安全与韧性 安全管理体系 要求
解读和应用指导材料

目次

ISO 28000-2022 《安全与韧性—安全管理体系要求》

引言

大多数组织正经历着安全环境中越来越多的不确定性和波动性。因此，他们面临着影响其目标的安全问题，他们希望在其管理体系内系统地解决这些问题。正式的安全管理方法可以直接增进组织的业务能力和可信度。

本标准规定了安全管理体系要求，包括对供应链安全保证至关重要的方面。它要求组织：

——评估其运营的安全环境，包括其供应链（包括依赖关系和相互依存关系）；

——确定是否有足够的安全措施来有效管理与安全相关的风险；

——管理组织对法律法规和自愿义务的遵守情况；

——协调安全过程和控制，包括供应链的相关上游和下游过程和控制，以满足组织的目标。

安全管理与业务管理的许多方面相关联。它们包括组织控制或影响的所有活动（包括但不限于对供应链产生影响的活动）。应考虑对组织安全管理有影响的所有活动、职能和业务，包括（但不限于）其供应链。

关于供应链，必须考虑到供应链本质上是动态的。因此，一些管理多个供应链的组织可能希望其供方满足相关的安全标准，作为纳入该供应链的条件，以满足安全管理的要求。

本标准将策划—实施—检查—处置（PDCA）模式应用于组织策划、建立、实施、运行、监视、评审、保持和持续改进安全管理体系的有效性，见表1和图1。

表1：PDCA模型的解释

策划（建立）	建立与改进安全相关的安全方针、目标、指标、控制措施、过程和程序，以提供符合组织总方针和目标的结果。
实施（执行和运行）	执行和运行安全方针、控制措施、过程和程序。
检查（监视和评审）	根据安全方针和目标监视和评审绩效，向管理层报告结果以供评审，并确定和授权补救和改进措施。
处置（保持和改进）	根据管理评审的结果，通过采取纠正措施，保持和改进安全管理体系，并重新评价安全管理体系的范围和安全方针和目标。

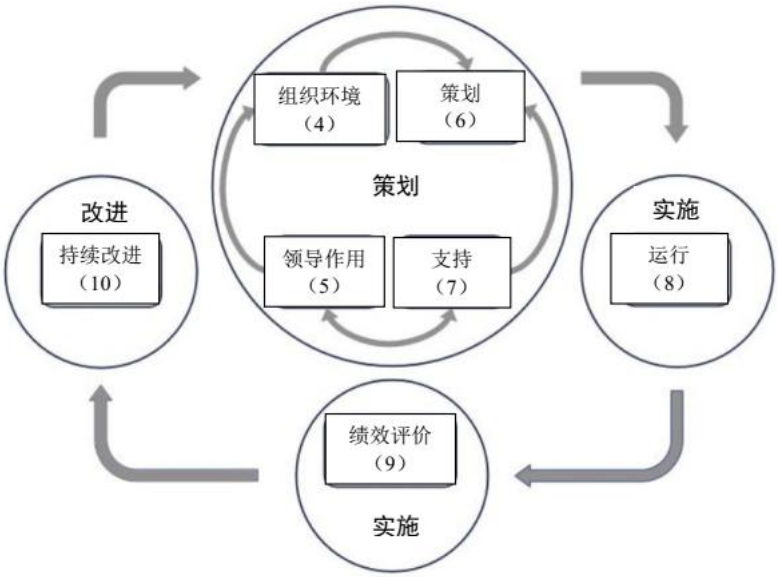


图1：应用于安全管理体系的PDCA模式

图1：应用于安全管理体系的PDCA模式

这确保了与其他管理体系标准的一致性，如ISO 9001、ISO 14001、ISO 22301、ISO/IEC 27001、ISO 45001等，从而支持与相关管理体系的一致和整合实施和运行。

对于有此愿望的组织，可以通过外部或内部审核程序来验证安全管理体系与本标准的一致性。

引言

(1)安全管理体系的引入背景与重要性；

(a)**安全环境的不确定性与波动性：**当前，大多数组织都面临着安全环境中日益增加的不确定性和波动性。这种不确定性可能来自外部环境的变化、新技术的引入、竞争格局的变动等，而波动性则可能表现为安全风险的频繁发生和影响的不可预测性；

(b)**安全问题对组织目标的影响：**由于安全环境的不确定性和波动性，组织面临着众多影响其目标实现的安全问题。这些问题可能涉及到人员安全、信息安全、供应链安全等方面，直接关系到组织的日常运营和长期发展；

(c)**系统解决安全问题的需求：**面对这些安全问题，组织需要一种系统化的方法来解决。这意味着组织需要在其管理体系内建立一套完整的安全管理体系，通过明确的安全方针、目标、控制措施、过程和程序来系统地管理和控制安全风险；

(d)**正式安全管理方法的业务价值：**引入正式的安全管理方法对组织具有显著的业务价值。首先，它可以帮助组织有效地识别、评估和管理安全风险，降低安全事故发生的概率和影响。其次，正式的安全管理方法可以提高组织的业务能力和可信度，增强客户、合作伙伴和利益相关方对组织的信任和满意度。最后，通过持续改进和优化安全管理体系，组织还可以不断提升其安全管理水平，以适应不断变化的安全环境。

(2)安全管理体系对供应链安全的全面规范；

(a)**安全管理体系对供应链安全的重视：**ISO 28000 标准特别强调了安全管理体系在保障供应链安全方面的重要性。它认为供应链的安全是组织整体安全不可或缺的一部分，需要特别关注和管理；

(b)**全面评估运营的安全环境：**标准要求组织评估其运营的安全环境，这包括对其供应链的全面审视。组织需要了解供应链中的依赖关系和相互依存关系，以便识别潜在的安全风险；

(c)**确保足够的安全措施：**在评估了安全环境后，组织需要确定是否有足够的安全措施来有效管理这些与安全相关的风险。这可能涉及制定针对性的安全策略、程序、过程和应对方法；

(d)**合规性管理：**除了风险管理外，标准还要求组织管理其对法律法规和自愿义务的遵守情况。这意味着组织需要确保自身的运营活动符合相关的法律法规要求，并遵守行业内的自愿标准或承诺；

(e)**协调安全过程和控制：**为了实现组织的目标，标准强调了在安全管理体系中协调供应链相关上游和下游过程和控制的重要性。这包括确保供应链的各个环节都遵循统一的安全标准，以实现整个供应链的安全性和韧性。

(3)动态供应链的安全管理要求；

(a)**供应链的动态特性：**供应链具有动态变化的特性，这表现在供应商、客户需求、运输方式等多个方面都可能随着时间的推移而发生变化。这种动态性增加了组织在供应链安全管理中面临的挑战；

(b)**多供应链管理的复杂性：**一些组织可能同时管理多个供应链，每个供应链都有其独特的结构和安全需求。因此，组织需要针对每个供应链制定和执行特定的安全管理策略；

(c)**供方安全标准的重要性：**在动态供应链中，供方的表现直接影响到整个供应链的安全状况。为了保障供应链的安全，组织可能会要求其供方满足特定的安全标准，以确保其产品和服务符合安全要求；

(d)**安全标准作为供应链准入条件：**作为纳入供应链的条件之一，组织可能会要求潜在供方达到特定的安全标准。这有助于组织筛选出符合安全要求的供方，从源头上降低供应链中的安全风险；

(4)**安全管理体系与业务管理的关联性；安全管理与业务管理的全面关联：**安全管理体系并非孤立存在，而是与组织的业务管理紧密相关。这体现在安全管理体系需要涵盖组织控制或影响的所有活动，这些活动包括但不限于对供应链产生影响的业务环节；

(a)**全面考虑安全管理的影响因素：**在制定和实施安全管理体系时，组织需要考虑所有可能对安全管理产生影响的活动、职能和业务。这种全面的考虑不仅有助于组织识别潜在的安全风险，还能确保安全管理体系的有效性和针对性；

(b)**供应链的特别关注：**供应链作为组织运营的重要组成部分，其安全状况直接影响到组织的整体安全。因此，标准特别强调了对供应链安全的关注，要求组织在评估和管理安全风险时充分考虑供应链的依赖关系和相互依存性；

(c)**业务活动与安全管理的一体化：**通过将安全管理体系与业务管理紧密融合，组织可以在日常运营中实现安全风险的预防和控制。这不仅可以提高组织的运营效率，还能增强组织的竞争力和市场信誉。

(5)PDCA 模式在安全管理体系中的应用；

(a)PDCA 模式的引入：

——ISO 28000 标准将策划－实施－检查－处置（PDCA）模式应用于安全管理体系的建立、实施、监视、

评审、保持和持续改进过程中。这一模式有助于组织系统地管理其安全活动，确保安全管理体系的有效性和适应性。

(b)PDCA 模式的具体应用；

表1：PDCA模型的解释

策划（建立）	建立与改进安全相关的安全方针、目标、指标、控制措施、过程和程序，以提供符合组织总方针和目标的结果。
实施（执行和运行）	执行和运行安全方针、控制措施、过程和程序。
检查（监视和评审）	根据安全方针和目标监视和评审绩效，向管理层报告结果以供评审，并确定和授权补救和改进措施。
处置（保持和改进）	根据管理评审的结果，通过采取纠正措施，保持和改进安全管理体系，并重新评价安全管理体系的范围和安全方针和目标。

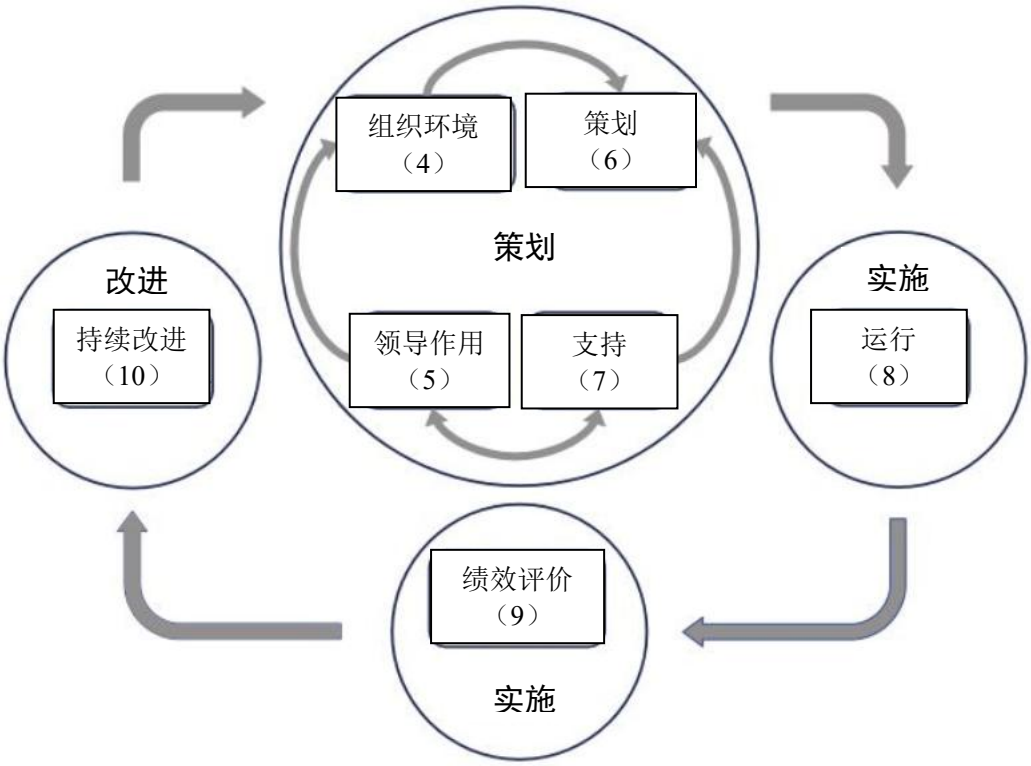


图1：应用于安全管理体系的PDCA模式

(c)**与其他管理体系标准的一致性：**通过应用 PDCA 模式，ISO 28000 标准确保了与其他管理体系标准（如 ISO 9001、ISO 14001、ISO 22301、ISO/IEC 27001、ISO 45001 等）的一致性。这种一致性使得组织可以更容易地将安全管理体系与其他管理体系进行整合，实现资源的共享和效率的提升；

(d)**支持管理体系的整合实施和运行：**PDCA 模式的应用支持了安全管理体系与其他管理体系的一致和整

合实施和运行。组织可以在一个统一的框架内同时管理多个管理体系，减少重复工作，提高整体管理效率。

(6)**对于有此愿望的组织，可以通过外部或内部审核程序来验证安全管理体系与 ISO 28000 的一致性**。

(a)**审核的必要性：**对于希望确保其安全管理体系与 ISO 28000 标准一致性的组织来说，进行外部或内部审核是必要的步骤。这些审核程序有助于组织验证其安全管理体系是否符合标准要求，从而确保其有效性和适应性。

(b)外部与内部审核；

——外部审核通常由独立的第三方机构执行，旨在客观评估组织的安全管理体系是否符合 ISO 28000 标准。外部审核的结果通常具有更高的权威性和公信力，有助于提升组织的市场形象和信誉；

——内部审核则由组织自身执行，旨在自我评估和改进安全管理体系。内部审核有助于组织发现潜在的不足和问题，并及时采取措施进行纠正和改进，从而提高安全管理体系的持续改进能力。

(c)**审核程序和方法：**无论是外部还是内部审核，都需要遵循一定的程序和方法。这包括确定审核目标、范围、频次和方法，选择合格的审核员实施审核，收集和分析审核证据，编制审核报告，并向相关管理者报告审核结果等步骤。审核程序和方法的具体细节应根据组织的实际情况和需要来确定。

(d)**审核结果的利用：**审核结果对于组织来说具有重要的利用价值。通过审核，组织可以了解其安全管理体系的当前状况和存在的问题，并据此制定改进计划和措施。同时，审核结果还可以作为组织持续改进和寻求更高管理绩效的重要依据和参考。

ISO 28000-2022 《安全与韧性—安全管理体系—要求》解读和应用指导材料

ISO 28000-2022 《安全与韧性—安全管理体系要求》

1 范围

本标准规定了安全管理体系要求，包括与供应链相关的方面。

本标准适用于所有类型和规模的组织（如商业企业、政府或其他公共机构和非营利组织），旨在建立、实施、保持和改进安全管理体系。它提供了一个整体的、共同的方法，并不针对具体行业或部门。

本标准可以在组织整个生命周期中使用，并可应用于任何层级的内部或外部活动。

1 范围

(1)标准的普适性：

——ISO 28000 标准规定了安全管理体系的要求，并明确指出其适用于所有类型和规模的组织，无论其是商业企业、政府机构、公共机构还是非营利组织；

——这种普适性确保了无论组织的具体性质如何，都可以采用本标准来建立、实施、保持和改进其安全管理体系。

(2)**跨行业的应用：**标准提供了一个整体的、共同的方法，并不针对特定行业或部门。这意味着无论组织所在行业如何，都可以采用统一的标准来指导其安全管理体系的建设和运行；

(3)**全生命周期的适用性：**本标准不仅可以在组织的某一特定阶段使用，而且可以在整个组织生命周期内持续应用。这包括组织的初创阶段、发展阶段、成熟阶段以及任何可能的转型或重组阶段；

(4)**内部与外部活动的覆盖：**标准的应用范围不仅限于组织的内部活动，还可以扩展到组织的外部活动。这意味着无论是组织内部的生产、运营、管理等活动，还是与外部合作伙伴、客户、供应商等进行的业务往来，都可以纳入安全管理体系的范畴。

(5)**对供应链的关注：**特别值得注意的是，标准特别强调了与供应链相关的方面。这要求组织不仅要关注自身的安全管理，还要关注其供应链中各个环节的安全管理，确保整个供应链的安全性和韧性。

(6)**整体的、共同的方法：**ISO 28000 标准提倡的是一个整体的、共同的安全管理方法。这意味着组织需要采取一种综合性的、协调一致的方式来管理其安全风险，而不是孤立地、片段化地处理问题。

ISO 28000-2022 《安全与韧性—安全管理体系要求》

2 规范性引用文件

下列文件对于本标准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标准。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本标准。

ISO 22300 安全与韧性——术语

2 规范性引用文件

下列文件对于本标准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标准。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本标准。

ISO 22300 安全与韧性——术语

ISO 28000-2022 《安全与韧性—安全管理体系要求》

3 术语和定义

ISO 22300 界定的以及下列术语和定义适用于本标准。

ISO和IEC在以下地址维护用于标准化的术语数据库：

ISO在线浏览平台：https://www.iso.org/obr

IEC在线电工术语库：http://www.electropedia.org/

3.1

组织 organization

为实现目标，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（利益相关方） interested party; stakeholder

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。

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

最高管理者 top management

在最高层指挥和控制组织的一个人或一组人。

注1：在保留对安全管理体系）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。

3.4

管理体系　management　system

组织用于建立方针和目标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、岗位和职责、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。

3.5

安全管理体系 safety management system

用于建立和实现安全方针和目标的管理体系或管理体系的一部分。

3.6

方针　policy

由组织最高管理者正式表述的组织的意图和方向。

3.7

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。

3.8

风险 risk

不确定因素对目标的影响。

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 （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：本标准中风险指安全风险。

3.9

过程　process

利用输入实现预期结果的相互关联或相互作用的一组活动。

注：过程的“预期结果”称为输出，还是称为产品）或服务，随相关语境而定。

3.10

能力 competence

应用知识和技能实现预期结果的本领。

3.11

成文信息 documented information

组织需要控制并保持的信息及其载体。

注1：成文信息可以任何格式和载体存在，并可来自任何来源。

注2：成文信息可涉及：

—— 管理体系，包括相关过程；

—— 为组织运行而产生的信息 （一组文件）；

—— 实现结果的证据（记录）。

3.12

绩效 performance

可测量的结果。

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。

3.13

持续改进 continual improvement

提高绩效的循环活动。

注1：提高绩效涉及使用安全管理体系以实现与安全方针（3.11）和安全目标）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。

3.14

有效性 effectiveness

完成策划的活动并得到策划的结果的程度。

3.15

要求 requirement

明示的、通常隐含的或必须履行的需求或期望。

注1： “通常隐含”是指组织和相关方的惯例或一般做法，所考虑的需求或期望是不言而喻的。

注2： 规定要求是经明示的要求，如：在成文信息（3.8.6）中阐明。

3.16

符合 conformity

满足要求。

3.17

不符合 nonconformity

未满足要求 。

3.18

纠正措施 corrective action

为消除不合格的原因并防止再发生所采取的措施。

3.19

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ISO 19011。

3.20

测量 measurement

确定数值的过程。

3.21

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 术语和定义

以上术语和定义解读见 4 至 10 章各章节部分内容。

ISO 28000-2022 《安全与韧性—安全管理体系要求》

4 组织所处的环境

4.1 理解组织及其所处环境

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，包括其供应链的要求。

4 组织环境

4.1 理解组织及其所处环境

(1)**理解组织所处运营环境以建立有效安全管理体系：**组织在建立和实施安全管理体系时，应深入理解其所处运营环境，包括识别和分析那些与组织宗旨紧密相关且可能对实现安全管理体系预期结果产生影响的内部和外部因素。

(e)对组织“宗旨”的理解；

——**组织的根本目的：**组织宗旨应明确组织为何存在，即组织的基本目标和追求。它可能包括为客户提供优质产品、实现社会福祉、促进科技发展等；

——**核心价值：**组织宗旨反映组织的核心价值和信仰，这是组织文化和价值观的体现。它可能涉及诚信经营、客户至上、创新驱动等；

——**指导原则：**组织宗旨作为组织的指导原则，影响着组织的战略制定、业务运营和日常管理。它确保组织在追求经济效益的同时，不偏离其核心价值和使命；

——**长期愿景：**组织宗旨通常包括一个长期愿景，即组织在未来一段时间内期望达到的状态和目标。这个愿景为组织的发展提供了方向和目标。

(f)组织拟实现的安全管理体系预期结果，包括：

——**防止人员伤害、健康损害、财产损失和环境破坏：**这是安全管理体系最直接和核心的预期结果，确保组织在其运营过程中能够最大限度地避免对员工、客户、公众造成的人身伤害和健康损害；同时，还要避免财产损失，如设备、设施、原材料的损坏或丢失。保护环境，防止组织活动对环境的破坏和污染；

——**达到或维持一个稳定、可靠的安全环境：**组织期望通过实施安全管理体系，确保组织内部和外部环境的安全稳定，为组织的正常运营提供一个可靠的保障；

——**应对安全相关的风险：**安全管理体系应有效地识别、评估、应对和监控各种安全风险，确保组织在面对潜在的安全威胁时能够迅速做出反应，减少或避免损失；

——**履行合规义务（合规性）：**组织必须遵守相关的法律法规和行业标准，确保所有运营活动都符合合规要求。这也是安全管理体系预期结果的重要组成部分；

——**实现组织的安全目标：**组织的安全管理体系应该与组织整体战略和目标相一致，确保安全管理体系的实施能够促进组织目标的实现；

——**持续改进安全绩效：**安全管理体系是一个持续改进的过程，组织应该通过定期的内部审核、管理评审等方式，不断发现问题、总结经验教训，并采取措施加以改进，以持续提高安全绩效。

(g)**确定内部因素：**为利于理解内部环境，一般考虑与组织的属性、特征、价值观和文化等有关的因素；

内部因素指组织内部那些能够对其安全管理体系产生影响的条件、特性或变化，包括：

——**组织属性与特征：**组织应理解其自身的属性与特征，包括其类型、规模、结构、资源、运营方式等。这些属性与特征直接影响了组织建立、实施、保持和改进安全管理体系的方式和重点；

——**价值观：**组织的价值观是其文化、信仰和长期愿景的核心组成部分。安全管理体系的建立和实施应紧密贴合组织的价值观，确保在实现安全目标的同时，不偏离组织的核心价值和使命；

——**文化：**组织文化包括其日常运营中的行为模式、沟通方式、决策过程等。在建立安全管理体系时，组织应充分考虑其文化特点，确保安全管理活动能够与组织的日常运营有效融合，避免造成管理上的断层或冲突。

(h)**确定外部因素：**组织应关注外部环境，如来自国际、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等，这些外部变化可能对组织的安全管理带来挑战或机遇。

外部因素指组织外部环境中的那些能够影响其安全管理体系的条件、特性或变化，包括：

——**政治因素**：政治稳定性和政策导向对组织的安全管理有着重要影响。组织应密切关注国内外政治环境的变化，以及这些变化可能对组织运营和供应链安全带来的潜在影响；

——**法律法规因素**：组织必须遵守相关法律法规和标准，以确保其运营活动的合法性和合规性。组织应关注法律法规的变化，及时调整其安全管理体系，确保符合最新的法律要求；

——**文化和社会因素**：不同的文化和社会环境对组织的安全管理有不同的要求和期望。组织应了解其所处文化和社会环境的特点，以便在制定安全策略和程序时能够充分考虑相关方的需求和期望；

——**经济或金融因素**：经济或金融环境的变化可能影响组织的财务状况和供应链稳定性，从而对安全管理产生间接影响。组织应关注经济或金融市场的动态，以便在必要时调整其安全管理策略和计划。

——**技术因素**：技术的发展为安全管理提供了新的手段和工具，同时也带来了新的风险和挑战。组织应关注技术的最新发展，以便及时引进和应用新的安全技术和管理工具，提高安全管理水平。

——**市场竞争因素**：市场竞争的激烈程度可能影响组织的运营策略和市场定位，从而对安全管理产生影响。组织应关注市场竞争的动态，以便在制定安全管理策略和计划时能够充分考虑市场竞争的因素。

