果；

e) 与其相关的安全风险和所确定的措施；

f) 从其所认为的存在急迫且严重危及其生命或健康的状况中逃离的能力，以及为保护其免遭由此而产生的不当后果所做出的安排。

7.2.3 资金

组织应确保安全管理体系建立、实施和持续改进所需的资金，必要时，设立安全管理专项资金，并专款专用。

7.2.4 设备设施与物资

组织应：

a) 确定所需的设备设施与物资；

b) 及时维护和更新这些设备设施与物资，确保其本身的安全性以及使用性能；

c) 确保人员能够正确使用这些设备设施与物资。

7.2.5 知识与技术

组织应：

a) 确定所需的安全相关的知识和技术；

b) 持续维护、更新、补充安全相关的知识与技术；

c) 确保人员能够掌握这些知识与技术，并开展评价。

注：组织的知识与技术也包括经验。

7.2.6 外部资源

组织应评估自身资源，可建立相适应的外部资源支持机制，包括但不限于：

a) 确定需求；

b) 识别外部资源，并评估其适用性；

c) 建立、实施、保持合作。

注1:组织不应因外部资源而减少自身必需的资源配备。

注2:组织宜考虑的外部资源包括政府机构、周边组织、专业化安全相关组织、外部自然环境等。

7.3 安全文化

组织应进行安全文化建设，构建良好安全文化氛围，强化全员安全意识，提高全员安全素质，增强人员对安全管理体系的理解和执行，以利于安全管理体系的实施、保持和持续改进。

7.3.1 组织安全文化

组织安全文化，应确保：

a) 明确安全愿景；

b) 明确安全管理战略、方针、目标；

c) 达成共识的安全管理理念、意识；

d) 推行安全管理机制及其文件化信息；

e) 提升全员安全能力；

f) 安全文化信息宣传、推广与共享；

g) 激励员工安全行为；

h) 重视员工安全心理素质；

i) 安全文化审核评估与持续改进；

j) 推进安全文化支撑安全管理体系的建设与发展。

7.3.2 个体安全文化

个体安全文化，应做到：

a) 全员安全承诺；

b) 全员安全自律。

7.4 沟通

7.4.1 总则

组织应建立、实施并保持和安全管理体系有关的内外部沟通所需过程，包括确定：

a) 沟通的内容

b) 沟通的时机；

c) 沟通的对象；
d) 沟通的方式；
e) 传播前就信息的敏感性的确认。

在考虑沟通需求时，组织应考虑：

- 各种差异(如性别、年龄、语言、民族、文化、读写能力、残障)；
- 沟通对象在沟通意愿方面的可能性，以确保沟通的有效性和安全性；
- 沟通对象可能的心理状况，及可能对事态的影响；
- 可能存在的沟通盲点和特殊人群，及使其获取告知内容的方式与效果。

组织应确保紧急情况下的沟通方案。在适用的情况下，组织应考虑如下方面的沟通：

—— 向可能遭受实际或即将发生的安全事件影响的相关方发出警示；

____确保与多个响应组织之间适当的协调和沟通。

沟通和警示应作为组织测试和培训项目的一部分进行演练。

组织应对有关安全管理体系的沟通做出响应。

组织应确保所沟通的安全信息与其安全管理体系内所形成的信息一致且可靠。

组织应建立对沟通效果的追踪和评价的机制。

组织应适当保留文件化信息作为其沟通的记录。

7.4.2 内部沟通

组织应：

a) 就其安全管理体系的相关信息在其不同层次和职能之间进行内部沟通，并确保沟通内容均被考虑；
b) 促使其沟通过程能够使工作人员为持续改进做出贡献。

7.4.3 外部沟通

组织应就安全管理体系的相关信息与相关方进行沟通，并必须遵守法律法规要求和其他要求。

7.5 文件化信息

7.5.1 总则

组织的安全管理体系文件应包括：

a) 相关法律法规和其他要求；
b) 本文件要求的文件化信息；
c) 组织确定的实现安全管理体系有效性所必需的文件化信息。

7.5.2 创建和更新

组织创建和更新文件化信息，内容应清晰明确，应确保适当的：

a) 标识和说明(如标题、日期、编者或文件编号)；
b) 形式(如语言文字、软件版本、图表)与载体(如纸质载体、电子载体)；
c) 评审和批准，以确保适宜性和充分性。

7.5.3 管理和控制

文件化信息应予以管理和控制，以确保：

a) 在需要的场所和时间均可获得并适用；

b) 得到充分的保护(如防止失密、不当使用或完整性受损)。

适用时，组织应针对下列活动来控制文件化信息：

——分发、访问、检索和使用；

——存储和保护，包括保持易读性；

____变更控制(如版本控制)：

——分类分级保留和处置。

组织应识别其所确定的、策划和运行安全管理体系所必需的、来自外部的文件化信息，适当时应对其予以控制。

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1: “访问”可能指仅允许查阅文件化信息的决定，或可能指允许并授权查阅和更改文件化信息的决定。