——**自然环境因素**：自然环境的变化如自然灾害、气候变化等可能对组织的运营和供应链带来直接影响。组织应关注自然环境的变化趋势，以便制定相应的风险管理策略和应急计划。

(2)确定供应链的要求；

(a)**供应链定义**：从原材料来源到通过运输途径将产品或者服务交付至终端用户的一系列资源和流程。

- **全流程性**：供应链覆盖了从原材料获取到最终用户交付的整个流程，包括原料采购、生产制造、物流配送、分销零售等多个环节；
- **多元参与性**：供应链中涉及多个实体，包括原材料供方、生产商、物流供方、分销商、零售商等，这些实体之间通过合同、协议等方式进行合作，共同完成供应链中的各个环节；
- **资源整合性**：供应链不仅仅是产品或服务的流动，更涉及了人力、物力、财力等多种资源的整合和配置。这些资源在供应链中的合理分配和高效利用，是确保供应链顺畅运行的关键。

(b)**供应链要求整合。**组织应考虑其供应链的安全要求，包括：

——供方的安全标准与合规性；

- 供方必须遵守所有相关的安全法规和行业标准；
- 供方应有完善的安全管理制度和记录，确保产品或服务在生产、运输和存储过程中的安全性。

——供应链的透明度和可追溯性；

- 供应链应提供足够的透明度，以便组织能够追踪和验证产品或服务的来源和流向；
- 在出现问题时，应能迅速识别并隔离风险，确保整个供应链的安全不受影响。

——供应链伙伴的安全能力和信誉；

- 供应链中的合作伙伴应具备良好的安全实践记录和信誉；
- 合作伙伴应有能力保障其提供的产品或服务的安全性，包括质量控制、安全存储和运输等。

——供应链中的信息安全；

- 供应链应确保信息的保密性、完整性和可用性，防止数据泄露或被篡改；
- 应有有效的信息安全措施，如加密技术、访问控制和数据备份等。

——供应链的韧性和连续性；

- 供应链应能在面临突发事件或危机时保持运作，确保关键产品或服务的持续供应；
- 应有应对供应链中断的预案和恢复计划。

——环境、社会和治理（ESG）标准。

- 供应链应遵守环境、社会和治理标准，确保可持续性和负责任的采购；
- 这包括环境保护、劳工权益、反腐败等方面的要求。

(3)全面分析与应对组织所处运营环境。

内部和外部因素可能是正面的，为组织的安全管理体系带来新的机遇或优势。它们也可能是负面的，给组织的安全管理带来挑战或风险。组织在建立和实施安全管理体系时，应全面分析这些内部和外部因素，明确它们对安全管理体系的具体影响，并据此制定相应的策略和措施。对于正面因素，组织应积极把握和利用；对于负面因素，则需要采取有效的应对措施来减少其可能带来的不利影响。

4.2 理解相关方的需求和期望

4.2.1 总则

组织应确定：

——与安全管理体系有关的相关方；

——这些有关的相关方的要求；

——这些需求中哪些将通过安全管理体系来解决。

4.2 理解相关方的需求和期望

4.2.1 总则

(7)相关方（利益相关方）定义：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。

——影响决策或活动：包括那些有能力或权力影响组织决策或活动的个人或组织，如监管部门、非政府组织、投资方等。他们的意见、政策或要求可能对组织的安全决策和活动产生直接影响；

——受决策或活动所影响：指那些直接受到组织决策或活动影响的个体或团体，如工作人员、顾客、供方等。组织的安全决策和活动直接关系到这些人的安全和健康；

——自认为受决策或活动影响：此类相关方可能并不直接受到组织决策或活动的影响，但他们主观上认为自己受到了影响，如游客、居民、社区、邻近组织等。

(8)组织应确定与安全管理体系有关的相关方；

——组织应应明确哪些个人或组织与其安全管理体系相关；

——相关方可能包括顾客、 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。

(9)组织应确定与安全管理体系有关的相关方的要求；

——组织应建立与相关方的沟通机制，通过问卷调查、访谈、会议等方式收集他们的需求和期望；

——组织在确定相关方的需求和期望时，还应考虑并遵守适用的法律法规要求；

——对于影响决策或活动的相关方，组织应关注其政策、标准和要求，确保合规性；

——对于受决策或活动影响的相关方，组织应关注其安全和健康需求，确保运营活动不对其造成负面影响；

——对于自认为受决策或活动影响的相关方，组织应通过沟通和协作，了解其关注点，并采取相应措施以减轻或消除其担忧。

(10)组织应确定这些安全管理体系有关的相关方的要求中哪些将通过安全管理体系来解决。

——在识别和理解相关方要求的基础上，组织应确定哪些要求将通过安全管理体系来解决，这可以通过设定明确的安全目标、制定相关的安全政策和程序来实现；

——组织在策划和建立安全管理体系时，需要充分考虑并应对已采纳的相关方的所有需求和期望，以确保安全管理体系的充分性和针对性。

相关方类别	相关方对组织的需求和期望示例
顾客	- 提供安全可靠的产品和服务 - 保证供应链的透明度和可追溯性
游客	- 提供安全的旅游环境和活动 - 制定有效的应急响应和撤离计划
居民	- 维护居住环境的安全和安宁 - 提高公共安全的保障水平
社区	- 确保社区设施的安全运营 - 采取措施减少对环境的不良影响
供方	- 应与其建立稳定、可靠的安全管理合作关系，确保供应链的安全性和可靠性 - 遵循合规性和伦理标准
监管部门	- 遵守相关的法律法规和行业标准 - 保障公共安全和健康
非政府组织	- 履行组织的社会和环境责任 - 关注并保护弱势群体的安全 - 与非政府组织合作，共同推进安全管理和环境保护工作
投资方	- 建立稳健的安全管理体系，确保财务稳定和业务连续性，降低投资风险

工作人员	- 提供安全和健康的工作环境 - 提供安全培训和防护设备，确保员工的健康和安全 - 提供持续的职业培训和发展机会 - 强调职业道德和规范的遵守

ISO 28000-2022 《安全与韧性—安全管理体系要求》

4.2 理解相关方的需求和期望

4.2.2 合规义务

组织应：

a) 实施和保持过程，以确定、获取和评估与其安全有关的适用合规义务；

b) 确保在实施和保持其安全管理体系时考虑到这些适用的合规义务；

c) 将这些信息形成文件并保持更新；

d) 适当时将此信息传达给相关方。

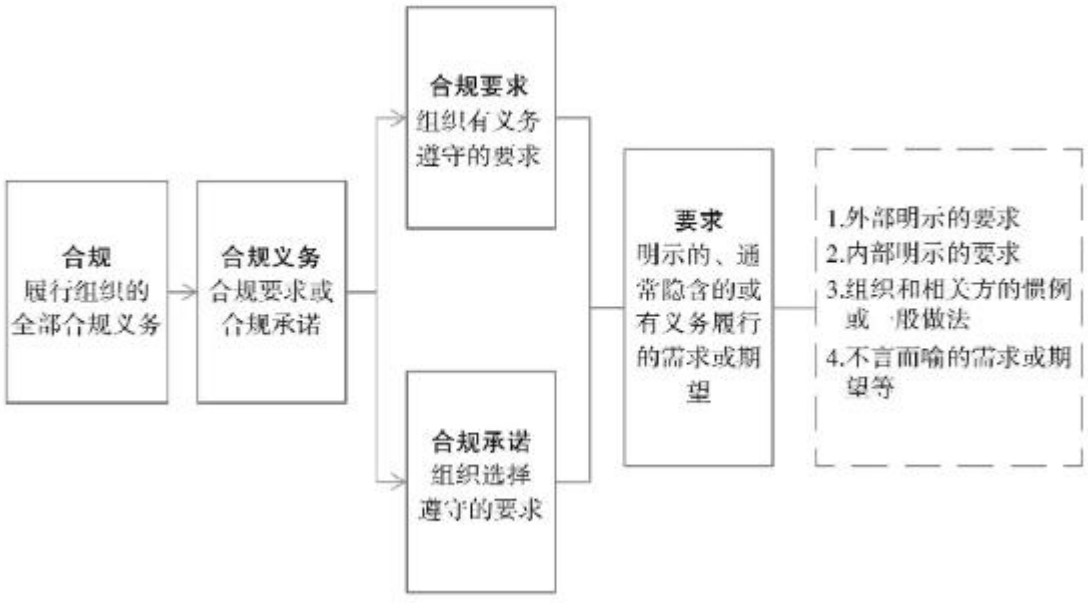
4.2.2 合规义务

(1)与合规义务有关的术语；

(a)“合规义务”的定义

组织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。

——**合规义务定义：**合规义务是指组织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。



合规与合规义务之间的关系图示

——**合规义务可能会给组织带来风险和机遇：**合规义务可能给组织带来风险，例如不遵守可能导致法律处罚或声誉损害；同时，合规也可能带来机遇，如通过合规实践提升组织形象，吸引和保留人才。

(a)**合规：**履行组织的全部合规义务。

——**合规：**组织应履行其全部合规义务，确保安全管理体系的建立、实施、运行和保持均符合相关合规义务；

——**全面履行：**组织应确保所有相关的合规义务都得到充分履行，不存在遗漏或违反情况；

(b)**不合规：**未履行合规义务。

——**未履行合规义务：**指组织在建立、实施、保持和持续改进其安全管理体系的过程中，未能满足或遵守合规义务；

——**不合规后果：**不合规可能导致组织面临法律责任、处罚，同时可能危害安全，影响组织的形象和声誉。

(2)组织应实施一个持续的过程来识别与其安全活动直接相关的所有合规义务；

(a)确定、获取和评估合规义务：

——这些合规义务可能包括法律、法规、行业标准、合同要求以及其他自愿遵守的准则。

——组织需要系统地收集这些信息，并对它们的适用性进行评估，确保对组织的安全管理活动有直接影响；

(b)确保在实施和保持其安全管理体系时考虑到这些适用的合规义务；

——在策划、建立、实施、运行、监视、评审、保持和持续改进安全管理体系时，组织应始终考虑这些合规义务；

- 组织的安全生产方针应体现对遵守法律法规的承诺；
- 法律法规是确定需要应对的风险和机遇的重要依据；
- 建立安全目标与策划如何实现其安全目标应考虑个满足法律法规要求；
- 培训与沟通及文件和文件管理不仅要包含安全生产法律法规信息、安全意识，培训而且还应满足其有关要求；
- 运行是组织对规范组织作业活动、控制风险的重要途径，也是满足安全生产法律法规的重要途径；
- 合规性评价与纠正措施是评价组织安全管理活动对法律法规的符合情况，并对各种不符合采取纠正措施的重要手段；
- 管理评审要依据安全生产法律法规等的发展变化情况，对安全管理体系进行修订和调整；

——安全管理体系的设计和运行应确保所有活动和过程都符合适用的合规义务。

(c)将这些信息形成文件并保持更新；

——组织应将确定的合规义务形成文件，这些文件应明确列出所有适用的法律、法规、标准和其他要求；

——随着外部环境和内部条件的变化，组织应定期更新这些文件，确保合规义务的准确性和时效性。

(d)适当时传达给相关方。

——组织应根据需要将这些合规义务的信息传达给所有相关方；

——传达的方式和频率应根据相关方的需求和期望来确定，以确保他们充分理解组织在安全方面的合规承诺和实践。

ISO 28000-2022 《安全与韧性—安全管理体系要求》

4.2 理解相关方的需求和期望

4.2.3 原则

4.2.3.1 总则

组织中安全管理的目的是创造价值，特别是保护价值。

组织应采用图2中给出的原则，并在4.2.3.2至4.2.3.9条款中描述。

图2：原则

4.2.3.2 领导作用

各级领导应建立统一的目标和方向。他们应创造条件，使组织的战略、方针、过程和资源协调一致，以实现其目标。

4.2.3.3 基于现有最佳信息的结构化和全面性的程序方法

包括供应链在内的结构化和全面性的安全管理方法应有助于取得一致和可比较的结果，只有将活动作为相互关联的连贯系统进行运行的过程来管理时，才能更加有效和高效地得到结果。

4.2.3.4 定制化

安全管理体系应是定制的，并与组织的外部和内部环境和需求要适应。安全管理体系应与其目标有关。

4.2.3.5 包容的人员积极参与

组织应适当地、及时地让相关方参与进来。它应适当考虑他们的知识、观点和看法，以提高对安全管理的认识并促进知情的安全管理。组织应确保所有层级的人都得到尊重和参与。

4.2.3.6 整合方法

安全管理是所有组织活动的有机组成部分。它应与组织的所有其他管理系统相整合。

组织的风险管理（无论是正式的、非正式的还是直观的）都应被整合至安全管理体系中。

4.2.3.7 动态和持续改进

组织应持续关注通过学习和经验进行改进，以保持绩效水平，对变化做出反应，并随着组织的外部和内部环境的变化创造新的机会。

4.2.3.8 考虑人和文化因素

人的行为和文化对安全管理各方面都有很大影响，应在每个层次和阶段都考虑到。决策应基于对数据和信息的分析和评价，以确保决策更加客观，对决策有信心，更有可能产生预期的结果。应考虑每个人的看法。

4.2.3.9 关系管理

为了持续的成功，组织应管理好与所有相关方的关系，因为他们可能会影响组织的绩效。

4.2.3 原则

4.2.3.1 总则

(1)**安全管理的目的：**组织实施安全管理的根本目的在于创造价值，尤其是保护组织的价值。安全管理不仅仅是遵守法规或避免风险，更是作为组织实现其目标、增强竞争力和确保长期生存的一种战略手段；

(2)**采用图中给出的原则：**图 2 中列出的原则为组织提供了一个框架，指导其在构建、实施和运行安全管理体系时应考虑的关键因素。这些原则帮助组织实现安全管理目的，并确保其安全管理体系与组织的整体战略和目标保持一致；

(3)**原则在具体条款中的描述：**4.2.3.2 至 4.2.3.9 条款详细描述了图 2 中列出的每一项原则（包括领导作用、基于现有最佳信息的结构化和全面性的程序方法、定制化、包容的人员积极参与、整合方法、动态和持续改进、考虑人和文化因素、关系管理），并提供了具体的实施指导。这些条款涵盖了从领导作用到持续改进等多个方面，为组织提供了全面的安全管理实践指南。

图2：原则

4.2.3.2 领导作用

各级领导应建立统一的目标和方向。他们应创造条件，使组织的战略、方针、过程和资源协调一致，以实现其目标。

(1)**建立统一的目标和方向：建立统一的目标和方向：**在安全管理体系的构建和实施过程中，各级领导应确立清晰、统一的安全管理目标和方向。这不仅为组织的安全管理工作提供了明确的指导，也确保了组织上下对安全管理目标的高度共识；

(2)**协调战略、方针、过程和资源：**各级领导应确保组织的战略、安全管理方针、管理过程以及所需资源之间的协调一致。通过合理规划和资源配置，使安全管理活动能够紧密结合组织的整体战略，形成有效的合力；

(3)**创造有利条件：**为了实现安全管理目标，各级领导应积极创造条件，包括提供必要的资源支持、营造良好的安全文化氛围、强化员工的安全意识等，以促进员工对安全管理的认知和参与；

(4)**实现组织目标：**通过各级领导的引导和协调，组织的安全管理体系将更加高效和有针对性地实现其安全管理目标。

4.2.3.3 基于现有最佳信息的结构化和全面性的程序方法

包括供应链在内的结构化和全面性的安全管理方法应有助于取得一致和可比较的结果，只有将活动作为相互关联的连贯系统进行运行的过程来管理时，才能更加有效和高效地得到结果。

(1)**结构化和全面性的方法：**安全管理体系强调采用结构化和全面性的方法来管理组织的安全。这种方法要求从整体上考虑组织的各项活动，包括供应链在内，以确保所有安全管理活动的一致性和可比较性；

(2)**强调供应链安全：**安全管理不仅关注组织内部的活动，还特别强调了供应链的安全管理。领导层应认识到供应链对组织整体安全的重要性，并采取有效措施确保供应链中的每个环节都符合安全管理要求。

(3)

(4)**相互关联的连贯系统：**为了实现高效和一致的安全管理结果，组织需要将各项安全管理活动视为一个相互关联的连贯系统。这意味着各项活动之间应存在清晰的逻辑关系和相互依赖，以便更有效地识别、评估和管理风险；

(5)**提升效率和效果：**通过实施结构化和全面性的安全管理方法，组织能够更加高效和有针对性地识别和管理风险，从而确保安全管理活动的有效性和效率。领导层应通过持续监督和评估，确保这种方法得到有效实施。

4.2.3.4 定制化

安全管理体系应是定制的，并与组织的外部和内部环境和需求相适应。安全管理体系应与其目标有关。

(1)**定制化的必要性：**安全管理体系的设计和实施应充分考虑组织的外部和内部环境，以及组织特有的需求。定制化的安全管理体系能够更好地适应组织的实际情况，确保安全管理的有效性和针对性；

(2)**外部环境的考虑：**组织所处的外部环境对安全管理体系的设计具有重要影响。定制化安全管理体系需要充分考虑这些外部因素，确保管理体系的合规性和适应性；

(3)**内部环境的评估：**定制化安全管理体系需要对组织的内部环境进行全面评估，确保管理体系与组织的实际情况相匹配；

(4)**与目标的关联：**安全管理体系的设计和实施应与组织的目标紧密关联。通过明确组织的安全管理目标，可以确定安全管理体系的关键要素和优先级，确保管理体系的有效性和针对性。

(5)**适应性与灵活性：**定制化安全管理体系应具备一定的适应性和灵活性。随着组织内外部环境的变化，管理体系应能够及时调整和完善，以应对新的安全挑战和风险。

4.2.3.5 包容的人员积极参与

组织应适当地、及时地让相关方参与进来。它应适当考虑他们的知识、观点和看法，以提高对安全管理的认识并促进知情的安全管理。组织应确保所有层级的人都得到尊重和参与。

(1)**相关方的广泛参与：**组织在实施安全管理体系时，应广泛邀请并鼓励相关方参与进来，他们的参与能够为安全管理体系提供多视角、多维度的信息和建议；

(2)**尊重并考虑相关方的知识、观点和看法：**组织在吸引相关方参与的同时，应尊重他们的知识和经验，充分考虑他们的观点和看法；

(3)**提升对安全管理的认识：**通过相关方的参与，组织能够加强内部员工和外部合作伙伴对安全管理重要性的认识，提高他们的安全意识；

(4)**促进知情的安全管理：**相关方的参与使得安全管理更加透明和知情。组织能够及时获取相关方的反馈和建议，针对实际问题进行调整和改进，提高安全管理体系的针对性和有效性；

(5)**确保所有层级的人员参与：**安全管理不仅仅是高层管理者的责任，更是全体员工的共同任务。组织应确保从高层管理者到基层员工都能参与到安全管理体系中来，形成一个全员参与、共同负责的安全管理格局；

(6)**创造尊重和参与的文化：**组织应营造一种尊重和参与的文化氛围，鼓励员工积极提出安全管理方面的建议和意见。同时，组织应给予员工必要的培训和支持，提高他们的安全管理能力和参与度。

4.2.3.6 整合方法

安全管理是所有组织活动的有机组成部分。它应与组织的所有其他管理系统相整合。

组织的风险管理（无论是正式的、非正式的还是直观的）都应被整合至安全管理体系中。

(1)**安全管理作为组织活动的有机组成部分：**安全管理体系并非孤立存在，而是组织日常运营活动不可分割的一部分。它应被视作组织活动的重要支柱，与其他业务活动和管理过程相互依存、相互促进；

(2)**与其他管理系统的整合：**安全管理体系应与组织的所有其他管理系统（如质量管理体系、环境管理体系、职业健康与安全管理体系等）相整合。通过整合，可以确保安全管理的要求和措施贯穿于组织管理的各个层面和环节，实现资源共享、信息互通，提高管理效率；

(3)**风险管理的全面整合：**组织的风险管理活动，无论是正式的、非正式的还是直观的，都应被整合至安全管理体系中。这意味着组织应建立一套全面的风险管理框架，将各类风险纳入统一的管理体系进行识别、评估、监控和应对，以确保组织能够全面、系统地识别和管理安全风险；

(4)**实现管理的一致性和协调性：**通过整合方法的应用，组织可以实现安全管理与其他管理体系的协调一致。这有助于避免管理重叠和冲突，提高管理效能。同时，整合方法还有助于组织在应对复杂多变的安全挑战时，能够迅速调动资源、协调各方力量，形成合力，共同应对风险。

4.2.3.7 动态和持续改进

组织应持续关注通过学习和经验进行改进，以保持绩效水平，对变化做出反应，并随着组织的外部和内部环境的变化创造新的机会。

(1)**持续学习与经验积累：**组织应不断从日常运营中学习，总结经验教训，并将这些学习和经验应用于安全管理体系的改进之中。这种持续的学习和经验积累是安全管理体系不断进化的基础；

(2)**保持绩效水平：**通过持续的学习和改进，组织应确保安全管理体系的绩效水平得以保持，甚至在面对日益复杂多变的安全挑战时也能保持高效运行；

(3)**对变化的快速响应：**组织应能够迅速识别外部环境（如法律法规、市场动态、技术进步等）和内部环境（如组织结构调整、业务流程变更、人员流动等）的变化，并及时调整安全管理体系以应对这些变化，确保组织的稳健运营。

(4)**创造新的机会：**通过持续改进，组织不仅能够应对当前的挑战，还能够发现并利用新的机会。这些机会可能来自于新的技术、新的市场或新的业务模式，它们能够为组织带来竞争优势和增长动力。

4.2.3.8 考虑人和文化因素

人的行为和文化对安全管理各方面都有很大影响，应在每个层次和阶段都考虑到。决策应基于对数据和信息的分析和评价，以确保决策更加客观，对决策有信心，更有可能产生预期的结果。应考虑每个人的看法。

(1)**人与文化的核心影响：**在安全管理体系的构建和实施过程中，人和文化因素占据着核心地位。人的行为、态度和价值观，以及组织的文化背景和氛围，都会直接或间接地影响安全管理的效果；

(2)**行为与文化对安全管理的影响：**员工的行为习惯、安全意识和职业素养，直接关系到安全管理措施的执行情况和安全管理目标的实现。同时，组织的文化氛围和核心价值观也会影响员工对安全管理的态度和行为；

(3)**在每个层次和阶段考虑：**在安全管理体系的不同层次和阶段，都需要充分考虑人和文化因素的影响。无论是顶层设计的制定，还是基层操作的执行，都需要以人为本，以文化为先导，确保安全管理措施的有效性和可行性；

(4)**基于数据的决策：**在做出安全管理决策时，应基于对数据和信息的深入分析和科学评价。通过收集和分析员工行为数据、安全绩效数据等，可以更客观地了解安全管理现状和问题，为决策提供有力支持；

(5)**增强决策客观性和信心：**考虑人和文化因素可以使得安全管理决策更加客观和具有信心。通过了解员工的需求和期望，考虑文化的差异和特点，可以制定出更符合实际、更易于执行的安全管理措施，从而增强决策的有效性和可行性；

(6)**关注每个人的看法：**在安全管理过程中，应充分尊重每个人的看法和意见。通过建立开放的沟通机制和参与平台，鼓励员工积极参与安全管理决策和执行过程，可以提高员工的归属感和责任感，促进安全管理措施的有效实施。

4.2.3.9 关系管理

为了持续的成功，组织应管理好与所有相关方的关系，因为他们可能会影响组织的绩效。

(1)**关系管理的重要性：**在安全管理体系中，关系管理扮演着至关重要的角色。组织需要识别并管理好与所有相关方的关系，因为这些关系可能直接影响到组织的绩效；

(2)**管理关系的策略和方法：**组织应制定具体的关系管理策略和方法，包括定期沟通、问题解决机制、信息共享等，以确保与相关方的关系得到良好的维护和发展；

(3)**关系管理对组织绩效的影响：**良好的关系管理有助于增强组织内部的凝聚力和外部的影响力，从而提升组织的整体绩效。

ISO 28000-2022 《安全与韧性—安全管理体系要求》

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：

——4.1中提及的各种外部和内部因素；

——4.2中提及的要求。

组织应将范围形成成文信息。

如果组织选择外部提供任何影响其安全管理体系符合性的过程时，组织应确保这些过程受控。此类外部提供过程的必要控制和责任应在安全管理体系中加以确定。

4.3 确定安全管理体系的范围

(1)组织应确定安全管理体系的边界和适用性，以确定其范围；

(a)**确定范围的重要性：**在建立和实施安全管理体系之前，组织应先明确其范围。范围界定安全管理体系的边界和适用性，确保安全管理体系能够覆盖所有重要活动和过程，同时也避免不必要的复杂性和资源浪费；

(b)**边界的确定：**组织应识别并确定安全管理体系的边界，这通常包括哪些活动、过程、部门或设施将纳入管理体系中。边界的确定应基于组织的运营特点和安全管理需求，确保管理体系的全面性和针对性。

(c)**适用性的评估：**在确定范围时，组织应评估管理体系的适用性。这涉及分析组织的内外部环境、业务需求、法律法规要求等，确保管理体系的设计和实施能够满足组织当前和未来的安全管理需求。

(2)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；

——**外部因素的具体考虑：**外部因素通常影响组织的运营环境，对安全管理体系的范围设定具有直接影响。例如，法律法规的要求可能决定了管理体系必须涵盖的特定领域或过程；供应链状况可能影响对供方管理的重视程度；

——**内部因素的具体考虑：**内部因素反映组织的实际情况和特定需求，同样对安全管理体系的范围设定具有重要影响。例如，组织的规模决定安全管理体系的复杂程度；业务流程的特点决定需要重点管理的关键活动和过程。

(b)**4.2 中提及的要求：**在确定范围时，应特别关注 4.2 中提及的相关方的需求和期望，这些需求和期望可能直接影响安全管理体系的设计和实施，确保管理体系能够切实满足内外部相关方的要求。

(3)组织应将范围形成成文信息；

(a)**范围应形成文件：**组织应将安全管理体系的范围明确并形成文件，以确保范围的明确性、一致性和可追溯性；

(b)**安全管理体系范围成文信息内容包括：**

——**范围的明确描述：**清晰地界定安全管理体系所覆盖的特定范围，包括但不限于组织内的部门、业务单元、地理位置，以及特定的活动、产品和服务；

——**边界的界定：**明确划定安全管理体系的边界，指明哪些部分包含在体系内，哪些部分被排除在外。边界的界定应基于组织的实际情况和安全管理需求；

——**适用性的说明：**解释为何选定特定的范围，考虑到的风险因素、合规义务、业务目标等。同时，应明确说明范围是否涵盖了组织的关键安全管理过程和活动。

(c)**成文信息的可获取性：**安全管理体系的范围作为成文信息，应具备高度的可获取性，以便组织内部和外部的相关方能够方便地获取相关信息。确保所有需要了解安全管理体系范围的人员都能及时、准确地获取到这些信息；

(d)**文件方式的灵活性：**组织在形成和保存安全管理体系范围文件时，可以选择适合其特定情况的灵活方式。这些方式包括但不限于文字描述、手册、网站内容、平面图、组织结构图或符合性声明等。同时，文件媒介也可以是多样化的，如电子文档、纸质文件、音频或视频记录，甚至可视化展示（如图表、流程图等），以满足不同利益相关方的信息获取需求。

(4)如果组织选择外部提供任何影响其安全管理体系符合性的过程时，组织应确保这些过程受控。此类外部提供过程的必要控制和责任应在安全管理体系中加以确定。

(a)**外部过程的影响性：**当组织选择外部提供某些可能影响其安全管理体系符合性的过程时，这些外部过程必须被纳入管理体系的考虑范围。这是因为外部过程的输出可能直接影响组织的安全管理绩效；

(b)**外部过程的控制要求：**组织应确保这些外部提供的过程受到适当的控制。控制手段包括但不限于对供方的评价和选择、合同条款的明确、过程输出的验证和监视等，以确保外部过程的质量和安全；

(c)**确定必要的控制和责任：**组织应在安全管理体系中明确这些外部提供过程的必要控制和责任。这包括识别哪些外部过程需要被控制，以及确定谁负责实施这些控制。明确的控制和责任分配有助于确保外部过程的有效管理和监督；

(d)**体系内的整合：**这些外部过程的管理应被整合到组织的安全管理体系中。组织应确保外部过程的管理流程、标准、目标和绩效指标与整体安全管理体系保持一致，以实现协同管理和持续改进。

ISO 28000-2022 《安全与韧性—安全管理体系要求》

4.4 安全管理体系

组织应按照本标准的要求建立、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。

4.4 安全管理体系

(1)组织应按照 ISO 28000 标准的要求建立、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；

(a)**建立安全管理体系：**组织应依据 ISO 28000 的标准，建立一套完整的安全管理体系。这一体系旨在实现组织的安全目标，确保组织的运营安全；

(b)**包含必要的过程及其相互作用：**安全管理体系应包括组织为实现其安全目标所需的所有关键过程，并明确这些过程之间的相互作用和依赖关系；

(c)**实施安全管理体系：**在体系建立完成后，组织应确保其在实际运营中得到有效实施。这包括按照体系规定的程序、方法和要求开展日常安全管理活动。

(d)**保持安全管理体系：**组织应持续监控和维护安全管理体系的有效性。通过定期评审、更新和改进，确保体系能够适应组织内部和外部环境的变化，保持其适应性和有效性。

(e)**持续改进安全管理体系：**组织应不断寻求改进机会，通过收集和分析数据、开展内部审核和管理评审等方式，识别体系中存在的问题和不足，制定改进措施并予以实施，从而实现安全管理体系的持续改进和优化。

(2)应用 PDCA 概念构建与改进安全管理体系。

(a)策划（Plan）；

——确定和评价风险与机遇：组织应全面识别和评价与安全管理体系相关的各种风险、机遇，以及可能对组织安全产生影响的其他潜在因素；

——制定目标和建立过程：基于风险评估的结果，组织应明确设定安全目标，这些目标应与组织的安全方针相一致。同时，组织应策划必要的过程和控制措施，以确保能够达成所设定的安全目标。

(b)**实施（Do）**：组织应严格按照策划的结果，实施所确定的安全管理过程和控制措施，确保这些措施得到有效执行；

(c)检查（Check）；

——**监视和测量**：组织应依据安全方针和目标，对其安全管理活动、过程和绩效进行持续的监视和测量，以确保各项活动符合策划要求；

——**报告结果**：**组**织应定期收集和分析监视与测量的数据，并将结果报告给相关管理层和利益相关者，以便及时发现问题和改进方向。

(d)改进（Act）。

——基于检查阶段的结果，组织应识别安全管理体系中的改进机会，采取针对性的纠正措施和预防措施，以实现体系的持续优化和提升；

——通过持续的改进活动，组织能够不断提升安全绩效，更好地应对不断变化的安全挑战。

ISO 28000-2022 《安全与韧性—安全管理体系要求》

5 领导作用

5.1 领导作用和承诺

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：

——确保制定安全方针和安全目标，并与组织战略方向相一致；

——确保识别和监视组织相关方的需求和期望，并及时采取适当措施来管理这些期望，以确保安全管理体系要求融入组织的业务过程；

——确保将安全管理体系要求融入组织的业务流程；

——确保安全管理体系所需的资源是可获得的；

——沟通有效的安全管理和符合安全管理体系要求的重要性；

——确保安全管理体系实现其预期结果；

——确保安全管理目标、指标和方案的可行性；

——确保组织的其他部分产生的任何安全方案都能补充安全管理体系；

——指导和支持人员为安全管理体系的有效性作出贡献；

——推动组织安全管理体系的持续改进；

——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。

5 领导作用

5.1 领导作用和承诺

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：

(1)确保制定安全方针和安全目标，并与组织战略方向相一致；

——**安全方针与安全目标的制定：**最高管理者负责确保安全方针和安全目标的制定。这些方针和目标不仅是组织安全管理的基础，更是引导组织实现安全目标的行动指南；

——**与战略方向的一致性：**安全方针和安全目标的制定必须与组织的战略方向相一致。这意味着安全管理工作要与组织的整体发展目标紧密衔接，确保安全管理成为实现组织战略目标的重要支撑；

——**战略层面的承诺：**最高管理者通过制定与战略方向一致的安全方针和安全目标，向组织内外展示了其对安全管理工作的重视和承诺。这种承诺不仅体现了最高管理者的领导力，也为组织的安全管理提供了战略层面的保障；

——**明确方向与期望：**明确的安全方针和安全目标有助于组织内部各级人员明确安全管理的方向和期望，促进全员参与安全管理，共同维护组织的安全和韧性。

(2)确保将安全管理体系要求融入组织的业务流程；

—— **业务流程的广义理解：**此处的“业务”一词在标准中被广义地理解为涉及组织存在目的的核心活动。无论是生产、销售、研发还是服务等核心职能，都应纳入安全管理体系的覆盖范围；

—— **安全管理体系要求与业务流程的融合：**最高管理者应确保安全管理体系的要求不是孤立存在的，而是深入组织的核心业务流程之中。在组织的日常运营、决策制定和资源配置等各个方面，都应充分考虑到安全管理体系的要求；

—— **提升组织安全管理水平：**通过将安全管理体系要求融入业务流程，组织能够在日常运营中及时发现和解决安全问题，提升安全管理水平。同时，这种融合还有助于优化资源配置，提高组织的整体运营效率。

(3)确保安全管理体系所需的资源是可获得的；

——**资源的核心作用：**资源是安全管理体系有效运行的基础和保障。没有充分的资源支持，任何安全管理体系都难以发挥其应有的作用；

——**资源的全面性：**资源不仅仅指物资、设备、资金等物质资源，还包括人力资源、技术资源、信息资源等非物质资源。所有这些资源都是安全管理体系有效运行不可或缺的要素；

——**确保资源的可获取性：**最高管理者应确保组织在任何时候都能够获得安全管理体系所需的各种资源。这包括资源规划、调配、采购、使用等环节的有效管理，确保资源供应的稳定性和连续性；

——**资源分配与优先级：**在资源有限的情况下，最高管理者应根据安全管理体系的优先级和关键性，合理分配资源。对于影响组织安全的关键因素，应给予更多的资源保障；

——资源管理的持续改进：最高管理者应持续关注资源管理的效果，并根据组织的发展和安全形势的变化，及时调整资源管理策略。通过不断优化资源配置，提高资源利用效率，为安全管理体系提供更有力的支持。

——沟通有效的安全管理和符合安全管理体系要求的重要性；

——**沟通的重要性：**在安全管理体系中，沟通是连接各个环节、确保体系有效运行的关键。最高管理者应认识到沟通的重要性，并积极推动组织内外的有效沟通；

——**安全管理重要性的沟通：**最高管理者应清晰地传达有效安全管理的重要性，强调其对组织目标实现的贡献；

——**符合安全管理体系要求重要性的沟通：**最高管理者应通过沟通强调符合安全管理体系要求的重要性。这包括遵循法律法规、标准、合同等合规义务，以及执行组织内部制定的安全政策和程序。通过强调体系要求，最高管理者可以促进组织内部对安全管理的重视和遵循。

——**安全意识的培养：**通过沟通安全管理的重要性和符合体系要求的重要性，最高管理者有助于培养员工的安全意识。员工将认识到自己在安全管理中的责任和角色，积极参与安全管理活动，共同维护组织的安全。

(4)确保安全管理体系实现其预期结果；

——预期结果的明确性：最高管理者应确保安全管理体系的预期结果是明确、具体且可衡量的。这些预期结果应与组织的安全方针和目标相一致，并反映组织在安全方面的整体战略和愿景；

——**安全管理体系预期结果包括：**

- **人员、健康与财产的全面保护：**防止人员伤害与健康损害，保护财产安全，防止环境破坏；
- 达到或维持一个稳定、可靠的安全环境：通过建立和维护一个全面、系统的安全管理体系，确保组织内部和外部环境的稳定与安全，为组织持续运营提供有力保障；
- **应对安全相关的风险：**建立全面的风险评估机制，有效识别、评估、应对和监控各种安全风险，确保组织在面对潜在的安全威胁时能够迅速做出反应，将风险降至最低；
- **履行合规义务（合规性）：**严格遵守所有适用的法律法规和行业标准，确保组织的所有运营活动都符合合规要求，避免因违规行为导致的法律风险和声誉损失；
- **实现与组织目标相一致的安全绩效：**将安全管理体系与组织整体战略和目标紧密结合，确保安全管理体系的实施能够助力组织实现其既定的业务目标和愿景。通过不断的安全绩效改进，提升组织的整体竞争力和市场地位；

——**结果的监测与评估：**为了确保安全管理体系达到预期的结果，最高管理者应建立有效的监测和评估机制。这包括对体系运行过程中的关键指标进行定期测量和评估，以及对体系的整体绩效进行定期审查和总结。通过这些监测和评估活动，最高管理者可以及时了解体系的运行状况，并采取必要的措施来确保预期结果的实现。

——**结果的责任归属：**最高管理者在安全管理体系中的领导作用和承诺还体现在对结果的责任感上。他们应确保组织对安全管理体系的预期结果负责，并在体系未能达到预期结果时承担相应的责任。

(5)确保安全管理目标、指标和方案的可行性；

——**目标的可行性：**最高管理者应确保组织设定的安全管理目标是实际可行的，既考虑到组织的资源限制，又符合组织长期发展战略和安全需求；

——**指标的量化与衡量：**安全管理指标应具有可衡量性，能够清晰地反映安全管理目标的达成情况，为持续改进提供数据支持；

——**方案的实施性：**制定的安全管理方案应具有可操作性，能够确保安全管理目标得到有效实施，降低安全风险；

——**基于实际情况的决策：**在设定安全管理目标、指标和方案时，最高管理者应充分考虑组织的实际情况，包括资源、技术、人员等方面的限制。只有基于实际情况的决策，才能确保所设定目标的可行性和可操作性。

——**评估与审核的必要性：**为了确保安全管理目标、指标和方案的可行性，最高管理者应组织相关部门对其进行定期的评估和审核。通过评估和审核，可以及时发现并解决存在的问题，确保目标的顺利实现。

(6)确保组织的其他部分产生的任何安全方案都能补充安全管理体系；

——**方案的补充性：**最高管理者承诺确保组织其他部门或职能领域（如研发、生产、销售等）产生的安全方案，能够补充和完善已建立的安全管理体系，增强其适应性和全面性；

——**避免遗漏、重复和冲突：**通过领导作用，确保安全管理体系覆盖组织的所有相关活动，且不同部门的安全方案之间不出现重复或冲突，而是相辅相成，形成合力，共同提升组织的安全管理效能；

——**全面性与协调性：**最高管理者在安全管理体系中的领导作用，体现在确保组织各个部分的安全方案都能有效地与安全管理体系相协调，形成一个整体性的安全保障体系。

(7)指导和支持人员为安全管理体系的有效性作出贡献；

——**指引方向：**最高管理者应为组织内的各级人员提供明确的安全管理方向和目标，确保所有人员都明白自己的角色和职责。

——**提供资源：**为人员提供必要的资源支持，如培训、工具和信息，帮助他们更好地执行安全管理任务；

——**解决问题：**当人员在执行安全管理任务中遇到问题时，最高管理者应及时介入，提供必要的指导和帮助，确保问题得到妥善解决。

(8)推动组织安全管理体系的持续改进；

——**设定明确目标：**最高管理者应设定清晰的安全管理目标，包括提升体系适宜性、充分性和有效性的具体指标，以指导改进工作的实施；

——**制定改进计划：**根据目标设定，最高管理者应制定具体的改进计划，包括改进措施、实施步骤和时间表等。

——**确保资源投入：**为推动改进计划的实施，最高管理者应确保必要的资源投入；

——**内部审核与管理评审：**通过定期开展内部审核和管理评审活动，最高管理者可以识别安全管理体系中存在的问题和不足，为改进工作提供方向；

——**绩效评估：**建立安全管理绩效评价体系，对体系运行效果进行定期评估，识别改进空间；

——**知识更新与经验分享：**最高管理者应关注行业最新动态和最佳实践，及时更新安全管理体系内容，并通过内部培训和经验分享等方式，提升全员的安全管理意识和能力。

(9)支持其他相关管理者在其职责范围内发挥领导作用。

——**资源提供：**最高管理者应合理调配组织资源，确保各级管理者在开展安全管理工作时拥有充足的资源支持，以确保安全管理工作的顺利开展；

——**决策支持：**在安全管理决策过程中，最高管理者应积极听取其他管理者的意见和建议，为他们提供决策支持和指导；

——**能力培养：**最高管理者应关注各级管理者的能力培养，提供必要的培训和学习机会，提升他们的安全管理能力和水平。

ISO 28000-2022 《安全与韧性—安全管理体系要求》

5 领导作用

5.2 安全方针

5.2.1 建立安全方针

最高管理者应制定安全方针，以便：

a) 与组织的宗旨相适应；

b) 为建立安全目标提供框架；

c) 包括对满足适用要求的承诺；

d) 包括对持续改进安全管理体系的承诺；

e) 考虑安全方针、目标、指标、方案等可能对组织的其他方面产生的不利影响。

5.2.2 安全方针要求

安全方针应：

——与其他组织方针相一致；

——与组织整体安全风险评估相一致；

——规定在收购或与其他组织合并或在其他情况下，对其进行评审。

——组织业务范围发生变化，可能影响安全管理体系的连续性或相关性；

——描述并分配主要的责任和成果责任；

——作为成文信息而可被获取；

——在组织内予以沟通；

——适宜时，可为有关相关方所获取。

注：组织可以选择有一个详细的安全管理方针供内部使用，其中包括将提供足够的信息和指导，以推动安全管理体系（部分内容可以保密），并有一个包含广泛目标的摘要（非保密）版本，以便向其相关方传播。

5.2 安全方针

5.2.1 建立安全方针

(1)**安全方针定义：**指由组织最高管理者正式制定并表述的，旨在明确组织在安全管理和实现安全目标方面的总体意图和核心方向。

——**安全方针的核心指导作用：**安全方针是组织安全管理体系的核心组成部分，它明确了组织在安全管理和实现安全目标方面的总体意图和核心方向；

——**安全方针的制定者：**安全方针由组织的最高管理者正式制定并表述，体现了最高管理者对组织安全管理的重视和承诺；

——**明确意图和方向：**安全方针应清晰阐述组织在安全管理和实现安全目标方面的总体意图和核心方向，为组织的安全管理提供明确的指导；

——**安全方针与组织目标的关联：**与组织目标相一致：安全方针的制定应与组织的宗旨、战略目标相一致，确保安全管理工作的方向性与组织整体目标相协调。

(2)最高管理者应制定安全方针，以便：

(a)与组织的宗旨相适应；

——**组织的宗旨：**是一个组织存在和发展的根本理由，它描述了组织希望实现的长远目标和价值观。宗旨通常包含组织的使命和愿景，使命说明了组织的核心业务和目标受众，而愿景则描绘了组织希望在未来达到的理想状态；

——**宗旨的适应性：**最高管理者在制定安全方针时，应确保其与组织的宗旨紧密相连。安全方针的制定要考虑到组织的使命、愿景和核心价值观，确保安全管理活动与组织的整体目标和方向一致。

组织的宗旨	组织的安全方针示例
使命：致力于提供安全、高效、可靠的物流服务，满足全球客户需求	**安全方针：**我们将持续投资于物流安全管理，确保每一环节都符合最高安全标准，为客户提供无懈可击的物流体验
愿景：成为全球最值得信赖的物流服务提供方，创造安全、便捷的商业环境	**安全方针：**我们致力于构建一个全面的安全管理体系，通过持续的风险评估和改进，确保我们的服务始终符合客户的期望和法规要求
核**心价值观：**安全至上，客户为先，团队合作，创新驱动	**安全方针：**安全是我们所有决策和行动的首要前提，我们将积极采纳创新的安全技术和方法，保障客户的安全利益，并通过团队合作不断提升安全管理水平

(b)为建立安全目标提供框架；

——**为建立安全目标提供了具体的框架：**安全方针应明确阐述安全管理的目标和方向，以便组织能够据此设定具体、可衡量的安全目标；

——**安全方针对目标设定的影响**

- **目标一致性：**在安全方针的框架下，组织可以确保所设定的安全目标与组织的宗旨和整体战略保持一致，从而增强安全管理的针对性和有效性；
- **目标可操作性：**明确的安全方针有助于组织将抽象的安全管理理念转化为具体的、可操作的安全目标，为安全管理活动的实施提供明确的方向和路径。

——**方针与目标的协调统一**在安全方针的框架下，组织可以形成统一的安全管理行动准则，确保所有安全管理活动都围绕实现安全目标展开，从而提高安全管理的整体效率和效果。

安全方针示例	安全目标示例	安全方针为建立安全目标提供框架说明
我们致力于建立一个全面、系统、持续改进的安全管理体系，以确保员工、资产和信息的保护，维护组织的声誉和持续发展	**员工安全**：减少工伤事故率至少 20%，提高员工安全意识培训参与率至 90%以上	安全方针提供确保员工安全的总体方向，安全目标则具体化了减少工伤事故和提高培训参与率的目标
	资产保护：确保所有关键资产得到适当保护，降低资产损失风险至可接受水平	安全方针强调资产保护的重要性，安全目标则量化资产损失风险的降低目标
	信息安全：提高信息系统的安全性，减少信息安全事件发生率至每年不超过 2 次	安全方针明确信息安全的总体要求，安全目标则设定具体的信息安全事件发生率降低目标
	合规性：确保所有业务活动符合法律法规和行业要求，避免重大合规风险	安全方针强调了合规性的重要性，安全目标则明确了避免重大合规风险的目标

(c)包括对满足所有适用要求的承诺；安全方针应明确包含对满足所有适用要求的承诺，这些要求可能来自于法律法规、行业标准、国际标准和组织内部的安全标准、合同协议等；

(d)包括对持续改进安全管理体系的承诺；

——**持续改进的承诺：**安全方针中应明确表达出组织对持续改进安全管理体系的坚定承诺。这一承诺不仅反映了组织对提升安全管理绩效的积极态度，也是推动安全管理体系不断完善和进步的重要动力；

——**持续改进内涵解释：**指组织为了不断提升其安全绩效而实施的一系列循环活动。组织应不断寻求提升安全管理效能的机会，包括但不限于对现有流程、制度、技术和管理的优化和创新。这种改进可以是对现有做法的微调，也可以是根本性的变革，旨在更好地应对不断变化的安全环境和挑战；

——**组织文化：**将持续改进作为安全方针的一部分，有助于在组织中营造一种追求卓越、不断学习的文化氛围。这种文化将鼓励员工积极参与安全管理改进活动，提出建设性意见和建议，共同推动安全管理体系的不断完善。

(e)考虑安全方针、目标、指标、方案等可能对组织的其他方面产生的不利影响。

——**全面影响评估：**在制定和实施安全方针、目标、指标和方案时，组织应全面考虑这些措施可能对组织的运营、财务、人力资源等多个方面产生的不利影响。这要求组织具备前瞻性和系统性思维，以确保安全管理措施与组织整体运营相协调；