注2: “访问”相关文件化信息包括工作人员及其代表(若有)的“访问”。

8 运行

8.1 运行的策划和控制

8.1.1 总则

组织应通过以下方式对过程进行策划、实施和控制，以满足安全管理体系的要求，并实施第6章确定的措施，将其融于组织的各项活动中：

a) 建立过程准则；

b) 根据准则实施过程控制。

组织应适时与其他相关组织协调安全管理体系的相关部分。

组织应对外部供应方提供的产品和/或服务过程进行控制，确保其符合组织安全管理体系的要求。

组织应保留必要的文件化信息，确保过程已按策划得到实施。

8.1.2 安全风险管控

组织应基于对安全风险的识别(见6.2.2)、分析和评价(见6.2.3)的结果，及时确定所需应对的风险，制定和实施精准的风险管控措施。

组织应通过采用下列控制层级，建立、实施和保持用于降低安全风险的过程：

a) 消除危险源；

b) 用危险性低的过程、操作、材料或设备等替代；

c) 采用技术控制和重新组织活动；

d) 采用管理控制措施，包括培训；

e) 增强防护。

组织应针对降低安全风险的过程编制方案计划，该计划应作为文件化信息保留，在需要的时间和地点，组织应确保每项计划都能获得并且可用。

8.1.3 隐患排查治理

组织应基于风险识别、分析和评价(见6.2.3)的结果和相关法律法规要求和其他要求(见6.1)，识别、评价安全隐患信息，及时制定隐患排查治理的方案计划，实施和保持隐患排查治理过程，并保持和保留与此相关的文件化信息。

在确定隐患排查需求和频率时，应考虑：

a) 隐患引发安全事故的可能性；

b) 隐患可能引发的安全事故后果的严重程度；

c) 隐患自身可能发生的频率。

组织的隐患排查应明确：

——对象和范围

——内容和标准

——方法和频次

组织的隐患排查工作应在各职能层次开展，需要时可进行分级排查。

组织应针对排查出的安全隐患采取治理措施。隐患治理措施应结合事件、不符合和纠正措施(10.1)执行，并满足改进要求(见10.2)。

隐患排查治理工作应结合绩效评价(见9)要求。

注：隐患可能由风险管控的失效引起。

组织应针对隐患排查治理的过程编制方案计划，该计划应作为文件化信息保留，在需要的时间和地点，组织应确保每项计划都能获得并且可用。

8.2 应急准备和响应

为了对所识别的潜在紧急情况(见6.2.2)进行应急准备并做出响应，组织应建立、实施和保持所需的过程，包括：

a) 针对紧急情况建立响应机制、制定应急预案，包括提供急救；

b) 明确资源需求，并确保其处于随时可用状态；

c) 提供相应培训；

d) 定期开展应急预案演练，测试应急响应能力；

e) 评价绩效，必要时(包括在测试之后，尤其是在紧急情况发生之后)修订应急预案；

f) 与所有工作人员沟通明确其义务与职责，并提供有关信息；

g) 与其他相关方沟通相关信息；

h) 考虑所有有关相关方的需求和能力，适当时确保其参与制定应急预案，实现联动互助。

组织应保持和保留关于响应潜在紧急情况的过程和计划的文件化信息。

9 绩效评价

9.1 监视、测量、分析、评价

9.1.1 总则

组织应建立、实施和保持用于监视、测量、分析评价绩效的过程。

组织应确定：

a) 需要监视和测量的内容，包括：

1) 满足法律法规要求和其他要求的程度；

2) 与所识别的风险、隐患相关的活动和运行；

3) 与应急准备和响应、事故事件处理相关的活动和运行；

4) 实现目标的进展情况；

5) 与组织活动过程及其他标准的融合程度。

b) 适用时，为确保结果有效所采用的监视、测量、分析和评价绩效的方法；

c) 组织评价其安全绩效所依据的准则；

d) 实施监视和测量的时机；

e) 分析、评价和沟通监视和测量的结果的时间。

组织应评价其安全管理绩效并确定安全管理体系的有效性。

组织应确保监视和测量设备在适用时得到校准或验证，并被适当使用和维护。

组织应保留适当的文件化信息：

——作为监视、测量、分析和评价绩效的结果的证据；

——记录有关测量设备的维护、校准或验证。

9.1.2 合规性评价

组织应建立、实施和保持用于对法律法规要求和其他要求(见6.1)的合规性进行评价的过程。

组织应：

a) 确定实施合规性评价的频次和方法；

b) 评价合规性，并在需要时采取措施(见10.2)；

c) 保持对其关于法律法规要求和其他要求的合规状况的认识和理解；

d) 保留合规性评价结果的文件化信息。

9.2 内部审核

9.2.1 总则

组织应按计划的时间间隔进行内部审核，以确定安全管理体系的下列信息：

a) 是否符合：

1) 组织自身对安全管理体系的要求；

2) 本文件的要求。

b) 是否得到有效的实施和保持。

9.2.2 内部审核程序

组织应策划、建立、实施、保持和持续改进一个或多个审核方案，包括频次、方法、职责、策划要求和报告，审核方案应该考虑到所关注过程的重要性和以往审核的结果。

审核宜与其他内部审核结合进行。

组织应：

a) 规定每次审核的准则和范围；

b) 确保审核人员的选择与审核过程客观公正；

c) 确保将审核结果上报相关管理者；

d) 及时采取适当的纠正措施；

e) 保留文件化信息，作为审核方案和审核结果的证据。

注1:审核方案，包括任何日程安排，应以组织活动的风险评估和以往的审核结果为基础。

注2:审核程序应涵盖范围、频次、方法和能力，以及执行审核和报告结果的职责和要求。

9.3 管理评审

9.3.1 总则

最高管理者应该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。

组织应基于分析和评价的结果(9.1)以及管理评审的输出，确定是否存在与业务或安全管理体系有关的需求或机遇，作为持续改进的一部分。

注：组织可以通过安全管理体系的过程(例如领导作用、策划、绩效评价等)以实现改进。

9.3.2 管理评审输入

策划和实施管理评审时应该考虑以下内容：

a) 以往管理评审所采取的措施及其状况；
b) 与安全管理体系相关的内外部因素的变化；
   1) 法律法规要求和其他要求；
   2) 风险和机遇；
   3) 相关方的需求和期望。
c) 安全方针和安全目标的实现程度；
d) 安全绩效的信息，包括以下方面的趋势：
   1) 事件、不符合、纠正措施状态和持续改进；
   2) 监视和测量的结果；
   3) 对法律法规要求和其他要求的合规性评价的结果；
   4) 审核结果；
   5) 相关方的协商和参与；
   6) 风险和机遇。
e) 资源的充分性；
f) 与相关方的沟通，包括投诉；
g) 持续改进的机会。

9.3.3 管理评审输出

管理评审的输出应包括与持续改进机遇有关的决定和安全管理体系变更的任何需要。

组织应保留文件化信息，作为管理评审结果的证据。

10 改进

10.1 事件、不符合和纠正措施

组织应建立、实施和保持包括报告、调查和采取措施在内的过程，以确定和管理事件及不符合。当出现事件和不符合时，组织应：

a) 及时对事件和不符合做出的反应，并在适用时：
   1) 采取措施进行控制和纠正；
   2) 对结果进行处理。
b) 通过以下方式评估是否需要采取行动消除不符合项，避免其再次发生或者在其他场合发生：
   1) 调查事件或评审不符合；
   2) 确定导致事件或不符合的原因；
   3) 确定类似事件是否曾经发生过，不符合是否存在，或它们是否可能会发生。
c) 在适当时，对现有的安全风险评价进行评审(见6.2.3)；
d) 按照安全风险管控(见8.1.2)和变更的策划(见6.4)，确定并实施任何所需的措施，包括纠正措施；
e) 在采取措施前，评价相关的安全风险；
f) 评审任何所采取措施的有效性，包括纠正措施；

g) 在必要时，变更安全管理体系。

组织应保留文件化信息作为证据，包括事件和不符合的性质、产生原因、以及所采取的措施和结果等。

组织应就此文件化信息与相关方进行沟通。

注1:当出现迫在眉睫的对人身生命或公共安全的威胁时，应立即采取措施，可不必对纠正措施进行实施前的评价。

注2:任何纠正措施应与所遇到的事件和不符合的风险的严重程度相适应。

10.2 持续改进

组织应积极寻求改进的机会，采取必要措施，对安全管理体系的适宜性、充分性和有效性进行持续改进，通过：

a) 完善组织安全管理体系，提升安全绩效；
b) 促进支持安全文化；
c) 促进相关方参与安全管理体系持续改进措施的实施；
d) 就有关持续改进的结果与相关方进行沟通；
e) 加强安全管理体系与其他管理体系的融合；
f) 加强安全能力建设(见7)；
g) 保持和保留文件化信息作为持续改进的证据。

参 考 文 献

[1] GB/T 19000—2016 质量管理体系基础和术语

[2] GB/T 45001—2020 职业健康安全管理体系要求及使用指南

[3] GB/T 24001-2016 环境管理体系要求及使用指南

[4] GB/T 33000-2016 企业安全生产标准化基本规范

[5] ISO 28000:2022 Security and resilience — Security management systems — Requirements

[6] IS031000-2018 Risk management — Guidelines