——**潜在影响识别：**组织应识别和分析安全管理体系相关要素可能带来的潜在不利影响，包括但不限于对生产效率、成本控制、员工满意度、企业文化、客户关系和合规性等方面的影响。

——**风险平衡：**在追求安全管理目标的同时，组织应努力平衡安全管理措施可能带来的潜在风险与收益。在决策过程中，组织需要综合考虑各种因素，确保安全管理措施的实施不会给组织带来不必要的负担或损失。

5.2.2 安全方针要求

(1)安全方针应与其他组织方针相一致；

——**一致性原则：**安全方针应与组织的其他重要方针（如质量方针、环境方针、职业健康安全方针等）保持一致，确保组织在追求多目标时能够统一行动、协调一致；

——一致性的具体体现。

- 理念融合：安全方针应与其他方针共同体现组织的核心价值观和发展愿景，形成统一的管理理念；
- 目标对接：安全目标应与其他方针目标相互衔接，共同推动组织整体目标的实现；
- 措施协同：安全管理体系的具体措施应与其他管理体系的措施相互协同，形成互补和增强效应。

(2)安全方针应与组织整体安全风险评估相一致；

——**风险评估的关联性：**安全方针的制定应基于组织整体安全风险评估的结果，确保方针能够针对性地解决组织面临的主要安全问题；

——**风险评估结果融入方针：**将组织整体安全风险评估的结果充分融入安全方针的制定过程中，确保方针的针对性和适应性；

——**提高安全管理效能：**通过确保安全方针与组织整体安全风险评估的匹配性，组织能够更加精准地识别和管理安全风险，提高安全管理的效能。

(3)安全方针应规定在收购或与其他组织合并或在其他情况下，对其进行评审。

——特定情况的定义；

- **收购或合并：**当组织进行收购或与其他组织合并时，组织的安全环境、业务流程和管理结构都可能发生重大变化；
- **其他情况：**涵盖一系列可能导致组织安全状况发生显著变化的事件或决策，例如组织结构的重大调整、业务范围的显著扩大或缩小等。

——评审的必要性；

- **保持方针的适应性：**通过评审，组织可以确保安全方针在新的环境下依然有效，依然能够指导组织的安全管理活动；
- **应对新风险：**随着组织环境的变化，组织可能面临新的安全风险。通过评审，组织可以及时发现并应对这些新的风险。

——评审的内容与流程；

- **内容：**评审应重点关注安全方针是否依然与组织的宗旨、战略目标以及当前的安全环境相匹配，是否依然能够指导组织有效地管理安全风险；

- **流程：**评审应由最高管理者或指定的安全管理负责人牵头，组织相关部门和专家进行。评审过程应公开透明，确保所有关键利益相关方都能参与并提出意见。

——评审的结果处理。

- **调整方针：**如果评审发现安全方针存在不适应的情况，组织应及时对方针进行调整，确保其能够适应新的环境和管理需求。
- **制定改进计划：**基于评审结果，组织应制定详细的改进计划，明确改进的方向、措施和时间表，并指定专人负责实施和跟进。

(4)安全方针应组织业务范围发生变化，可能影响安全管理体系的连续性或相关性；

——业务范围变化的识别；

- **业务范围定义：**业务范围是指组织所从事的主要活动、产品或服务的范围；
- **变化识别：**组织应持续关注其业务范围的变化，包括新增业务、业务缩减或重组等。

——业务范围变化对安全管理体系的影响评估；

- **连续性评估：**业务范围的变化可能影响到安全管理体系的连续性，即是否能够在变化后继续保持其有效性和适用性；
- **相关性评估：**业务范围的变化也可能影响到安全管理体系与当前业务活动的相关性，即管理体系是否能够紧密贴合组织新的业务需求。

——**安全方针更新：**当业务范围发生变化时，组织应根据评估结果对安全方针进行更新，确保其能够适应新的业务范围和变化后的安全环境。

(5)安全方针应描述并分配主要的责任和成果责任；

——责任与成果责任的定义；

- 责任：指在组织安全管理体系中，各层级、各部门和个人所承担的具体职责和任务；
- 成果责任：指为实现特定的安全管理目标或绩效，相关责任人需承担的确保目标达成或绩效提升的责任。

——成果责任的分配；

- **目标导向：**成果责任的分配应基于组织的安全管理目标，确保每个责任人都明白自己的工作如何为实现这些目标做出贡献；
- **结果衡量：**成果责任的分配应与具体的绩效指标相结合，以便对责任人的工作成果进行衡量和评价。

——**安全方针中的责任与成果责任描述：**安全方针中应具体描述每个层级、部门和个人在安全管理体系中的主要责任和成果责任，确保职责和目标的明确性。

(6)安全方针应作为成文信息而可被获取；

(a)**成文信息形式：**组织应确保安全方针以书面形式或等同于书面形式的成文信息形式存在，这样的形式有助于确保方针的正式性、稳定性和可获取性；

(b)安全方针的详细性与保密性处理要求；

——详细的内部安全管理方针；

- **内容深度：**组织可以选择制定一个详细的安全管理方针，用于组织内部使用。此方针应包含足够的信息和指导，以便为内部安全管理活动提供全面的支持和指导；
- **内部适用性：**详细的方针应考虑到组织内部各部门、岗位和层级的需求，确保安全管理措施能够准确、有效地被执行。

——保密内容的处理；

- **保密性要求：**对于涉及组织敏感或机密信息的内容，方针中应有明确标识，确保这些信息的保密性；
- **访问控制：**组织应建立相应的访问控制机制，确保只有授权人员能够访问这些保密信息。

(c)**员工和相关方的获取：**组织应确保员工和相关方能够方便地获取安全方针，这包括但不限于通过内部公告、电子邮件、员工手册、官方网站等途径进行发布和宣传；

(d)**配有解释或说明：**安全方针应当配有相应的解释或说明，解释或说明应简洁明了，用通俗易懂的语言阐述方针的核心意义、目的和关键要求，以帮助员工和相关方更好地理解方针的内容；

(e)**传播方式：**安全方针可以单独发布，如单独的文件、公告或宣传册，也可以融入其他文档中（如安全管理手册、宣传手册、员工手册等），以便更广泛地传播。

(7)安全方针应在组织内予以沟通；

——安全方针的沟通：组织有责任确保安全方针在组织内部得到充分沟通和深入理解；

——考虑不同层次的沟通需求：为了让所有工作人员都清楚安全方针，组织应考虑不同层次人员的意识和沟通需求，确保信息能够准确传达；

——多样化的沟通方法：沟通安全方针的方法可以多样化，如会议、培训、内部文件、公告板、在组织网站上公布、设置电脑屏保程序等。

(8)适宜时，安全方针应可为有关相关方所获取。

——安全方针的外部可及性：组织应让外部的相关方在适当的时候（需要时）能够方便地获取其安全方针；

——获取与发布的方式：根据相关方的具体要求，组织可以选择通过直接提供文件、在网站上公开发布或者其他适当的方式，确保相关方能够方便、快捷地获取到组织的安全方针。

ISO 28000-2022 《安全与韧性—安全管理体系要求》

5 领导作用

5.3 岗位、职责和权限

最高管理者应确保相关岗位的职责和权限在组织内得到分配和沟通。

最高管理者应指定以下职责和权限：

a) 确保安全管理体系符合本标准的要求；

b) 向最高管理者报告安全管理体系的绩效。

5.3 岗位、职责和权限

(1)最高管理者应确保相关岗位的职责和权限在组织内得到分配和沟通；

(a)**职责和权限的分配：**最高管理者负责确保安全管理体系中相关岗位的职责和权限得到全面而合理的分配。这要求组织明确每个岗位在安全管理体系中的角色和责任，确保所有人员都清楚自己的职责范围；

(b)**职责和权限的沟通：**最高管理者应确保这些职责和权限在组织内部得到充分的沟通。所有相关人员都应清楚了解自己在安全管理体系中的职责和权限，以便在实际工作中有效履行。

(2)最高管理者应指定以下职责和权限：

(a)**符合性保障：**指定专人或团队负责确保安全管理体系符合 ISO 28000 标准的要求。这一职责要求相关人员具备足够的专业知识和能力，能够监督和评估安全管理体系的运行情况，确保其始终符合标准要求。

(b)**绩效报告：**指定专人或团队负责向最高管理者报告安全管理体系的绩效。这一职责要求相关人员能够定期收集和分析安全管理体系的运行数据，客观评价其效果，并向最高管理者提供准确的绩效报告，以便管理层能够及时了解安全管理体系的运行状况，做出相应的决策。

ISO 28000-2022 《安全与韧性—安全管理体系要求》

6 策划

6.1 应对风险和机遇的措施

6.1.1 总则

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：

——确保安全管理体系能够实现其预期结果；

——预防或减少不利影响；

——实现持续改进。

组织应策划：

a) 应对这些风险和机遇的措施；

b) 如何：

——在安全管理体系过程中整合并实施这些措施；

——评价这些措施的有效性。

管理风险的目的是创造和保护价值。管理风险应融入安全管理体系。与本组织及其相关方的安全有关的风险在8.3中述及。

6 策划

6.1 应对风险和机遇的措施

6.1.1 总则

(1)风险的定义

不确定因素对目标的影响。

——**风险的概念：**不确定性对安全目标的影响。这种不确定性一旦发生，会对一个或多个安全目标产生积极或消极的影响；

——**影响的双向性：**影响是对预期的偏离，这种偏离可以是正面的或负面的。风险不仅包括潜在的损失或不利情况，还可能包含潜在的机遇或正面结果；

——**不确定性的本质：**不确定性源于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。风险的本质是无法完全预测和控制的未知因素；

——**风险的描述方式：**风险通常以潜在事件和后果，或两者的组合来描述其特性。评估风险时，应考虑可能发生的事件及其可能带来的后果，以及这些事件发生的可能性；

——**ISO 28000 中的风险特指安全风险：**风险主要关注的是可能对组织安全产生不利影响的不确定因素。与本组织及其相关方的安全有关的风险在“8.3 风险评估和应对”中述及。

(2)管理风险的目的是创造和保护价值；

——**管理风险的目的：**管理风险的根本目的在于创造和保护价值。组织不应仅仅将风险管理视为一种避免损失的防御措施，而应当将其作为一种积极的管理工具，通过有效管理风险，发掘和利用其中的机遇，为组织创造和增加价值；

——**创造价值的途径（识别和利用机遇）：**在管理风险的过程中，组织应积极识别和利用与风险相关的机遇。这些机遇可能包括市场的新趋势、技术的创新、客户需求的变化等，通过有效识别和利用这些机遇，组织可以开发新的业务机会，拓展市场份额，提高盈利能力；

——**保护价值的措施：**减少和避免损失：同时，管理风险也包括减少和避免潜在损失的措施。组织应通过识别、评估和控制潜在的风险因素，减少其对组织目标的不利影响，保护组织的资产、声誉和竞争力。

(3)策划安全管理体系时综合考虑风险与机遇

(a)**策划安全管理体系的考虑因素：**组织在策划安全管理体系时应考虑到 4.1 所提及的因素和 4.2 所提及的要求

——内部和外部因素：在策划安全管理体系时，组织应充分考虑与其宗旨相关的内部和外部因素（见 4.1），这些因素可能包括组织文化、资源状况、市场环境、技术趋势等；

——相关方需求和期望：同时，组织还应关注相关方的需求和期望（见 4.2），确保安全管理体系能够满足这些需求和期望，促进组织与相关方的良好关系。

(b)组织在策划安全管理体系时应确定需要应对的风险和机遇；

——**识别风险与机遇：**基于对上述因素的考虑，组织应识别出与安全管理相关的潜在风险和机遇。风险可能包括安全漏洞、合规性问题、供应链中断等；而机遇则可能包括新技术应用、市场扩张等；

——**应对措施的制定**：对于识别出的风险，组织应制定相应的应对措施，以降低风险发生的可能性或减轻其影响；对于机遇，则应制定利用计划，抓住机遇促进组织发展。

(c)确定需要应对的风险和机遇的目的。

——**实现预期结果**：策划安全管理体系的首要目标是确保体系能够实现组织的预期结果，包括提高安全绩效、增强组织韧性等；

——**预防或减少不利影响**：通过有效的风险管理，组织应能够预防或减少潜在的不利影响，保护组织的资产、声誉和竞争力；

——**实现持续改进**：持续改进是安全管理体系的核心原则之一。组织应通过不断的评估、学习和创新，不断完善安全管理体系，提高其有效性和适应性。

(4)组织应策划：

(a)**策划应对风险和机遇的措施**：组织在策划阶段应针对已识别的风险与机遇，制定具体的应对措施。这些措施应具有针对性和可操作性，以确保能够有效降低风险或抓住机遇。

(b)措施在安全管理体系中的整合与实施

——**整合的重要性**：组织应将应对措施整合到安全管理体系的过程中，确保这些措施能够在组织的日常运营中得到有效实施。这要求组织在策划阶段就充分考虑到措施与现有管理体系的兼容性；

——**实施的具体步骤**：在整合措施后，组织应明确实施的具体步骤和责任人，确保措施能够按计划得到执行。实施过程中，组织应保持对措施执行情况的监控，确保措施的有效性和及时性。

(c)**管理风险融入安全管理体系**：管理风险不应被视为与安全管理体系相分离的活动，而应被视为安全管理体系的一个重要组成部分。将管理风险融入安全管理体系，有助于组织更加系统地识别、评估、应对和监控风险，提高安全管理体系的有效性和可持续性。

(d)评价措施的有效性。

——**评价的目的**：组织应定期对已实施的应对措施进行有效性评价，以确定措施是否达到预期的效果，并据此对措施进行调整和优化；

——**评价的方法**：有效性评价可以通过对措施实施后的结果进行定量或定性的分析来实现。组织可以根据实际情况选择适合的评价方法，如数据分析、问卷调查、专家评审等。

ISO 28000-2022 《安全与韧性—安全管理体系要求》

6 策划

6.1 应对风险和机遇的措施

6.1.2 确定与安全有关的风险并确定机遇

确定与安全有关的风险以及识别和利用机遇，需要进行主动的风险评估，其中应包括考虑但不限于以下方面：

a) 物理或功能故障以及恶意或犯罪行为；

b) 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；

c) 安全设备的设计、安装、维护和更换；

d) 组织的信息、数据、知识和通信管理；

e) 与安全威胁和漏洞有关的信息；

f) 供方之间的相互依存关系。

6.1.2 确定与安全有关的风险并确定机遇

(1)确定与安全有关的风险以及识别和利用机遇，应进行主动的风险评估

(a)**主动风险评估的必要性：**在确定与安全有关的风险以及识别和利用机遇时，组织必须采取主动的风险评估方法。这要求组织不仅仅对已知的风险保持警觉，还要预见可能的新兴风险，以确保安全管理体系的全面性和前瞻性；

(b)**风险评估的深度与广度：**风险评估应深入组织的各个层面和各个环节，包括但不限于供应链、信息技术系统、物理设施和人员安全等。通过全面、细致的风险评估，组织可以更加准确地识别出自身面临的安全挑战和潜在机遇。

(2)风险评估应包括考虑但不限于以下方面：

(a)物理或功能故障以及恶意或犯罪行为；

——**物理或功能故障：**组织应评估其运营过程中可能发生的物理设备损坏或功能失效的风险。这可能包括生产线上的机械故障、关键设施的电力中断、信息系统的硬件问题等。这些故障可能对组织的生产连续性、服务质量和客户满意度产生重大影响；

——**恶意或犯罪行为：**组织应识别可能针对其发起的各种恶意攻击或犯罪行为。这些攻击可能来自外部的黑客、竞争对手、恐怖组织等，包括网络攻击、数据盗窃、勒索软件、欺诈行为等。组织应评估这些攻击对其信息安全、资产安全和声誉可能造成的威胁。

(b)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；

——**环境因素：**这包括但不限于自然环境的变化（如气候灾害、地震等）、社会政治环境的稳定性（如政策变动、国际关系紧张等）以及经济环境的变化（如经济衰退、市场竞争激烈等）。这些因素可能影响组织的运营连续性、供应链稳定性以及员工安全等；

——**人文因素：**人文因素包括员工素质、管理层决策风格、组织文化以及公众意见等。员工的技能和态度、管理层的领导风格以及组织文化都可能对组织的安全产生影响。此外，公众对组织的看法和态度也可能成为潜在的风险或机遇；

——**文化因素：**文化因素涉及组织所在地的文化背景、宗教信仰、风俗习惯等。这些因素可能影响组织的合规性、市场进入策略以及与当地合作伙伴的关系；

——**组织控制之外的因素：**这些因素包括供应链伙伴的安全状况、合作伙伴的信誉度以及外部供方的质量保证等。虽然这些因素在组织控制之外，但它们可能对组织的安全产生重大影响。

(c)安全设备的设计、安装、维护和更换；

——**设计风险**：评估安全设备设计是否符合组织的安全需求和行业标准，是否存在设计缺陷或漏洞，这些缺陷或漏洞可能导致设备无法正常运行或容易受到攻击；

——**安装风险**：在安装过程中，考虑安装环境、操作人员的技能水平、安装流程的规范性等因素对设备性能和安全性的影响。错误的安装可能导致设备性能下降或安全隐患；

——**维护风险**：定期维护对于保持设备性能至关重要。评估维护计划的合理性和执行情况，包括维护周期、维护内容、维护人员的专业能力等。维护不足可能导致设备性能下降，甚至发生故障；

——**更换风险**：随着技术的发展和设备的老化，可能需要更换现有的安全设备。评估更换时机、更换设备的选型、更换过程中的数据迁移和安全保障措施等。不当的更换计划可能导致服务中断或安全风险增加。

(d)组织的信息、数据、知识和通信管理；

——**信息安全**：评估组织的信息系统是否存在安全漏洞，是否容易受到外部攻击或内部泄露。包括数据加密、访问控制、防病毒措施等方面的评估；

——**数据管理**：分析组织数据收集、存储、处理、传输和使用过程中可能存在的风险，如数据丢失、篡改、泄露等。评估数据备份、恢复策略和灾难恢复计划的完整性；

——**知识管理**：评估组织内部知识的获取、共享和保护情况。识别关键知识资产，如专利、商业秘密等，并评估其保护措施的有效性；

——**通信管理**：评估组织内部和外部通信的安全性和可靠性。包括电子邮件、电话、即时通讯等通信渠道的安全性评估，以及应对网络钓鱼、社交工程等攻击的预防措施。

(e)与安全威胁和漏洞有关的信息；

——**安全威胁信息**：组织应收集和分析来自各种渠道的安全威胁信息，包括最新的网络安全攻击模式、黑客活动报告、安全漏洞公告等。这些信息有助于组织了解当前和潜在的安全威胁，从而制定相应的应对策略。

——**安全漏洞信息**：组织应定期评估其系统和应用程序的安全漏洞，包括已知和潜在的漏洞。通过及时获取和分析这些漏洞信息，组织可以迅速采取修复措施，防止恶意利用这些漏洞进行攻击；

——**威胁情报的整合**：组织应将安全威胁和漏洞信息与自身的业务运营和安全管理体系相结合，形成综合的威胁情报体系。这有助于组织更加全面地了解自身的安全状况，并据此制定针对性的风险管理措施。

(f)供方之间的相互依存关系。

——**供方关系识别**：组织应明确识别与其业务运营紧密相关的供方，包括原材料供方、服务提供方、技术支持伙伴等。了解这些供方的业务范围、服务能力以及其与组织的合作方式；

——**依存关系分析**：深入分析组织对供方的依存程度，包括供方提供的资源或服务对组织运营的重要性、供方失效对组织可能产生的影响等。这有助于组织了解潜在的安全风险；

——**风险传播评估**：评估供方可能面临的安全风险如何传播到组织自身。例如，供方的信息系统遭受攻击可能导致组织的数据泄露，或者供方的供应链中断可能影响组织的正常运营。

ISO 28000-2022 《安全与韧性—安全管理体系要求》

6 策划

6.1 应对风险和机遇的措施

6.1.3 应对与安全有关的风险和利用机遇

对已确定的安全相关风险的评价应提供以下输入（但不限于此）：

a) 组织的整体风险管理；

b) 风险应对；

c) 安全管理目标；

d) 安全管理过程；

e) 安全管理体系的设计、规范和实施；

f) 确定足够的资源，包括人员配置；

g) 确定培训需求和所需的能力水平。

6.1.3 应对与安全有关的风险和利用机遇

对已确定的安全相关风险的评价应提供以下输入（但不限于此）：

(1)**组织的整体风险管理：**组织在评估安全风险时，应参考其整体风险管理框架和策略，确保风险应对措施与组织的风险管理目标一致；

(2)**风险应对：**组织应制定具体的风险应对措施，包括预防措施、减轻措施、转移措施和应急措施等，以降低风险发生的可能性和影响程度；

(3)**安全管理目标：**安全管理目标是组织安全管理活动的导向，风险应对措施应与安全管理目标相一致，确保实现组织的整体安全目标；

(4)**安全管理过程：**组织应评估现有的安全管理过程是否能够有效应对已识别的安全风险，必要时对过程进行改进或调整；

(5)**安全管理体系的设计、规范和实施：**组织应考虑安全管理体系的设计、规范和实施情况，确保风险应对措施与管理体系的要求相符合，以实现安全管理体系的有效运行；

(6)**确定足够的资源，**包括人员配置：组织应评估所需资源，特别是人员配置的充足性，以确保风险应对措施的顺利实施；

(7)**确定培训需求和所需的能力水平：**组织应根据风险应对措施的要求，识别并确定所需的培训和能力水平，以提升员工应对安全风险的能力。

ISO 28000-2022 《安全与韧性—安全管理体系要求》

6 策划

6.2 安全目标及其实现的策划

6.2.1 建立安全目标

组织应在相关的职能和层次上建立安全目标。

安全目标应：

a) 与安全方针保持一致；

b) 是可测量的（如可行）；

c) 考虑到适用的要求；

d) 予以监视；

e) 予以沟通；

f) 适时更新；

g) 作为成文信息提供。

6.2 安全目标及其实现的策划

6.2.1 建立安全目标

(1)**目标：**组织在安全管理体系中期望实现的具体结果。

(a)**目标的定义：**安全目标是组织在安全管理体系中设定的、与安全方针保持一致、与安全相关的具体目标。这些目标直接关联到组织的安全管理活动；

(b)目标的特性与分类；

——**战略性与战术性：**目标可以是战略性的，着眼于组织长远发展和整体安全性能的提升；也可以是战术性的，关注于短期内的具体任务和安全绩效的改善；

——**领域多样性：**目标可以涉及多个领域，包括但不限于财务目标、健康安全目标、环境目标等，这些领域共同构成了组织整体安全管理体系的目标体系；

——**层面广泛性：**目标可应用于不同层面，如战略层面、组织整体层面、项目层面、产品和过程层面等，确保从各个层面推动组织安全性能的提升；

——**表述灵活性：**目标可以按多种方式表述，如预期结果、意图、追求、目的、运行准则等，以满足不同组织和不同管理情境的需求。

(2)**安全目标的重要性；**安全目标评估组织安全管理绩效和持续改进的重要依据。设定明确、具体的安全目标有助于组织：

——**明确安全管理方向：**通过设立明确的安全目标，为组织的安全管理活动提供明确的指导方向；

——**衡量安全管理绩效：**通过对比目标与实际成果，识别改进空间和优化策略；

——**促进持续改进：**安全目标的设立与实现是推动组织持续改进的重要驱动力，有助于不断提升组织的安全管理水平。

(3)组织应在相关的职能和层次上建立安全目标。

(a)在相关的职能上建立安全目标；

——**相关的职能全面覆盖：**组织应在所有与安全相关的职能部门中建立安全目标。“相关的职能”指的是那些直接参与或影响组织安全管理工作的职能部门。这些职能包括但不限于以下几个方面：

- **运营职能：**运营部门直接负责组织的日常运营活动，这些活动通常涉及到各种可能的安全风险。因此，运营部门需要在其职能范围内设定明确的安全目标，确保运营活动的安全性和合规性。
- **安全管理职能：**安全管理职能部门是专门负责组织安全管理工作的部门，他们需要制定和实施安全管理政策、程序和控制措施，确保组织整体安全管理体系的有效运行。该部门应设立全面的安全目标，以指导其安全管理工作。
- **采购与供应链管理职能：**采购和供应链管理部门负责选择和管理组织的供方和供应链合作伙伴。由于供应链安全对组织整体安全具有重要影响，这些部门需要在其职能范围内设定安全目标，确保供应链的安全和可靠性。
- **人力资源职能：**人力资源部门负责管理组织的人员，包括招聘、培训、绩效管理等。在安全管理体系中，人力资源部门需要确保员工具备必要的安全意识和技能，因此在人力资源职能上设立安全目标，促进员工安全行为的形成和提升。
- **信息技术职能：信**息技术部门负责组织的信息系统和技术支持，包括网络安全、数据安全等方面。信息技术部门需要在其职能范围内设立明确的安全目标，确保信息系统的安全稳定运行，保护组织的信息资产免受损害。
- **风险评估与管理职能：**风险评估与管理职能部门负责识别和评估组织面临的各种安全风险，制定相应的风险管理措施。这些部门需要设立具体的安全目标，以指导风险评估和管理工作的有效进行。
- **合规与法律事务职能：**合规与法律事务部门负责确保组织的运营活动符合法律法规的要求。在安全管理体系中，该部门需要设立合规性相关的安全目标，确保组织在遵守法律法规方面的合规性和安全性。

——**职能特定性：**安全目标的设立应针对各职能部门的特性和业务需求，确保目标的具体性和可操作性；

——**协同一致：**各职能部门的安全目标应与组织整体的安全方针和战略保持一致，确保各部门在安全管理工作上的协同和一致性。

在相关的职能上建立安全目标示例

职能部门	安全目标示例（可测量）
运营职能	确保每季度内安全事故发生率降低 10%
安全管理职能	年度内完成至少两次安全管理体系的全面审核，并确保所有不符合得到纠正
采购与供应链职能	与关键供方签订安全协议的比例达到 95%以上
人力资源职能	员工年度安全培训参与率达到 100%，且培训后安全知识测试通过率不低于 90%
信息技术职能	网络安全事件响应时间缩短至 30 分钟内，年度内重大数据安全泄露事件为零
风险评估职能	至少每半年进行一次全面的安全风险评估，并根据评估结果实施相应的风险缓解措施

合规与法律事务职能	确保所有运营活动均符合法律法规要求，全年无严重合规性问题发生

(b)在相关的层次上建立安全目标。

——**层次明确性：**组织应在各个管理层级上设定相应的安全目标，确保目标从顶层战略到底层执行的连贯性；“相关的层次”指的是组织内部不同级别的管理层次，包括但不限于以下几个方面：

- **战略层：**战略层是组织的最高决策层，负责制定组织的长期目标和战略方向。在安全管理体系中，战略层应设立与组织整体安全战略相一致的安全目标，确保安全管理工作与组织的战略目标相一致；
- **战术层：**战术层位于战略层之下，负责将战略层的决策转化为具体的行动计划和管理措施。在安全管理体系中，战术层应根据战略层设定的安全目标，制定具体的实施方案和监控措施，确保安全目标的顺利实施。
- **操作层：**操作层是组织的基层执行层，负责具体执行组织的运营活动和管理措施。在安全管理体系中，操作层应根据战术层制定的实施方案和监控措施，执行具体的安全管理措施和操作，确保安全目标在操作层面的有效执行。

——**目标分解：**将组织整体的安全目标分解至各个层级，明确各层级在安全管理中的责任和期望成果。

在相关的层次上建立安全目标示例

管理层次	安全目标示例（可测量）
战略层	到 XXXX 年底，实现组织整体安全风险降低 20%的战略目标
战术层	每年至少进行两次全面的安全风险评估，并制定实施相应的风险缓解计划
操作层	确保每月进行一次安全巡检，及时发现并处理潜在的安全隐患

(4)安全目标应：

(a)**与安全方针保持一致：**安全目标必须与组织的安全方针相一致，确保目标设定与组织的总体安全战略方向相符合。这一要求旨在保证安全目标的一致性和方向性，避免目标设定与组织安全战略出现偏差。

(b)**是可测量的（如可行）：**安全目标应当是具体、可量化的，以便能够对目标实现情况进行准确的评估和监控；

(c)**考虑到适用的要求：**在制定安全目标时，必须考虑适用的法律法规、标准和其他相关要求，确保目标设定满足合规性要求，这些要求可能涉及组织运营活动的各个方面，如环境保护、职业健康与安全等；

(d)**予以监视：**安全目标应受到持续的监视和评估。通过定期检查和审计，组织可以了解目标实现的进展情况，及时发现问题并采取纠正措施。这种监视和评估机制有助于确保安全目标的顺利实现；

(e)**予以沟通：**安全目标应当向组织内部的相关人员进行充分的沟通和解释。这不仅有助于增强员工对安全目标的认识和理解，还能激发他们为实现目标而共同努力的积极性和责任感。通过沟通，组织可以形成一个共同的安全管理氛围和团队精神；

(f)**适时更新：**随着组织运营环境的变化、安全风险的演变以及安全管理水平的提高，安全目标需要适时进行更新和调整。这种更新有助于保持目标的针对性和有效性，确保它们能够始终反映组织当前的安全管理需求和挑战；

(g)**作为成文信息提供：**安全目标应以成文信息的形式提供，确保目标设定的明确性、可追溯性和可审计性，为安全管理提供标准化的指导和管理依据。成文信息可以包括目标设定的文件、监控和评估记录、沟通记录等。

ISO 28000-2022 《安全与韧性—安全管理体系要求》

6 策划

6.2.2 确定安全目标

在策划如何实现其安全目标时，组织应确定：

—— 要做什么；

—— 需要什么资源；

—— 由谁负责；

—— 何时完成；

—— 如何评价结果。

在建立和评审其安全目标时，组织应考虑到：

a) 技术、人力、管理和其他选择；

b) 相关方的意见和影响。

安全目标应与组织对持续改进的承诺相一致。

6.2.2 确定安全目标

(1)**在建立和评审安全目标时，组织应综合考虑以下因素，**确保目标的科学性和合理性：

(a) **技术、人力、管理和其他选择：**技术可行性、人力资源的配备、管理策略和方法的选用，以及可能的其他替代方案；

(b)**相关方的意见和影响：**充分了解和考虑相关方的需求和期望，确保目标的设定能够平衡各方利益。

(2)**安全目标应与组织对持续改进的承诺相一致：**

——安全目标的设定应与组织对持续改进的承诺相一致，旨在确保组织的安全管理目标不仅反映当前的安全管理需求，还能够支持组织的长期发展愿景；

——持续改进的承诺：组织应明确表达对持续改进安全管理体系的承诺，这体现在组织对安全管理工作的持续投入、不断学习和改进的态度上。

(3)**实现安全目标的策划：**在策划如何实现其安全目标时，组织应确定：

——**要做什么：**具体描述为实现安全目标需要开展的工作和活动；

——**需要什么资源：**评估实现目标所需的资源，如人力、物力、财力等，并合理规划和配置；

——**由谁负责：**明确各项工作的责任人和执行团队，确保责任的明确和分工的合理；

——**何时完成：**设定明确的时间表和里程碑，确保工作按计划推进；

——**如何评价结果：**建立科学的评估标准和评价方法，对目标实现情况进行定期检查和评估，及时调整和优化管理策略和措施。

ISO 28000-2022 《安全与韧性—安全管理体系要求》

6 策划

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，包括第10章中所确定的变更，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。

6.3 变更的策划

(1)变更策划与实施的原则；

——当组织确定需要对安全管理体系进行变更时，无论是出于内部需求还是根据第 10 章中提到的改进要求，变更必须按照事先策划好的方式进行实施；

——此要求旨在确保变更过程的有序性、可预测性和可控性，避免因随意变更而给组织的安全管理带来不可预见的风险和混乱；

——变更策划应包含明确的变更目标、步骤、时间表和责任人，确保变更活动按计划有序进行。

(2) 变更策划应考虑的因素：

(a)变更目的及其潜在后果：

——**变更目的：**组织应明确变更的具体目的，是为了满足新的业务需求、优化流程、提高效率，还是为了响应外部环境的变化。明确变更目的有助于组织聚焦变革的核心，确保变革的方向正确；

——**潜在后果评估：**组织应对变更可能带来的潜在后果进行全面评估，包括正面和负面的影响。正面影响可能包括提升业务效率、增强客户满意度等；负面影响可能涉及成本增加、员工适应性问题等。通过综合评估，组织可以权衡利弊，为变更决策提供科学依据。

(b)安全管理体系的完整性：

——**体系结构的保持：**安全管理体系是一个由多个相互关联、相互作用的要素构成的有机整体。在进行安全管理体系变更时，组织应确保这些变更不会对安全管理体系的结构造成破坏，保证其完整性不受损害；

——**流程和标准的连贯性：**安全管理体系包括一系列明确的管理流程和操作标准，这些流程和标准是保证组织安全管理的关键。变更过程中，组织应关注这些流程和标准的连贯性，确保变更后的体系仍然能够按照既定的标准和流程进行运作。

(c)资源的可获得性：

——**资源的重要性：**在安全管理体系变更过程中，资源确保变更活动顺利进行的基石。没有足够的资源支持，任何变更计划都可能面临失败的风险；

——**资源的全面评估：**在进行安全管理体系变更之前，组织应全面评估所需资源的可获得性。这包括对现有资源的存量、使用状况和未来需求的预测。通过全面评估，组织可以准确判断变更所需的资源是否充足，并据此做出合理的决策；

——**资源的提前规划：**为了确保安全管理体系变更的顺利进行，组织应提前规划资源的获取和使用。这包括制定详细的资源需求计划、寻找可靠的资源供方、协商合理的价格条款等。通过提前规划，组织可以确保在变更过程中能够及时获取到所需的资源，避免因资源不足而延误变更进度。

——**资源的优化配置：**在安全管理体系变更过程中，资源的优化配置同样重要。组织应根据变更的具体需求和资源的实际情况，对资源进行合理的分配和利用。通过优化配置，组织可以最大限度地发挥资源的作用，提高变更活动的效率和效果。

(d)职责和权限的分配或再分配：

——**考虑变更对职责与权限的影响：**组织应充分考虑安全管理体系变更对现有职责和权限体系的影响。这包括分析变更可能带来的新任务、新要求以及对现有职责和权限的潜在影响，从而确定是否需要调整或重新分配职责和权限；

——**合理分配与明确沟通：**根据变更的实际需要，组织应重新分配或再分配相关人员的职责和权限。这包括但不限于明确指定新的责任人、调整工作范围、分配新的任务等。同时，组织应通过有效沟通确保所有相关人员都清楚了解并接受这些变更后的职责和权限；

——**确保权责一致：**在重新分配或再分配职责和权限时，组织应确保权责一致，即赋予相关人员足够的权力以履行其职责，同时也应明确其应承担的责任和后果。这有助于提高员工的责任感和工作积极性，促进变更活动的顺利实施。

ISO 28000-2022 《安全与韧性—安全管理体系要求》

7 支持

7.1 资源

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管理体系。

7 支持

7.1 资源

(1)**资源的重要性：**组织为了建立、实施、保持和持续改进其安全管理体系，必须首先确定并提供所需的资源；

(2)**资源类型的全面性：**资源包括但不限于人员、设施、设备、技术、资金、时间、信息等，它们是安全管理体系有效运行的基础；

(3)**资源提供的明确性：**组织应清晰地确定哪些资源是必需的，并且确保这些资源是可获取的，以满足安全管理体系各阶段的需求；

(4)**资源的持续供应：**资源供应不应仅局限于安全管理体系的初始建立阶段，而应贯穿于实施、保持和持续改进的全过程；

(5)**资源优化的必要性：**在确定和提供资源时，组织应考虑资源的优化配置，以确保资源的高效利用，避免资源浪费；

(6)**资源评估与调整：**随着安全管理体系的运行和外部环境的变化，组织应定期评估资源的充足性和有效性，并根据需要适时调整资源分配；

(7)**资源获取的合规性：**组织在获取资源时，应遵守相关法律法规和伦理准则，确保资源的合法性和合规性。

ISO 28000-2022 《安全与韧性—安全管理体系要求》

7 支持

7.2 能力

组织应：

——确定在其控制下从事影响其安全绩效的工作的人员所需具备的能力；

——确保这些人员基于适当的教育、培训或经验是能胜任的，必要时获得适当的安全许可；

——适用时，采取措施以获得所需的能力，并评价措施的有效性；

——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。

7.2 能力

(1)组织应确定在其控制下从事影响其安全绩效的工作的人员所需具备的能力；

(a)在组织控制下从事影响其安全绩效的工作的人员包括：

——**安全管理团队：**包括安全经理、安全专员等，负责策划、实施、监视和评审安全管理体系；

——**风险评估人员：**负责识别、评估组织面临的安全风险，提出风险应对策略；

——**应急响应团队：**在发生安全事件时迅速响应，负责事件的处置和恢复工作；

——**一线操作员**：直接参与组织运营活动的员工，其操作可能直接影响到组织的安全绩效；

——**供应链管理人员**：负责供应链的协调和管理，确保供应链的安全和稳定；

——**信息技术人员**：负责维护组织的信息系统安全，防范信息安全威胁；

——**安全审核人员**：负责内部或外部的安全审核，评估组织安全管理体系的有效性。

(b)人员能力的重要性：组织应认识到在其控制下从事影响其安全绩效的工作的人员所具备的能力对于安全管理体系的有效运行至关重要。

(c)从事关键工作的人员具备必要能力；

——安全管理知识与技能：了解安全管理体系的基本原理、方法和工具，具备策划、实施、监视和评审安全管理体系的能力；

——风险评估能力：能够识别和评估组织面临的各种安全风险，包括物理安全、信息安全、供应链安全等；

——应急响应能力：在发生安全事件时能够迅速响应，采取有效的应对措施，减轻事件对组织的影响；

——沟通协调能力：能够与不同部门、不同层级的员工以及相关方进行有效沟通，确保安全信息的及时传递和协同应对；

——培训与教育能力：能够针对员工的不同需求提供相应的安全培训和教育，提高员工的安全意识和技能；

——合规与道德意识：遵守法律法规、行业准则和组织的道德规范，确保安全管理活动的合规性和道德性；

——持续改进意识：持续关注安全管理领域的新发展、新趋势，不断改进和优化组织的安全管理体系；

——决策能力：在复杂情况下能够迅速、准确地做出决策，确保组织的安全和稳定；

——团队协作能力：能够与团队成员紧密合作，共同应对各种安全挑战和问题。

(d)确定安全关键人员所需能力的需求：组织应明确识别这些人员所需具备的具体能力，这些能力应基于他们的岗位职责、安全管理体系的要求以及组织的安全目标来确定；

——分析岗位职责和要求；

- **岗位职责分析**：详细分析每个关键岗位的职责，明确他们在安全管理体系中的作用和责任；
- **工作要求分析**：基于岗位职责，分析完成这些工作所需要的知识、技能和能力。

——评估现有能力；

- **个人能力评估**：对每位关键岗位人员进行能力评估，确定他们当前具备的能力水平；
- **识别能力差距**：将现有能力与所需能力进行对比，识别出能力差距和不足。

——制定能力需求和提升计划。

- **明确能力需求**：基于岗位职责和评估结果，明确每个关键岗位人员所需具备的具体能力；
- **制定提升计划**：针对能力差距，制定个性化的能力提升计划，包括培训计划、实践机会等。

安全关键人员能力要求示例

安全关键人员类别	安全关键人员能力要求

安全关键人员类别	安全关键人员能力要求
安全管理团队	- 安全管理知识与技能 - 风险评估能力 - 应急响应能力 - 沟通协调能力 - 培训与教育能力 - 合规与道德意识 - 持续改进意识 - 决策能力 - 团队协作能力
风险评估人员	- 风险识别与分析技能 - 风险应对策略制定能力 - 数据收集与处理能力 - 沟通协调与报告能力 - 风险评估方法与工具应用能力
应急响应团队	- 快速响应与决策能力 - 事件处置与恢复能力 - 紧急沟通协调技巧 - 应急物资与资源管理能力 - 应对复杂情况的心理素质
一线操作员	- 安全操作规程的遵守能力 - 危险源识别与防范意识 - 安全事故预防与应急处理能力 - 安全培训与教育接受能力 - 安全操作技能与工具使用能力
供应链管理人员	- 供应链风险识别与应对能力 - 供方评估与选择能力 - 合同条款中的安全要求管理能力 - 供应链协同与沟通能力 - 供应链中断的应对与恢复能力
信息技术人员	- 信息系统安全知识 - 网络安全防护与监测能力 - 数据备份与恢复技能

安全关键人员类别	安全关键人员能力要求
	- 安全漏洞识别与修复能力 - 信息安全政策与标准遵守能力
安全审计人员	- 安全管理体系审核能力 - 安全法规与标准理解能力 - 审核工具与技术应用能力 - 审核结果报告与沟通能力 - 持续改进建议提出能力

(2)组织应确保这些人员基于适当的教育、培训或经验是能胜任的，必要时获得适当的安全许可；

(a)确保这些人员基于适当的教育、培训或经验是能胜任的：

——**教育：**组织应确保这些人员接受了与岗位要求相关的必要教育，以便他们具备相应的知识和技能；

——**培训：**对于特定技能或知识，组织应提供必要的培训，以确保这些人员能够胜任其工作；

——**经验：**经验也是评估人员胜任性的重要因素，组织应考虑人员在相关领域的实际工作经验。

(b)**必要时获得适当的安全许可：**对于某些特定岗位或活动，可能需要获得特定的安全许可或认证。组织应确保这些人员按照要求获得了相应的许可或认证。

特定岗位人员安全许可示例

安全许可类型	许可或认证示例
安全管理人员	- 安全工程师注册证书（如适用） - 安全生产管理人员安全培训合格证书（由专业机构或行业协会颁发）
危险物质处理人员	- 危险化学品经营许可证（如适用） - 放射性物质操作许可证（如适用）— 爆炸物品运输许可证（如适用）
信息安全专员	- 信息安全管理体系认证（如 ISO/IEC 27001 相关认证） - 信息安全专业人员认证（如 CISSP, CISM 等）
建筑施工安全主管	- 建筑施工安全生产许可证（如适用） - 建筑施工企业资质证书（如一级、二级建筑施工总承包资质）
特种设备操作人员	- 压力容器操作证 - 叉车驾驶证 - 起重机械操作证
环境与健康安全管理人员	- 环境管理体系认证（如 ISO 14001 内部审核员证书） - 职业健康安全管理体系认证（如 ISO 45001 内部审核员证书）
食品与药品安全专员	- 食品生产许可证相关岗位证书

安全许可类型	许可或认证示例
	- GMP（药品生产质量管理规范）内部审核员证书 - HACCP 认证相关岗位证书
消防安全责任人	- 消防安全责任人证书 - 消防设施操作员证书（如适用）

(3)组织应有适用时采取措施以获得所需的能力，并评价措施的有效性。

(a)**获取关键岗位人员所需能力的适用措施：**当组织识别出某些人员缺乏必要的能力时，应及时采取措施来弥补这一缺陷。这些措施可能包括：

——提供培训和教育；

- **向现有员工提供培训：**针对员工可能面临的工作相关危险源和安全风险，提供必要的技能和操作方法培训；
- **提供实时指导：**在日常工作中，为员工提供实时指导，确保其正确执行任务并遵守安全规程；
- **考虑不同层级员工：**培训应考虑不同层级员工的职责、能力和文化程度，以及工作所面临的具体风险；
- **培训对象：**包括但不限于管理人员、操作岗位人员、相关方的作业人员以及来访人员；
- **必要性：**员工必须接受必要的培训，以有效履行其在安全方面的职责。许多国家和地区都有法律法规要求组织为员工提供无偿培训。

——**重新分配工作：**当现有员工不具备完成某项工作所需的能力时，应将其重新分配给具备相应能力的员工；

——**简化工作或活动：**在不影响安全绩效的前提下，通过简化工作或活动来降低对员工能力的要求；

——**聘用和雇佣能胜任的人员：**直接招聘具备所需能力的员工，作为快速获取必要能力的一种有效方式；

——**外包与承包：**对于组织内部难以完成的高技能或专业工作，考虑将其承包给具备相应能力的外部人员或团队来完成。

(b)评价所采取措施的有效性。

——评价工作人员的能力：

- **监督活动和指导：**组织应通过日常监督活动对工作人员的操作进行观察、记录和反馈，并提供必要的指导和支持。这些活动应旨在确保工作人员正确执行工作程序，减少安全风险，并提升工作效率和质量；
- **现场观察：**组织应实施现场观察，以直观了解工作人员在实际工作环境中的操作表现。通过观察，组织可以评估工作人员的工作技能和职业素养，从而确定他们是否真正具备完成工作所必需的能力；

- **结果评价：**基于监督活动、指导和现场观察的结果，组织应对工作人员的能力进行综合评价。这些评价结果不仅可用于改进培训计划，提升工作人员的能力，还可作为评价安全管理体系整体有效性的重要指标。

——对外部供方能力的控制。

- 当关键工作或活动由外部供方执行时，组织应设置严格的控制措施。这包括在合同中明确规定外部供方应具备的能力要求，并通过实施定期的审核和评估来确保外部供方的工作质量和安全性能符合组织的标准；
- 审核和评估应关注外部供方的合规性、绩效目标达成情况以及安全管理体系的有效性。组织应保留审核和评估的记录，以便跟踪外部供方的表现，并在必要时采取纠正措施。

(4)组织应保留适当的成文信息，作为人员能力的证据。

组织应保留适当的成文信息作为员工能力的证据，这些信息应能证明员工具备完成工作所需的基本资格和能力，并能反映组织为提升员工能力所采取的措施和效果。具体应包括：

（a）**人员资格和能力证明：**组织应保留员工的学历证明（如文凭和执业证书）、培训证书（如培训结业证明）、安全许可（若适用）等文件，以证明员工具备从事相关工作所必需的资格和能力；

（b）**培训记录：**组织应详细记录员工接受的培训内容、培训日期、培训机构以及培训效果评估等信息，以证明组织为提高员工安全相关能力所采取的具体措施及其效果；

（c）**工作表现记录：**组织应记录员工在日常工作中的表现，包括任务完成情况、问题解决能力等方面的信息，以评估员工在实际工作中的安全相关能力和水平；

（d）**技能评估结果：**如果组织对员工进行了安全相关技能评估或测试，应保留评估或测试的结果作为文件化信息，以证明员工的技能水平，并确保员工能够胜任所从事的工作。

ISO 28000-2022 《安全与韧性—安全管理体系要求》

7 支持

7.3 意识

在组织控制下从事工作的人员应知晓：

——安全方针；

——他们对安全管理体系的有效性的贡献，包括改进安全绩效的益处；

——不符合安全管理体系要求的后果；

——他们在实现遵守安全管理方针和程序以及安全管理体系要求方面的作用和职责，包括应急准备和响应要求。

7.3 意识

(1)在组织控制下从事工作的人员应知晓：

(a)**了解安全方针：**所有在组织控制下从事工作的人应明确知晓组织的安全方针。这包括理解方针的目标、原则及组织在安全方面的总体承诺和期望；

(b)**认识个人贡献与改进益处：**员工应认识到自己在维护安全管理体系有效性方面的贡献，以及通过遵守和执行安全规程和标准，如何有助于改进组织的安全绩效；

(c)**了解不符合后果：**员工应明确了解如果不遵守安全管理体系的要求，可能会导致的不利后果。这包括可能发生的事故、伤害、设备损坏以及组织声誉受损等潜在风险；

(d)**明确个人角色与职责：**员工应清楚自己在实现遵守安全管理方针和程序，以及满足安全管理体系要求方面所承担的具体角色和职责。这包括应急准备和响应要求，即在紧急情况下应采取的行动和措施。

(2)提升在组织控制下从事工作的人员意识的措施。

措施类别	提升人员意识具体措施或途径
培训与教育	- 定期组织安全方针培训，确保每位员工理解并遵守 - 开展安全意识提升活动，如安全周、安全月等，强调安全的重要性 - 提供在线或实体课程，教授员工如何识别和改进潜在的安全风险
沟通与宣传	- 利用内部通讯渠道（如公告板、电子邮件、内部网站等）定期发布安全信息 - 举行安全会议，邀请专家或员工分享安全经验和教训 - 制作并分发安全手册或指南，方便员工随时查阅
激励机制	- 设立安全奖励制度，表彰在安全工作中表现突出的个人或团队 - 将安全意识纳入员工绩效评价体系，鼓励员工主动参与安全管理
模拟演练	- 定期组织应急演练，提高员工在紧急情况下的应对能力 - 设立模拟场景，让员工体验并学习如何应对各种安全风险
领导示范作用	- 高层领导积极参与安全活动，展示对安全工作的重视 - 领导层应定期与员工沟通安全事宜，鼓励员工提出安全建议和改进措施
安全文化建设	- 倡导并营造积极向上的安全文化氛围，让员工将安全视为共同的责任 - 鼓励员工之间互相监督和提醒，共同维护组织的安全环境
持续改进	- 定期对安全意识提升措施进行评估和反馈，识别改进空间 - 鼓励员工提出改进建议，不断完善和提升安全意识提升措施的效果

ISO 28000-2022 《安全与韧性—安全管理体系要求》

7 支持

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：

——沟通什么；

——何时沟通；

——与谁沟通；

——如何沟通；

——在沟通之前，对信息的敏感性进行评估。

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：

(1)**明确沟通内容：**组织需要明确哪些内容需要与安全管理体系相关的内部和外部相关方进行沟通。这包括但不限于安全方针、目标、风险评估结果、改进措施、紧急情况下的应对措施等；

(2)**确定沟通时机：**组织应确定何时进行沟通，以确保信息的及时性和有效性。这通常涉及定期沟通（如年度、季度、月度报告）和即时沟通（如发生紧急情况或重要变更时）；

(3)**识别沟通对象：**组织需要识别哪些内部相关方（如员工、管理层、相关部门）和外部相关方（如客户、供方、监管机构、公众）需要接收这些信息；

(4)**选择沟通方式：**组织应根据沟通内容和对象的特点选择合适的沟通方式，如口头报告、书面报告、电子邮件、会议、公告板等。确保信息能够准确、高效地传递给目标受众；

信息沟通机制（方式）示例

沟通方式分类	具体形式与工具	信息沟通方式适用范围
安全培训与教育	- 安全培训课程、研讨会 - 培训资料、作业指导书、工作辅助	全体员工，特别是新员工和需要提升安全知识的员工
文件	- 政策、程序、报告等书面文件（包括健康安全规章制度、操作规程和应急预案以及健康安全信息通报、公告等） - 小册子、时事通讯 - 安全须知	全体员工，特别是需要了解组织安全政策、程序和规定的员工
内部通知或公告	- 内部公共场所发布的通知或信息 - 看板、海报、板报、印刷品或海报、通讯简报、显示屏等宣传形式	全体员工，特别是在组织内部工作或访问的员工
会议	- 管理层会议 - 健康安全委员会会议 - 工作人员委员会会议 - 员工大会	参与会议的相关人员，包括管理层、员工代表等

沟通方式分类	具体形式与工具	信息沟通方式适用范围
	- 安全形势分析会、专题会、周例会、协调会、座谈会、班前班后会通报会等	
电子邮件或内部通讯系统	- 电子邮件、内部通讯系统 - 信件 - 内部网（用于内部通讯和信息共享）	全体员工，特别是需要快速、高效地接收和发送安全信息的员工
手机应用或在线平台 使用社交媒体：如电话、传真、网站、电子邮件、时事通讯以及微信、QQ、钉钉、公众号等	- 专门的手机应用或在线平台 - 互联网网站（用于查询职业健康安全信息）	全体员工，特别是需要随时随地获取安全信息的员工
访谈、交流（安全经验分享、技术交流活动、案例分析）	- 面对面交流、访谈、焦点小组 - 非正式讨论	参与访谈、交流的员工、管理层、相关方等
安全信息系统	- 专门的职业健康安全信息系统 - 安全工作系统（电子化的安全信息管理系统）	需要查询、更新或管理安全信息的员工
事故/事件报告系统	- 安全事故/事件报告系统 - 安全警报	全体员工，特别是需要及时报告和处理安全事故/事件的员工
安全建议箱/意见箱	- 安全建议箱/意见箱 - 调查（收集员工意见和反馈）	全体员工，特别是希望提供安全建议或反馈的员工
社交媒体与内部论坛	- 企业内部社交媒体或论坛中的职业健康安全讨论区	全体员工，特别是希望参与安全讨论和分享经验的员工
外部联系	- 与政府部门和社区的联系机制 - 新闻发布会— 媒体、新闻稿、报纸文章 - 市民顾问组、社区联络小组	外部相关方，包括政府部门、社区、媒体、公众等
外部专家讲座与研讨会	- 邀请外部专家举办讲座和研讨会 - 演讲、专业研讨会、会议	参与讲座和研讨会的员工、管理层、相关方等
其他	- 一对一辅导与咨询 - 现场访问、指导巡视	需要个性化安全辅导或现场指导的员工

(5)**评估信息敏感性：**在沟通之前，组织应对信息的敏感性进行评估，以确定是否需要采取特定的保密措施或限制信息的传播范围。这有助于保护组织的敏感信息，防止信息泄露或被滥用。

ISO 28000-2022 《安全与韧性—安全管理体系要求》

7 支持

7.5 成文信息

7.5.1 总则

组织的安全管理体系应包括：

a) 本标准所要求的成文信息；

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。

成文信息应说明实现安全管理目标和指标的职责和权限，包括实现这些目标和指标的手段和时限。

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、产品和服务的类型；

——过程及其相互作用的复杂程度；

——人员的能力。

组织应确定信息的价值，并确定所需的完整性水平和安全控制，以防止未经授权的访问。

7.5 成文信息

7.5.1 总则

(1)成文信息定义

组织需要控制并保持的信息及其载体。

——成文信息可以任何格式和载体存在，并可来自任何来源；

——成文信息可涉及：

- 安全管理体系，包括相关过程；
- 为组织运行而产生的信息一组文件；
- 实现结果的证据[记录]。

——载体可以是纸张，磁性的、电子的、光学的计算机盘片，照片或标准样品，或它们的组合。

(2)组织的安全管理体系应包括：

(a)**ISO 28000 标准所要求的成文信息：**组织的安全管理体系必须包含 ISO 28000 标准明确要求的成文信息。这些成文信息构成了安全管理体系的框架和基础，确保组织的安全管理活动符合国际标准和行业最佳实践；

(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：**组织应根据自身的实际需求和特点，自行确定和提供必要的成文信息。这些信息可能涉及组织特有的安全管理程序、操作指南、应急预案等，以支持组织实现其安全管理目标。

(3)成文信息应说明实现安全管理目标和指标的职责和权限，包括实现这些目标和指标的手段和时限。

——**职责和权限的明确性：**成文信息应清晰地阐述实现安全管理目标和指标所需的各级职责和权限。这包括从最高管理者到各级管理人员，以及执行层员工在安全管理中的具体职责和权限；

——**实现目标的手段说明：**成文信息应详细说明实现安全管理目标和指标所采取的具体措施或手段。这些手段可能包括安全管理制度、流程、操作规程、应急预案等，旨在确保安全管理体系的有效运行；

——**时限的设定与遵守：**成文信息应规定实现安全管理目标和指标的时限，并确保组织在规定的时限内完成相关任务。时限的设定应合理且具有挑战性，以推动组织持续改进安全管理绩效。

(4)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：

(a)**组织规模的影响：**不同规模的组织在安全管理体系成文信息的多少与详略程度上存在差异。大型组织可能由于管理层次多、活动范围广，需要更多的成文信息来支持其安全管理；而小型组织可能因其结构简单、活动范围有限，成文信息相对较少；

(b)**活动、过程、产品和服务的类型：**组织所从事的活动、过程、产品和服务的类型直接影响其安全管理体系成文信息的具体内容。例如，从事高风险活动的组织需要详细的安全操作规程和应急预案，而成文信息可能相对简单；

(c)**过程及其相互作用的复杂程度：**组织内部过程及其相互作用的复杂程度也决定了安全管理体系成文信息的详细程度。当组织内部过程相互关联、相互影响时，需要更详细的成文信息来确保过程的顺畅执行和安全管理的有效性；

(d)**人员能力的影响：**组织中人员的能力水平对成文信息的详略程度有一定影响。当人员具备较高的安全管理能力和技能时，可能不需要过于详细的成文信息；而当人员能力相对较弱时，则需要更详细的成文信息来指导其工作。

(5)组织应确定信息的价值，并确定所需的完整性水平和安全控制，以防止未经授权的访问。

(a)**信息的价值评估：**组织应明确每类成文信息的价值，这有助于组织合理分配资源，确保关键信息得到充分的保护和管理。信息的价值评估可能包括其重要性、敏感性以及对组织安全管理的影响程度；

(b)**完整性水平的确定：**成文信息的完整性对于确保安全管理活动的准确性和有效性至关重要。组织应根据信息的性质和用途，确定所需的完整性水平。这包括确保信息的准确性、一致性和完整性，避免信息在传递和使用过程中被篡改或遗漏；

(c)**安全控制的实施：**为了防止未经授权的访问，组织应建立适当的安全控制措施。这些措施可能包括访问权限管理、数据加密、安全审计等，以确保只有授权人员能够访问和使用关键的安全管理信息；

(d)**敏感信息的特殊处理：**对于特别敏感或重要的安全管理信息，组织应采取额外的保护措施。这可能包括限制信息的知悉范围、采用更高强度的加密技术、实施更严格的访问控制策略等。

ISO 28000-2022 《安全与韧性—安全管理体系要求》

7 支持

7.5 成文信息

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）；

——形式（如语言、软件版本、图表）和载体（如纸质的、电子的）；

——评审和批准，以保持适宜性和充分性。

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；

(a)**标识：**组织应为创建的每一份成文信息提供独特的标识，如标题、文件名或版本号。这些标识确保信息的唯一性和可追溯性，方便用户快速定位和使用；

(b)**说明：**除了标识外，组织还应为成文信息提供详细的说明信息，如日期、作者或索引编号。这些说明信息帮助用户了解文件的背景、来源和更新时间，增加信息的透明度和可信度。

(2)形式与载体；

(a)**形式：**组织应根据信息的性质和用途选择合适的形式进行表达，如使用不同的语言文字、软件版本或图表。这确保信息以用户易于理解和使用的方式呈现；

(b)**载体：**信息的载体可以是纸质的也可以是电子的。组织应根据信息的存储、访问和使用需求选择合适的载体，确保信息的易获取性和可保存性。

(3)评审和批准。

(a)**评审：**在创建或更新成文信息后，组织应对其进行全面评审。评审过程应关注信息的内容是否符合ISO 28000标准的要求，以及是否反映了组织的实际情况和最新进展。评审确保信息的准确性和适用性；

(b)**批准：**评审完成后，组织应对成文信息进行批准。批准应由具备相关权限和专业知识的人员进行，以确保信息的适宜性和充分性。批准过程增加了信息的权威性和可靠性，确保其在组织内的有效实施。

ISO 28000-2022 《安全与韧性—安全管理体系要求》

7 支持

7.5 成文信息

7.5.3 成文信息的控制

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）；

c）定期评审，必要时进行修订，并由授权人员批准其适当性；

d）过时的文件、数据和信息被迅速从所有发放点和使用点删除，或以其他方式保证不被非预期使用；

e）为法律或知识保存目的或两者而保留的档案文件、数据和信息得到适当的识别。

为控制成文信息，适用时，组织应进行下列活动：

——分发、访问、检索和使用；

——存储和防护，包括保持可读性；

——更改控制（如版本控制）；

——保留和处置。

对于组织所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。

注：对于成文信息的“访问”可能意味着仅允许查阅或者意味着允许查阅和并授权修改。

7.5.3 成文信息的控制

(1)组织应控制安全管理体系和 ISO 28000 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；

——确保信息的可获得性；

- 组织应确保在需要的场合和时机，所有相关的成文信息都是可获得的。这要求组织建立完善的信息管理系统，确保信息的存储、检索和传递畅通无阻；
- 当信息被存储在电子系统中时，组织应确保系统的稳定性和可靠性，以防止信息丢失或损坏。同时，对于纸质文档，组织应确保其物理存储的安全和易于访问。

——保证信息的适用性；

- 成文信息必须满足组织的实际需求，且应与组织的安全管理体系和ISO 28000标准的要求相一致。组织应定期对成文信息进行审查，以确保其内容的准确性和适用性；
- 当组织的业务活动、管理结构或安全要求发生变化时，组织应及时更新成文信息，以确保其与实际情况相符。

——控制过程的具体措施。

- 组织应实施一系列控制措施，如信息的分类管理、权限设置、版本控制等，以确保成文信息的准确性和有效性。
- 组织应建立信息保护机制，防止未经授权的访问和修改，确保成文信息的安全性和保密性。

(b)予以妥善保护（如：防止泄密、不当使用或缺失）；

——**成文信息的保护目的：**组织应确保安全管理体系和 ISO 28000 标准所要求的成文信息得到妥善保护，以防止信息的泄露、不当使用或缺失。这是确保组织安全管理活动顺利进行的重要基础；

——**防止信息泄密：**组织应采取一系列措施来防止信息的泄露，如设置访问权限、使用加密技术、实施物理隔离等。这些措施能够确保只有授权人员能够访问敏感信息，降低信息泄露的风险；

——**防止不当使用：**除了防止信息泄露外，组织还应关注信息的不当使用问题。组织应确保授权人员在使用信息时遵守相关规定和程序，不得将信息用于非法或不当目的。同时，组织还应加强对信息使用情况的监督和检查，及时发现和处理不当使用行为；

——**防止信息缺失：**信息缺失可能导致组织在安全管理活动中出现疏漏和失误。因此，组织应采取必要的措施来确保信息的完整性和连续性。例如，建立信息备份和恢复机制、定期检查和更新信息等。这些措施能够降低信息缺失的风险，确保组织在安全管理活动中能够获取完整、准确的信息支持。

(c)定期评审，必要时进行修订，并由授权人员批准其适当性；

——**定期评审的必要性：**组织应定期对安全管理体系和 ISO 28000 标准所要求的成文信息进行评审。这有助于确保信息的时效性、准确性和有效性，保证其与组织的安全管理需求和标准要求的一致性；

——**评审内容的全面性：**评审应涵盖所有成文信息的各个方面，包括但不限于内容的准确性、格式的规范性、与标准要求的符合性等。通过全面细致的评审，确保信息的完整性和可靠性；

——**必要时进行修订：**在评审过程中，如果发现成文信息存在错误、过时或不符合标准要求的情况，组织应及时进行修订。修订过程应遵循相关程序和规定，确保修订内容的准确性和合法性；

——**授权人员批准：**对成文信息的修订完成后，应由授权人员进行批准。授权人员应具备相应的专业知识和决策权限，能够对修订内容的适当性进行准确判断。批准过程应确保信息的权威性和可靠性。

(d)过时的文件、数据和信息被迅速从所有发放点和使用点删除，或以其他方式保证不被非预期使用；

——**过时信息的识别：**组织应定期识别和评估安全管理体系和 ISO 28000 标准所要求的成文信息，以确定哪些文件、数据和信息已过时或不再适用；

——**迅速删除过时信息：**一旦确定信息过时，组织应迅速将其从所有发放点和使用点删除，以防止非预期的使用。这有助于确保组织内部使用的信息始终是最新的和准确的；

——**非预期使用的预防措施：**对于不能立即删除或需要保留的过时信息，组织应采取其他措施，如设置访问限制、标注为“过期”或“仅供参考”等，以确保其不被非预期使用。

(e)为法律或知识保存目的或两者而保留的档案文件、数据和信息得到适当的识别。

——**法律与知识保存信息的重要性：**组织应意识到，某些成文信息由于法律要求或知识保存目的而需要长期保留。这些信息对组织的法律合规性和知识传承具有重要意义；

——**适当识别保留的信息：**组织应明确识别出哪些档案文件、数据和信息需要为法律或知识保存目的而保留。这要求组织对信息内容进行仔细评估，并与相关法律要求和组织知识管理策略相衔接；

——**明确标识与记录：**对于需要保留的档案文件、数据和信息，组织应给予明确的标识，并记录其保留的原因和期限。这有助于组织内部员工和相关方明确了解哪些信息是需要特别关注的；

——**存储与保护：**组织应采取适当的措施来存储和保护这些法律或知识保存目的的信息。这可能包括使用专用的存储设备、设置访问权限、定期备份等，以确保信息的安全性和可访问性；

——**定期审查与更新：**组织应定期对保留的信息进行审查，以确保其仍符合法律要求和知识保存的目的。如果信息不再需要保留或保留期限已到，组织应及时处理这些信息，以避免不必要的存储和管理负担。

(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；

——分发；

- **机制建立：**组织应建立确保成文信息按需、准确、及时分发的机制；

- **完整性和准确性保障：**分发过程需确保信息在传递中不被篡改或遗失；

——访问；

- **访问权限的设定：**对于成文信息的“访问”，组织应根据信息的敏感性和重要性设定适当的访问权限。这意味着某些信息可能仅允许特定人员查阅，而其他信息则可能允许查阅并进行修改。这种权限设定有助于保护信息的安全性和完整性；
- **查阅与更改权限：**根据组织规定，访问可能仅限于查阅或允许查阅和更改；
- **工作人员访问：**确保工作人员能够获取与工作相关的必要信息；

——检索；

- **信息检索系统：**建立支持关键词搜索、分类浏览等功能的信息检索系统；
- **高效获取：**确保人员能够快速准确找到所需信息；

——使用。

- **信息正确性：**确保使用中的成文信息正确且适宜；
- **信息更新与废止：**对过时或不再适用的信息及时更新或废止；
- **合规性关注：**确保信息使用符合相关法律法规和行业标准；

(b)存储和防护，包括保持可读性；

——**妥善存储：**确保信息完整性、可访问性和长期保存；

——**具体存储方式：**选择适合的存储方式，如电子表格、应用程序等；

——**保护措施：**采取物理安全、网络安全和访问控制等措施保护信息；

——**完整性和易读性：**定期检查和更新存储介质，保持信息完整和易读；

——**保密信息处理：**对敏感内容采取额外保护措施，如设置访问权限；

(c)更改控制（如版本控制）；

——**重要性：**严格控制信息变更，防止错误或混淆；

——**版本控制：**为每个版本分配唯一标识符，追踪管理修改历史；

——**实施方式：**评估变更必要性、批准变更请求、记录变更详情并更新信息；

——持**续性和适用性：**随着组织活动变化不断优化变更控制，适用于内外部信息；

(d)保留与处置。

——**保留目的：**确保持续跟踪、验证和评估体系绩效，满足法律法规要求；

——**保留期限：**根据信息性质、重要性和法规要求确定保留期限；

——**信息更新与过时：**定期评估信息有效性，及时更新或废弃过时信息；

——**信息处置：**建立安全销毁或转移程序，特别注意敏感或机密信息的保密性和安全性；

——文**档管理系统：**建立文档管理系统，提供信息分类、存储、检索、更新和销毁功能；

(3)对于组织所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。

(a)**识别外部成文信息的必要性：**在策划和运行安全管理体系的过程中，组织需要确定哪些来自外部的成文信息是其所必需的；

(b)对外部成文信息的适当识别：

——组织应建立一个机制，来系统地识别并评估这些外部成文信息，确保它们与组织的安全管理体系目标和要求相符合；

——识别过程应包括对信息来源的确认，以确保信息的可靠性和权威性；

(c)对于组织所安全管理体系所必需的来自外部的成文信息可能包括但不限于：

——法律法规与标准；

- 国家或地区的安全管理相关法律法规，包括职业健康安全、环境保护、数据保护等方面的法律要求；
- 行业标准，如ISO 9001、ISO 14001、ISO 27001等，这些标准提供了关于质量管理、环境管理和信息安全管理的框架和指南。

——**行业指南与最佳实践：**由行业协会或专业组织发布的行业指南，如供应链安全指南、业务连续性管理指南等，这些指南通常包含针对特定行业或领域的最佳实践和建议；

——**供应链合作伙伴提供的信息：**供应链中上游和下游合作伙伴提供的安全管理政策、程序、安全控制要求等信息，这些信息有助于组织了解供应链中的安全风险并采取相应的管理措施；

——风险评估与合规性报告；

- 外部风险评估机构提供的风险评估报告，这些报告可能包含组织运营环境中潜在的安全威胁和风险点；
- 合规性报告，如安全审计报告、合规性验证报告等，这些报告用于证明组织已经遵守了相关的法律法规和标准要求。

——**安全事件与漏洞通报：**来自安全漏洞通报平台或机构的安全事件和漏洞信息，这些信息有助于组织及时了解最新的安全威胁并采取相应的防护措施；

——**沟通与协作协议：**与外部组织（如监管机构、合作伙伴、应急响应机构等）签订的沟通与协作协议，这些协议规定了组织在发生安全事件时应如何与外部组织进行沟通和协作；

——**其他外部信息源：**来自政府机构、专业研究机构、安全咨询公司等提供的安全管理资讯、报告、建议等，这些信息有助于组织保持对安全管理领域的最新了解和认识。

(d)对外部成文信息的控制：

——在识别出必要的外部成文信息后，组织应建立相应的控制措施，以确保这些信息得到妥善的管理和使用；

——控制措施包括但不限于设置访问权限、定期验证信息的有效性、及时更新过时的信息以及记录信息的获取、使用过程等；

——这些控制措施旨在防止信息泄露、误用或滥用，确保组织的安全管理体系能够有效地利用这些外部成文信息。

(e)确保控制措施的有效性：

——组织应定期对外部成文信息的控制措施进行评审和更新，以确保其始终有效；

——在评审过程中，组织应关注外部环境的变化（如法律法规的更新）以及组织内部活动的发展，及时调整控制措施以适应新的要求。

(f)责任与程序；

——组织应指定专人负责外部成文信息的识别、获取和控制工作，确保控制措施得到有效实施；

——组织应建立明确的程序来指导外部成文信息的识别、控制和使用过程，以确保所有相关人员都能够遵循这些程序进行操作。

(g)外部成文信息的适当控制。

——**适当控制外部成文信息：**组织在识别到策划和运行安全管理体系所必需的外部成文信息后，应实施适当的控制措施以确保这些信息的准确性、可用性、及时性和合规性。这些控制措施可能涉及对外部成文信息的收集、验证、分发、存储、更新和废止等全过程的管理；

——**保持信息的准确性和完整性：**在控制外部成文信息的过程中，组织应特别关注信息的准确性和完整性。组织应建立有效的验证机制，确保所获取的外部成文信息准确无误，避免因信息不准确或不完整而导致的管理决策失误，从而保障安全管理体系的有效运行；

——**确保信息的合规性：**组织应确保所控制的外部成文信息符合相关的法律法规和标准要求。这包括定期审查所收集的外部成文信息，以确保其持续符合最新的法律法规和标准，从而避免因违反法律法规而导致的不必要的风险和损失。同时，组织应确保这些信息与组织的整体管理要求和策略相协调，以确保安全管理体系的合规性和有效性。

ISO 28000-2022 《安全与韧性—安全管理体系要求》

8 运行

8.1 运行的策划和控制

组织应策划、实施和控制满足要求所需的过程，并实施第6章确定的措施，具体方法是：

——建立过程准则；

——按照准则实施过程控制。

组织应保留必要的成文信息，确保过程已按策划得到实施。

8 运行

8.1 运行的策划和控制

(1)**运行策划的全面性：**组织应对满足安全管理体系要求所需的所有过程进行全面策划，确保这些过程的有效实施和控制；

(2)**实施第 6 章确定的措施：**组织在实施运行时，必须遵循第 6 章中所策划的风险和机遇应对措施、安全目标及其实现的策划以及变更的策划等内容，确保安全管理体系的一致性和有效性；

(3)**建立过程准则：**为了确保运行过程的有序进行，组织应为每个关键过程建立具体的准则（如流程、标准、规范等），准则内容应涵盖过程的输入、输出、活动步骤、所需的资源、时间期限、责任人、关键控制点、监测和评估标准等方面，以便所有相关人员能够清晰了解并执行。

(4)**按照准则实施过程控制：**在运行过程中，组织应严格按照所建立的准则进行过程控制，确保每个环节都符合预设的标准和要求，防止偏差和失误的发生；

(5)保**留必要的成文信息：**组织应保留足够的成文信息，以证明运行过程已按照策划得到实施，包括过程记录、操作指南、检查表等，这些信息对于后续的监视、测量、评审和改进都是至关重要的。

ISO 28000-2022 《安全与韧性—安全管理体系要求》

8 运行

8.2 确定过程和活动

组织应确定那些为实现以下目标所必需的过程和活动：

a）遵守其安全方针；

b）遵守法律法规和监管的安全要求；

c）其安全管理目标；

d）其安全管理体系的交付；

e）供应链所需的安全水平。

8.2 确定过程和活动

组织应确定那些为实现以下目标所必需的过程和活动：

(1)**遵守安全方针：**组织应识别并确定那些直接关联到其安全方针执行的过程和活动。这些过程和活动应能够体现方针的核心原则，确保组织的所有行动与其安全承诺保持一致；

(2)**遵守法律法规和监管要求：**组织需确定满足相关安全法律法规和监管要求的具体过程和活动。这些过程和活动应确保组织的运营符合所有适用的法律和监管标准，避免可能的法律风险和合规问题；

(3)**实现安全管理目标：**组织应识别与实现其安全管理目标直接相关的过程和活动。这些目标可能涉及减少事故率、提高员工安全意识等，相关过程和活动应直接服务于这些目标的达成；

(4)**安全管理体系的交付：**组织应明确确保安全管理体系有效交付的关键过程和活动。这些过程和活动不仅涉及体系的设计和维护，还包括对体系绩效的监视和改进，以确保体系的持续优化和适应变化。

(5)**供应链所需的安全水平：**对于涉及供应链的组织，应确定保证供应链安全所需的关键过程和活动。这些活动可能包括供方评估、风险管理、信息安全保障等，旨在确保供应链的稳定性和安全性，防止供应链中断或安全风险。

ISO 28000-2022 《安全与韧性—安全管理体系要求》

8 运行

8.3 风险评估和应对

组织应实施并保持风险评估和应对程序。

注：风险评估和应对的过程在ISO 31000中涉及。

组织应：

a) 确定其与安全有关的风险，根据其安全管理所需的资源对这些风险进行优先排序；

b) 分析和评估已确定的风险；

c) 确定哪些风险需要应对；

d) 选择并实施应对这些风险的方案；

e) 准备和实施风险应对计划。

注：本条款的风险涉及到组织及其相关方的安全。风险和与管理体系有效性有关的机遇将在6.1中讨论。

8.3 风险评估和应对

(1)风险与安全管理体系有效性的关联；

(a)**安全管理体系有效性机遇：**风险评估和应对不仅关注风险的防控，还与安全管理体系的整体有效性密切相关。组织在应对风险的同时，也应关注与安全管理体系有效性有关的机遇，以便实现持续改进和优化。

(b)**机遇识别与利用：**在风险评估过程中，组织应同时关注可能出现的机遇，如新技术的应用、市场需求的变化等，以便及时识别并利用这些机遇，推动组织的创新和发展。

(2)**风险评估与应对的重要性：**组织及其相关方安全：本条款明确指出了风险评估和应对不仅涉及组织自身的安全，还与其相关方的安全密切相关。这意味着组织在评估风险时，需要综合考虑所有可能受到影响的内外部相关方；

(3)**建立并保持风险评估与应对程序：**

(a)**组织应建立一套完善的风险评估和应对程序，并确保该程序得到持续有效的实施：**该程序应覆盖风险评估的全过程，包括风险识别、分析、评价、应对策略制定以及应对计划的实施等关键环节；

(b)**与国际风险管理标准的衔接：**风险评估和应对的过程应参照 ISO 31000:2018《风险管理指南》，这有助于组织系统地管理风险，提高风险应对的科学性和有效性。

(4)风险识别与优先排序；

(a)**风险识别：**组织应全面识别与其安全相关的风险，这些风险可能源自组织的运营活动、供应链、法律法规遵从性等多个方面；

(b)**优先排序：**根据安全管理所需的资源以及风险的严重性和可能性，对识别出的风险进行优先排序，以便有针对性地制定风险应对策略。

(5)风险的分析与评价；

(a)**风险分析：**对识别出的风险进行深入的分析，分析其发生的可能性和潜在的后果，以便为制定应对策略提供依据；

(b)**风险评价：**基于分析结果，对风险进行等级划分，明确哪些风险对组织的安全构成重大威胁，需要优先应对。

(6)确定风险应对策略；

(a)**应对策略识别：**根据风险评估结果，确定哪些风险需要采取具体的应对措施，以控制风险、减少损失或防止潜在安全威胁的发生；

(b)**策略制定：**针对需要应对的风险，制定相应的应对策略，这些策略可能包括风险避免、风险减轻、风险转移或风险接受等。

(7)选择并实施应对这些风险的方案；

(a)**选择方案：**根据风险评估结果和制定的风险应对策略，选择最适合的风险应对方案。这些方案应基于组织的实际情况和风险特点，确保针对性和有效性；

(b)**实施方案：**将选定的风险应对方案付诸实施，明确实施步骤、责任人、完成时限等，确保风险应对措施得到有效执行。

(8)风险应对计划的准备与执行。

(a)**计划准备：**为每一个需要应对的风险制定详细的应对计划，明确应对措施、实施步骤、监控和评审机制等，确保计划的完整性和可操作性；

(b)**计划执行：**风险应对计划制定后，组织应确保计划得到有效执行，并对执行情况进行持续的监控和评审，以便及时调整和完善计划。

ISO 28000-2022 《安全与韧性—安全管理体系要求》

8 运行

8.4 控制

8.2中所列过程应包括对人力资源管理的控制，以及适当时对与安全有关的设备、仪器和信息技术项目的设计、安装、运行、整修和调整。如果对现有的安排进行了改变，或引入了可能对安全管理产生影响的新安排，组织应在实施之前考虑相关的安全相关风险。要考虑的新的或改变的安排应包括：

a) 修订组织结构、岗位或责任；

b) 培训、意识和人力资源管理；

c) 修订安全管理方针、目标、指标或方案；

d) 修订过程和程序；

e) 引入新的基础设施、安全设备或技术，其中可能包括硬件和/或软件；

f) 适当时引进新的承包商、供方或人员；

g) 对外部供方的安全保证要求。

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。

组织应确保与安全管理体系相关的外部提供的过程、产品或服务得到控制。

8.4 控制

(1)8.2 中所列过程应包括对人力资源管理的控制，以及适当时对与安全有关的设备、仪器和信息技术项目的设计、安装、运行、整修和调整。

(a)**人力资源管理的控制：**人力资源管理控制应包括员工的选拔、培训、考核、激励以及行为监控等方面，确保员工具备相应的能力和素质，能够胜任与安全相关的工作；

(b)安全相关设备、仪器的控制：

——**设备控制的目的：**对与安全有关的设备、仪器进行全面的控制，旨在确保这些设备、仪器在设计、安装、运行、整修和调整等各个环节都符合安全要求，从而有效预防和控制安全风险；

——控制内容：

- **设计控制：**确保设备、仪器在设计阶段就考虑到安全因素，遵循相关标准和规范，具备必要的安全功能；
- **安装控制：**在安装过程中，确保设备、仪器按照设计要求和操作规范进行安装，防止安装不当引发的安全问题；
- **运行控制：**制定设备、仪器的操作规程和运行标准，确保其在运行过程中处于受控状态，及时发现和处理异常情况；
- **整修和调整控制：**定期对设备、仪器进行整修和调整，确保其性能和安全状态符合要求，防止因设备老化或损坏引发的安全风险。

(2)如果对现有的安排进行了改变，或引入了可能对安全管理产生影响的新安排，组织应在实施之前考虑相关的安全相关风险；

(a)变更与新安排的考虑背景；

——**组织动态性：**组织在运营过程中，可能会因为业务需求、技术进步或其他因素而对现有的管理安排进行变更，或引入新的安排；

——**安全管理影响：**这些变更和新安排可能会对组织的安全管理产生直接或间接的影响，从而增加安全风险。

(b)安全风险评估的必要性

——**预防原则：**组织在实施变更或新安排之前，应进行全面的安全风险评估，以便及时发现潜在的安全风险；

——**风险评估范围：**评估范围应涵盖变更或新安排可能对安全管理体系的各个方面产生的影响，包括但不限于人力资源、设备、过程等。

(c)安全风险评估的内容。

——**风险识别**：通过收集和分析相关信息，识别变更或新安排可能带来的具体安全风险。

——**风险分析**：对识别出的安全风险进行分析，确定其发生的可能性和潜在后果的严重程度。

——**风险评价**：根据分析结果，对安全风险进行优先排序，以便合理分配资源和管理精力。

(3)要考虑的新的或改变的安排应包括：

(a)修订组织结构、岗位或责任；

——**必要性**：随着组织的发展或业务环境的变化，可能需要修订组织结构、岗位设置或相关职责，以适应新的安全管理需求；

——**影响**：修订涉及组织结构、岗位或责任时，需评估这些变化对安全管理体系的影响，确保安全责任明确、过程流畅。

(b)培训、意识和人力资源管理；

——**培训与意识提升**：随着安全管理要求的变化，需对相关人员进行必要的培训，提升其对新要求的理解和掌握；

——**人力资源管理**：根据安全管理需要，调整人力资源管理措施，确保人员能力与岗位要求相匹配。

(c)修订安全管理方针、目标、指标或方案；

——**方针与目标的调整**：根据组织安全状况的变化和外部要求，及时更新安全管理方针和目标，确保其与组织战略相一致；

——**指标与方案的优化**：对安全管理指标和方案进行定期评审和优化，确保其有效性和适用性。

(d)修订过程和程序；

——**流程优化**：随着安全管理实践的深入，需对现有的安全管理过程和程序进行修订，以提高其效率和效果；

——**程序更新**：确保安全管理程序符合最新的法律法规和标准要求，避免因程序过时而引发的安全风险。

(e)引入新的基础设施、安全设备或技术，其中可能包括硬件和/或软件；

——**硬件与软件更新**：根据需要引入新的基础设施、安全设备或技术，以提升组织的安全保障能力；

——**评估与测试**：对新引入的基础设施、设备或技术进行全面的评估和测试，确保其性能稳定、安全可靠。

(f)适当时引进新的承包商、供方或人员；

——**评估与筛选**：对新引入的承包商、供方或人员进行严格的评估和筛选，确保其具备相应的资质和能力，满足组织的安全管理要求；

——**合作与协调**：与新引入的承包商、供方或人员建立有效的合作关系，明确双方在安全管理方面的责任和义务，确保合作顺畅。

(g)对外部供方的安全保证要求。

——**要求明确**：与外部供方建立明确的安全保证要求，确保其在提供产品或服务时符合组织的安全管理标准；

——监控与评审：定期对外部供方的安全管理绩效进行监控和评审，确保其持续满足组织的安全管理要求。

(4)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；

(a)策划变更的控制；

——**变更的必要性：**随着组织的发展、市场环境的变化以及法律法规的更新，组织可能需要对其安全管理体系进行变更以适应这些变化；

——这些需策划的运行变更主要包括但不限于以下几个方面：

- **安全管理策略与方针的调整：**随着组织目标、业务范围或外部环境的变化，可能需要调整安全管理策略与方针，以确保其与组织现状和发展方向保持一致；
- **安全目标、指标与方案的更新：**根据组织安全管理绩效的评估结果、内外部审核反馈或业务发展需求，组织可能需要更新安全目标、指标与实施方案，以提升安全管理的针对性和有效性；
- **安全管理过程与程序的优化：**随着安全管理实践的深入和法律法规的更新，组织可能需要优化现有的安全管理过程与程序，以简化流程、提高效率和降低风险；
- **基础设施、设备或技术的引入与更新：**为提升安全管理能力，组织可能需要引入新的基础设施、安全设备或技术，或对现有设施、设备或技术进行更新升级；
- **组织结构、岗位与职责的调整：**随着组织规模的扩大或业务范围的调整，组织可能需要调整组织结构、岗位设置与职责分配，以确保安全管理责任的明确与落实；
- **人员培训与能力提升：**针对新引入的安全管理要求、新技术或新设备，组织可能需要开展相应的培训与能力提升活动，以提升员工的安全意识和操作技能；
- **与外部供方和合作伙伴的关系管理：**当与外部供方或合作伙伴的合作模式、业务范围或技术要求发生变化时，组织可能需要调整相应的安全保证要求和管理措施。

——**控制的重要性：**组织应对策划的变更进行严格的控制，确保变更的实施过程有序、规范，符合组织的战略目标和安全管理体系的要求。

——控制措施。

- 明确变更的目标、范围、时间和资源需求；
- 评估变更对安全管理体系各要素的影响，并制定相应的应对措施；
- 制定详细的变更计划和实施步骤，明确责任人和时间表；
- 监控变更的实施过程，确保变更按照计划进行，并及时调整计划以适应实际情况。

(b)**非预期变更后果的评审；**

——**非预期后果的识别：**在实施变更过程中，可能会出现一些非预期的后果，这些后果可能会对组织的安全管理产生负面影响。组织应对这些非预期后果进行及时的识别；

——**后果的评审：**组织应对识别出的非预期后果进行评审，分析其对安全管理的影响程度和可能带来的风险；

——**风险评估：**基于评审结果，对非预期后果进行风险评估，确定其可能性和潜在影响的大小。

(c)减轻不利影响的措施。

——**制定应对策略：**针对评审出的非预期后果和潜在风险，组织应制定相应的应对策略和措施，以减轻这些后果对安全管理的不利影响；

——**资源分配：**根据应对策略的需要，合理分配资源，确保应对措施的有效实施；

——**持续监控与调整：**在实施应对措施的过程中，组织应持续监控其效果，并根据实际情况及时调整策略和资源分配，以确保非预期后果得到有效控制。

(5)组织应确保与安全管理体系相关的外部提供的过程、产品或服务得到控制。

(a)外部提供过程、产品或服务的定义与范围；

——**定义：**与外部实体（如供方、服务提供方等）合作，由其提供的安全管理体系相关的过程、产品或服务；

——**范围：**这些外部提供的过程、产品或服务可能涉及组织的多个领域，包括但不限于信息安全管理、供应链管理、设施维护等。

(b)全面控制的要求；

——**必要性：**为确保安全管理体系的完整性、有效性和符合性，组织必须对外部提供的过程、产品或服务进行全面控制；

——控制措施。

- 供方评价与选择：建立供方评价与选择机制，确保外部供方具备相应的能力、资质和信誉，能够满足组织的安全管理要求；
- 合同与协议管理：与供方签订明确的合同或协议，明确双方的权利、义务和责任，包括安全要求、质量标准、服务范围等；
- 过程监控与绩效评估：对外部供方提供的过程、产品或服务进行定期监控和绩效评估，确保其符合组织的安全管理要求和质量标准；
- 纠正与改进：针对监控和评估中发现的问题或不足，与供方共同制定纠正和改进措施，并及时跟踪实施效果。

(c)具体控制要点；

——**风险评估：**对外部供方提供的过程、产品或服务进行风险评估，识别潜在的安全风险和隐患，并制定相应的应对措施；

——**资源保障：**确保为外部供方提供必要的资源支持，包括技术支持、培训、信息共享等，以提高其安全管理能力和服务质量；

——**信息共享与沟通：**建立有效的信息共享和沟通机制，确保与外部供方之间的信息畅通，及时传递安全管理要求和标准；

——**持续改进：**与外部供方共同关注安全管理领域的最新发展动态，共同研究改进措施，推动安全管理体系的持续改进。

(d)组织内部责任与协调。

——**明确责任：**在组织内部明确与外部供方合作相关的责任人和部门，确保各项控制措施得到有效执行；

——**跨部门协作：**加强跨部门的协作与沟通，确保外部供方提供的过程、产品或服务能够顺利融入组织的安全管理体系中；

——**定期评审：**定期对外部供方提供的过程、产品或服务进行全面评审，评估其绩效和贡献，并根据评审结果进行相应的调整和优化。

ISO 28000-2022 《安全与韧性—安全管理体系要求》

8 运行

8.5 安全策略、程序、过程和应对方法

8.5.1 确定和选择战略和应对方法

组织应实施并保持系统的程序，以分析与安全有关的脆弱性和威胁。基于这种脆弱性和威胁分析以及随之而来的风险评估，组织应确定并选择一种安全策略，其中包括一个或多个程序、过程和应对方法。

识别的依据应是策略、程序、过程和应对的程度：

a）保持组织的安全；

b）减少安全漏洞的可能性；

c）减少威胁实现的可能性；

d）缩短任何安全处理缺陷的期限并限制其影响；

e）提供充足的资源。

选择应基于战略、过程和应对的程度：

——满足保护组织安全的要求；

——考虑组织可能或不可能承担的风险的数量和类型；

——考虑相关的成本和效益。

8.5.2 资源要求

组织应确定实施所选安全程序、过程和应对方法的资源要求。

8.5.3 应对的实施

组织应实施和保持选定的安全处理。

8.5 安全策略、程序、过程和应对方法

8.5.1 确定和选择战略和应对方法

(1)确定和选择系统分析与选择安全策略、程序、过程和应对方法；

(a)**系统程序实施：**组织应实施并保持一套系统的程序，旨在分析组织中与安全相关的各种脆弱性和威胁；

(b)**脆弱性和威胁分析：**通过系统的分析，组织能够识别出可能影响其安全性的各种脆弱性和潜在威胁，包括但不限于物理或功能故障、恶意行为、环境或人为因素等；

(c)**风险评估：**基于对脆弱性和威胁的分析，组织应进一步进行风险评估，确定这些风险对组织安全可能产生的影响和潜在后果；

(d)**安全策略确定：**在风险评估的基础上，组织应确定并选择一种或多种安全策略，这些策略旨在降低或消除识别出的风险，确保组织安全；

(e)**策略内容涵盖：**安全策略应包含一个或多个具体的程序、过程和应对方法，这些方法可能包括制定预防措施、应急响应计划、安全培训等，以确保组织在面对安全威胁时能够迅速、有效地作出响应。

(2)依据安全保护级别选择战略和应对方法：

(a)**保持组织的安全：**组织选择安全策略、程序、过程和应对方法的首要目标是确保组织的安全。这意味着所采取的措施必须能够有效防止安全事件的发生，或者在事件发生时能够迅速控制并降低其影响；

(b)**减少安全漏洞的可能性：**通过选择适当的安全策略、程序、过程和应对方法，组织应努力减少系统中存在的安全漏洞，从而降低潜在的安全风险；

(c)**减少威胁实现的可能性：**组织应关注降低安全威胁实现的可能性，这包括通过增强防护措施、加强监控和检测能力，以及在发现威胁时能够迅速响应；

(d)**缩短处理缺陷的期限并限制其影响：**一旦发现安全处理存在缺陷，组织应能够迅速采取行动进行修复，并采取措施限制缺陷对组织安全的影响；

(e)**提供充足的资源：**在选择安全策略、程序、过程和应对方法时，组织应确保所需的资源是充足的。这包括人力资源、技术资源、物资资源等，以确保所选方案能够得到有效的实施和维护。

(3)基于战略、风险及成本效益选择安全策略与应对方法。

(a)**战略契合度：**在确定和选择安全策略、程序、过程和应对方法时，首要考虑的是这些方法是否能够满足保护组织安全的需求。所选择的方案应与组织的整体战略方向相一致，确保在组织层面上实现安全防护；

(b)**风险评估：**组织应评估可能或不可能承担的风险的数量和类型。这包括对潜在安全威胁的全面分析，确定风险的可能性和潜在影响。基于这些评估结果，组织可以选择更为针对性的安全策略和方法，以确保资源的有效利用；

(c)**成本效益考虑：**在选择安全策略、程序、过程和应对方法时，组织应考虑相关的成本和效益。组织应在实现安全防护的同时，权衡投入与产出，确保所采取的措施在成本上合理且效益显著。

8.5.2 资源要求

组织应确定实施所选安全程序、过程和应对方法的资源要求：

(1)**资源确定的重要性：**在确定和实施所选的安全程序、过程和应对方法时，组织必须明确所需的资源，以确保这些方法和程序能够有效执行并达到预期的安全效果；

(2)**资源需求的全面分析：**组织应对所需资源进行全面分析，资源是确保安全策略、程序和应对方法顺利实施的基石；

(3)**资源的合理配置：**根据所需资源的重要性和紧迫性，组织应合理配置资源，确保关键安全领域得到足够的资源支持。同时，也应注意资源的合理利用，避免浪费；

(4)**资源需求的持续评估：**随着安全环境和组织状况的变化，组织应持续评估所需资源的变化情况，并及时调整资源分配，以确保安全策略、程序和应对方法的持续有效性；

(5)**资源保障的落实：**组织应确保所需资源的实际保障，包括资源的获取、分配、使用和维护等方面。同时，还应建立相应的监督和考核机制，确保资源使用的合规性和有效性。

8.5.3 应对的实施

(1)**全面实施：**实施过程应当涵盖所有选定的安全处理措施，无论是安全策略的执行、程序的落实、过程的监控还是应对方法的采用，都应得到全面有效的实施；

(2)**保持措施的有效性：**实施安全处理措施后，组织应确保这些措施持续有效。这意味着需要定期对措施的效果进行评估，及时调整或更新，以应对不断变化的安全威胁和环境。

ISO 28000-2022 《安全与韧性—安全管理体系要求》

8 运行

8.6 安全计划

8.6.1 总则

组织应根据选定的战略和应对方法，制定并将安全计划和程序形成文件。组织应实施并保持一个响应结构，以便能够及时有效地警告并向有关方面通报与安全有关的漏洞和迫在眉睫的安全威胁或正在发生的安全违规行为。响应结构应提供计划和程序，以便在迫在眉睫的安全威胁或正在发生的安全违规行为期间管理本组织。

8.6 安全计划

8.6.1 总则

(1)**制定和文件化安全计划与程序：**组织应根据所选的安全战略和应对方法，制定具体的安全计划和程序，并将它们形成书面文档；

(2)**建立响应结构：**组织应实施并保持一个高效的响应结构，以快速、有效地响应安全漏洞、迫在眉睫的安全威胁或正在发生的安全违规行为；

(3)**提供及时的警告和通报：**响应结构应当能够向组织内部和外部相关方及时警告和通报关于任何与安全有关的漏洞、威胁或违规行为。及时的沟通有助于降低潜在风险，减少损失，并维护组织的声誉和客户关系。

(4)**管理安全事件期间的组织运营：**在安全威胁或违规行为发生时，响应结构应提供明确的计划和程序，指导组织如何管理和应对这些事件，包括确保关键业务功能的连续性、保护资产和数据的完整性、协调内外部资源以及与相关方的有效沟通等。。

ISO 28000-2022 《安全与韧性—安全管理体系要求》

8.6 安全计划

8.6.2 响应结构

组织应实施并保持一种结构，确定一个指定的人或一个或多个小组负责应对与安全有关的脆弱性和威胁。指定人员或每个小组的作用和责任以及该人员或小组之间的关系。

应明确确定、沟通和记录团队。

总体而言，各小组应能做到：

a) 评估安全威胁的性质和程度及其潜在影响；

b) 根据预先确定的阈值评估影响，以证明启动正式回应的合理性；

c) 启动适当的安全响应；

d) 策划需要采取的措施；

e) 以生命安全为第一优先，确定优先次序；

f) 监视与安全有关的漏洞的任何变化、威胁者的意图和能力的变化或安全违规行为的影响以及组织的反应；

g) 启动安全应对；

h) 与相关方、当局和媒体沟通；

i) 与沟通管理部门一起为沟通计划做出贡献。对于每个指定的人或团队，应有：

——确定的工作人员，包括具有履行其指定职责的必要职责、权限和能力的候补人员；

——指导其措施的成文程序，包括应对措施的启动、运行、协调和沟通的程序。

8.6.2 响应结构

(1)组织应实施并保持一种高效的安全响应结构；

(a)**建立响应结构：**组织需要建立一个清晰、明确的响应结构，以便在面临与安全有关的脆弱性和威胁时，能够迅速、有效地作出反应。这一结构应包括确定指定的人员或小组，他们负责领导和管理与安全相关的响应活动。

(b)**指定人员或小组的明确责任：**每个被指定的人员或小组应明确知道自己的作用和职责，包括他们在响应过程中的领导角色、协调任务、决策权限等。这有助于确保在紧急情况下，每个人都能够迅速进入角色，高效协作。

(c)**关系界定：**在响应结构中，需要明确指定人员或小组之间的关系，如上下级关系、协作关系等。这有助于促进各小组之间的有效沟通和协作，避免在紧急情况下出现混乱或延误。

(d)**保持响应结构的动态性：**随着组织内外部环境的变化，以及安全威胁的不断演变，响应结构可能需要相应地进行调整和优化。组织应定期评审和更新响应结构，确保其始终能够适应当前的安全需求。

(2)应明确确定、沟通和记录团队。

(a)**明确确定团队：**组织应明确指定一个或多个小组或个人作为安全响应团队，负责应对与安全有关的脆弱性和威胁。这些团队或个人需具备处理紧急安全情况所需的技能、知识和资源；

(b)**有效沟通：**响应团队的角色、职责、权限以及他们之间的关系应得到充分的沟通和理解。这不仅包括团队内部的沟通，也包括与组织内其他相关部门、上级管理层以及外部合作伙伴之间的沟通；

(c)**详细记录：**安全响应团队的相关信息应被详细记录，包括团队成员的姓名、职责、联系方式、培训记录、紧急联络流程等。这些记录应作为组织安全管理文档的一部分，以便在需要时快速查阅和参考

(3)总体而言，各小组应能做到：

(a)评估安全威胁的性质和程度及其潜在影响；

——**威胁性质的分析：**安全响应小组的首要任务是对安全威胁的性质进行全面分析。这包括确定威胁的来源、动机、类型（如物理威胁、信息安全威胁、供应链威胁等），以便准确理解威胁的本质；

——**威胁程度的评估：**在分析威胁性质的基础上，小组需要评估威胁的严重程度。这通常涉及对威胁可能造成的直接和间接损失的量化评估，以及对组织运营和资产安全的影响程度；

——**潜在影响的预测：**除了评估当前的威胁状况外，小组还应预测威胁可能带来的潜在影响。这包括对未来可能发生的连锁反应、对组织声誉的长期损害、法律后果等方面的考虑；

——**科学决策的基础：**全面分析威胁的性质、程度和潜在影响，为安全响应小组提供了科学的决策基础。这有助于小组根据威胁的实际情况制定合适的响应策略，确保响应措施的针对性和有效性。

(b)**根据预先确定的阈值评估影响，以证明启动正式回应的合理性：**

——**阈值设定的重要性：**在安全管理中，为应对各类安全威胁，组织需要预先设定一系列阈值。这些阈值基于组织的风险承受能力、资产重要性、运营需求等因素制定，用于衡量安全威胁的严重程度和潜在影响；

——**影响评估的必要性：**当安全威胁发生时，响应小组需要立即对威胁的性质、程度和潜在影响进行评估。通过全面分析威胁的来源、动机、手段和目标，小组可以准确判断威胁对组织运营和资产安全的实际影响；

——**基于阈值的响应决策：**在完成影响评估后，响应小组需要根据预先设定的阈值来判断是否需要启动正式的响应程序。只有当威胁的影响超过设定的阈值时，才需要采取紧急措施来应对。这一步骤确保了响应措施的合理性和有效性，避免了不必要的资源浪费和过度反应。

(c)启动适当的安全响应；

——**快速响应的重要性：**在面对安全威胁时，及时、快速的响应是减少损失、控制事态发展的关键安全响应小组需要根据评估结果，迅速启动相应的响应措施，确保在第一时间内对威胁做出有效应对；

——**响应措施的适宜性：**响应措施的选择应根据威胁的性质、程度和潜在影响来确定，确保措施的针对性和有效性。这可能包括紧急通知、疏散人员、隔离危险源、启动应急预案等多种措施，小组需要根据实际情况灵活调整；

——**响应执行的协调性：**安全响应的执行需要各小组之间的密切协调和配合。小组之间应建立有效的沟通机制，确保信息的及时传递和共享，同时明确各自的职责和任务，避免出现混乱和延误；

(d)策划需要采取的措施；

——**响应措施策划的必要性：**在确定了安全威胁的性质、程度和潜在影响后，安全响应小组需要精心策划必要的响应措施。这些措施需要针对特定的威胁情况，确保能够有效地控制或消除威胁，保障组织的安全；

——**响应措施的全面性与针对性：**策划的响应措施应全面覆盖威胁可能涉及的各个方面，包括但不限于人员疏散、危险源控制、紧急通知、应急预案启动等。同时，措施应具有针对性，能够针对特定的威胁情况提供最有效的解决方案；

——**措施的可行性评估：**在策划响应措施时，小组需要评估措施的可行性，包括资源、时间、人员等方面的考虑。确保所策划的措施在实际操作中能够得到有效执行，达到预期的效果；

——**记录与沟通：**策划的响应措施应形成书面记录，并与其他相关小组进行充分沟通。确保所有参与安全响应的人员都清楚了解各自的任务和职责，以及需要采取的措施和步骤。

(e)以生命安全为第一优先，确定优先次序；

——**生命安全的首要性：**在面对安全威胁时，保障人员生命安全是首要任务。安全响应小组应始终坚持生命安全优先的原则，确保在任何情况下都能将保障人员生命安全放在首位；

——**优先次序的确定：**安全响应小组需要根据威胁的性质和程度，结合组织的实际情况，确定响应措施的优先次序。优先次序的确定应以保障人员生命安全为第一原则，确保在有限资源和时间内采取最有效的措施；

——**风险评估与决策支持：**在确定响应优先次序时，小组需要进行全面的风险评估，综合考虑威胁的紧迫性、潜在影响的严重性等因素。这有助于小组更准确地把握威胁的实际情况，为制定科学的响应决策提供有力支持。

(f)监视与安全有关的漏洞的任何变化、威胁者的意图和能力的变化或安全违规行为的影响以及组织的反应；

——**监视安全漏洞的变化：**安全响应小组需要持续监视与安全有关的漏洞的任何变化。这包括对已知漏洞的状态跟踪，以及及时发现新出现的漏洞。通过持续监视，小组能够及时发现潜在的安全风险，从而采取相应措施加以防范或应对；

——**关注威胁者的意图和能力变化：**在应对安全威胁的过程中，小组需要密切关注威胁者的意图和能力变化。这包括了解威胁者的动机、目标以及可能采取的行动手段。通过分析威胁者的意图和能力变化，小组能够更准确地预测威胁的发展趋势，为制定和调整响应策略提供有力支持；

——**评估安全违规行为的影响：**安全响应小组需要评估安全违规行为对组织的影响。这包括对违规行为造成的直接和间接损失进行量化分析，以及对组织运营和资产安全的潜在影响进行评估。通过评估违规行为的影响，小组能够更准确地把握组织的实际损失情况，为制定补救措施提供依据；

——**监视组织的反应和应对效果：**在实施安全响应措施的过程中，小组需要持续监视组织的反应和应对效果。这包括对响应措施的执行情况进行跟踪检查，以及对措施的有效性进行评估。通过监视组织的反应和应对效果，小组能够及时发现响应措施中存在的问题和不足，从而及时调整和完善响应策略。

(g)启动安全应对；

——**启动应对的及时性：**一旦确定存在安全威胁，安全响应小组需要迅速启动安全应对措施。这种及时性对于控制威胁的扩散和最小化潜在损失至关重要。小组应具备快速反应的能力，确保在安全事件发生后立即采取相应行动；

——**应对措施的有效性：**启动的安全应对措施必须针对威胁的性质和程度设计，以确保其有效性。这可能包括紧急通知、隔离危险源、启动应急预案、采取技术措施防止数据泄露等。小组应根据实际情况灵活调整应对措施，确保措施能够直接针对威胁的核心问题；

——**监控与反馈机制：**在应对措施实施过程中，小组需要建立监控与反馈机制，持续跟踪应对效果并收集反馈信息。这有助于及时发现应对措施中存在的问题和不足，从而及时调整和完善应对措施，确保应对活动的持续有效性和针对性。

(h)与相关方、当局和媒体沟通；

——**沟通的重要性：**在应对安全事件的过程中，与相关方、当局和媒体的有效沟通至关重要。这有助于确保信息的及时传递，增强各方对事件的理解，减少误解和恐慌，促进问题的快速解决；

——**明确沟通内容：**安全响应小组需要明确沟通的内容，包括安全事件的性质、影响范围、应对措施、进展情况以及预计的解决时间等。确保向相关方提供准确、全面的信息，以便他们做出适当的决策；

——**确保信息的准确性和一致性：**在沟通过程中，安全响应小组需要确保信息的准确性和一致性。避免传递错误或误导性的信息，以免引起不必要的恐慌和混乱；

——**积极回应关切和疑问：**对于相关方、当局和媒体提出的关切和疑问，安全响应小组需要积极回应，提供必要的解释和说明。这有助于增强各方对组织的信任，促进问题的顺利解决；

——**遵守法律法规和道德准则：**在沟通过程中，安全响应小组需要遵守相关的法律法规和道德准则，尊重他人的隐私和权益。避免发布未经证实的信息或散布谣言，以免引发不必要的法律纠纷和道德争议。

(i)确立明确的沟通计划与人员配置，保障响应过程的协调与高效；

(a)**明确指定人员与团队：**对于每个指定的响应小组或团队，应明确确定工作人员，并确保这些人员具备履行其指定职责的必要职责、权限和能力。此外，应为每个小组配备候补人员，以应对可能的人员变动或紧急情况，确保响应的连续性和稳定性；

(b)**成文程序的指导：**为每个响应小组制定详细的成文程序，用以指导他们如何启动、运行、协调和沟通应对措施。这些程序应清晰阐述各项措施的执行步骤、责任人、完成时限等关键要素，以确保响应过程的规范性和高效性；

(c)人员培训与准备：对确定的工作人员进行必要的培训和准备，使他们熟悉并理解安全计划中的沟通策略和响应程序。通过培训，工作人员能够在实际工作中迅速响应，有效执行各项措施，提高组织的整体应急响应能力；

(d)**信息的及时传递与共享：**建立有效的信息传递和共享机制，确保各响应小组之间以及与沟通管理部门之间的信息畅通无阻。通过及时、准确的信息传递，各小组能够保持协同作战，共同应对安全事件，减少潜在损失和风险。

ISO 28000-2022 《安全与韧性—安全管理体系要求》

8.6 安全计划

8.6.3 警告和沟通

组织应将以下程序形成文件并加以保持：

a) 向相关方进行内部和外部沟通，包括沟通的内容、时间、对象和方式；

注：组织应将如何以及在何种情况下与员工及其紧急联系人进行沟通的程序形成文件并加以保持。

b) 接收、记录和回应相关方的沟通，包括任何国家或区域风险咨询系统或同等机构；

c) 确保在违反安全规定、出现漏洞或威胁时沟通方式的可用性；

d) 促进与安全威胁和/或违法行为应对者的结构化沟通；

e) 提供组织在发生安全违规事件后对媒体反应的细节，包括沟通策略；

f) 记录违反安全规定的细节、采取的措施和作出的决定。

在适用的情况下，还应考虑和实施以下内容：

——提醒可能受到实际或即将发生的安全违规行为影响的相关方；

——确保多个应对组织之间的适当协调和沟通。警告和通信程序应作为组织测试和培训计划的一部分进行演练。

8.6.3 警告和沟通

(1)组织应将以下程序形成文件并加以保持：

(a)向相关方进行内部和外部沟通，包括沟通的内容、时间、对象和方式；

——**沟通内容：**组织应明确沟通的信息范围，确保信息的准确性和完整性；

——**沟通时间：**应确定何时进行沟通，以保证信息的及时传递；

——**沟通对象：**组织应识别并确定与哪些内部或外部的相关方进行沟通；

——**沟通方式：**选择适当的沟通渠道和方法，以确保信息能够有效传达。

注：组织应特别关注与员工及其紧急联系人的沟通程序，并将这些程序详细记录成文件。这包括但不限于紧急情况下的通知程序，确保在必要时能够快速有效地联系到员工或其指定的紧急联系人。

(b)接收、记录和回应相关方的沟通，包括任何国家或区域风险咨询系统或同等机构；

——**接收沟通：**组织应确保有一个有效的机制来接收来自相关方的沟通，包括任何来自国家或区域风险咨询系统或同等机构的信息。这些信息可能涉及最新的安全风险、预警或其他与安全相关的重要通知；

——**记录沟通：**对于接收到的每一条沟通信息，组织都需要详细记录。记录内容包括但不限于沟通的时间、来源、内容、涉及的风险或问题等；

——**回应沟通：**组织需要及时回应收到的沟通信息。回应内容应针对沟通中提出的问题或风险，提供适当的解决方案或建议，或者明确下一步的行动计划。

(c)确保在违反安全规定、出现漏洞或威胁时沟通方式的可用性；

——**违反安全规定时：**当组织内部或供应链上发生违反安全规定的行为时，组织应确保沟通方式畅通无阻，以便及时报告和应对这些违规行为；

——**出现安全漏洞时：**组织应有一个迅速响应安全漏洞的机制，包括确保在发现漏洞时能够立即通知相关人员和启动应急计划；

——**面临安全威胁时：**当组织面临外部安全威胁时，如网络攻击、恐怖袭击等，组织应能够迅速有效地与所有相关方沟通，传达威胁的性质、潜在影响和应对措施。

(d)促进与安全威胁和/或违法行为应对者的结构化沟通；

——**结构化沟通的重要性：**组织在与负责应对安全威胁和违法行为的组织或个人进行沟通时，应采用结构化的沟通方式；

——**明确的沟通框架：**结构化沟通应包括明确的沟通框架，如预定的沟通渠道、沟通内容模板、定期或不定期的会议安排等；

——**促进信息共享和协作：**通过结构化沟通，组织可以与应对者共享关键信息，如安全漏洞的详细情况、潜在影响、已采取的应对措施等。同时，也可以促进各方之间的协作，共同制定和执行应对计划。

(e)提供组织在发生安全违规事件后对媒体反应的细节，包括沟通策略；

——**媒体反应的重要性：**在发生安全违规事件时，组织应迅速且有效地与媒体进行沟通，以维护组织声誉，避免不实信息的传播，同时确保公众能够及时了解到真实情况；

——**详细的媒体反应程序：**组织应预先制定一套详细的媒体反应程序，明确在事件发生后应如何与媒体进行沟通，包括但不限于确定发言人、准备媒体声明、组织新闻发布会等；

——**明确的沟通策略：**组织应制定明确的沟通策略，包括确定沟通的重点内容、选择合适的沟通渠道、掌握沟通的节奏和语气等。沟通策略的制定应基于事件的具体情况，以确保信息的准确传达和组织的良好形象。

(f)记录违反安全规定的细节、采取的措施和作出的决定。

——**记录安全违规事件的细节：**当组织内部或供应链中发生违反安全规定的事件时，组织应详细记录事件的经过、涉及的人员、时间、地点等关键信息；

——**记录采取的应对措施：**在发生安全违规事件后，组织应及时采取必要的应对措施以控制风险、减少损失。这些措施可能包括紧急处置、调查取证、责任追究等。组织需要记录采取的每一项措施，以便于后续评估措施的有效性，并为类似事件的应对提供参考；

——**记录作出的决策：**在应对安全违规事件的过程中，组织可能需要作出一些关键决策，如确定责任人、调整安全策略、改进管理制度等。这些决策对于事件的最终解决和组织的长期发展具有重要意义。组织应详细记录这些决策的过程和结果，以便于后续的审查和追责。

(2)在适用的情况下，还应考虑和实施以下内容：

(a)提醒可能受到实际或即将发生的安全违规行为影响的相关方；

——**识别潜在受影响的相关方：**组织在面临安全违规风险时，应识别出那些可能直接或间接受到影响的相关方，可能包括供应链的上游和下游企业、客户、合作伙伴、政府部门或社区居民等；

——**评估影响的性质和程度：**组织应对安全违规行为可能给相关方带来的影响进行评估，包括潜在的经济损失、声誉损害、法律责任等；

——**确定提醒的方式和时机：**组织应根据评估结果，确定向相关方提醒的方式和时机。提醒可以通过书面通知、电子邮件、电话或会议等形式进行，确保信息能够及时、准确地传达给相关方；

——**提供必要的指导和支持：**在提醒的同时，组织还应向相关方提供必要的指导和支持，如应对措施建议、资源协调等，以帮助相关方降低潜在影响，共同应对安全违规风险。

(b)确保多个应对组织之间的适当协调和沟通。警告和通信程序应作为组织测试和培训计划的一部分进行演练。

——确保多个应对组织之间的适当协调和沟通：

- **多组织协同的重要性：**在安全违规行为或事件发生时，往往需要多个组织共同应对，包括内部部门、外部供应商、政府部门、安全机构等。确保这些组织之间能够进行有效的协调和沟通，对于提高应对效率、减少损失至关重要；
- **建立协调沟通机制：**组织应建立一套明确的协调沟通机制，如设立联合指挥部、定期召开协调会议、建立信息共享平台等，以确保信息在多个组织之间能够及时、准确地传递；
- **明确职责与分工：**在多组织协同应对的过程中，明确各组织的职责和分工，避免重复工作或责任不清的情况发生，提高应对工作的针对性和有效性。

——警告和通信程序应作为组织测试和培训计划的一部分进行演练。

- **测试与演练的必要性：**为了确保在实际应对过程中能够熟练运用警告和通信程序，组织应将其作为测试和培训计划的一部分进行定期演练。这有助于发现程序中的不足或问题，并及时进行改进和完善；
- **模拟实际场景：**在演练过程中，组织应模拟实际的安全违规行为或事件场景，以检验应对程序的可行性和有效性。同时，通过演练还可以提高相关人员的应对能力和团队协作能力；
- **总结与反馈：**演练结束后，组织应对演练过程进行总结和反馈，分析演练中存在的问题和不足，并制定相应的改进措施。这有助于持续提升组织的应对能力和通信程序的有效性。

ISO 28000-2022 《安全与韧性—安全管理体系要求》

8.6 安全计划

8.6.4 安全计划的内容

组织应安全计划形成文件并加以保持。这些计划应提供指导和信息，以协助团队应对安全漏洞、威胁和/或违规行为，并协助组织进行应对和恢复其安全。

总的来说，安全计划应包含：

a) 各小组将采取的措施的细节，以：

1）继续或恢复商定的安全状态；

2）监视实际或即将发生的安全威胁、漏洞或违规行为的影响以及组织对其的反应；

b) 参照预设的阈值和启动反应的过程；

c) 恢复组织安全的程序；

d) 管理安全漏洞和威胁或实际或即将发生的安全侵犯行为的直接后果的细节，并适当考虑到：

1）个人的福利；

2）可能受到损害的资产、信息和人员的价值；

3）防止核心活动的（进一步）损失或不可用。

每个计划都应包括：

——其目的、范围和目标；

——实施该计划的团队的作用和责任；

——实施解决方案的措施；

——启动(包括启动标准）、运行、协调、和沟通团队行动所需的信息；

——内部和外部的相互依存关系；

——其资源需求；

——其报告要求；

——退出过程。

每个计划都应是可用的，并在需要的时间和地点提供。

8.6.4 安全计划的内容

(1)组织应安全计划形成文件并加以保持。这些计划应提供指导和信息，以协助团队应对安全漏洞、威胁和/或违规行为，并协助组织进行应对和恢复其安全；

(a)**文件化安全计划的重要性：**组织需要制定详细的安全计划，并将其形成文件加以保持，以确保计划的一致性和可追溯性；

(b)**计划的指导性和信息性：**安全计划应为组织应对各种安全挑战提供明确的指导和信息。计划应涵盖对安全漏洞、威胁和违规行为的识别、评估、响应和恢复措施，以确保组织能够快速、有效地应对这些挑战；

(c)**支持组织的应对和恢复：**安全计划不仅为团队提供应对安全挑战的指导，还应支持组织在发生安全事件后进行恢复。计划应包含恢复策略和措施，以确保组织在遭受攻击或发生安全事件后能够迅速恢复正常运营状态。

(2)总的来说，安全计划应包含：

(a)各小组将采取的措施的细节，以：

——**继续或恢复商定的安全状态：**安全计划应明确各小组在发生安全事件后，如何继续或恢复到原先商定的安全状态的具体措施和步骤。这包括恢复关键服务和功能，确保业务连续性等；

——**监视实际或即将发生的安全威胁、漏洞或违规行为的影响：**安全计划需要详细列出各小组如何持续监视实际或即将发生的安全威胁、漏洞或违规行为可能对组织产生的影响。这涉及对潜在风险的识别、分析和评估，以及及时采取应对措施以减少或消除这些风险；

——**监视组织对其的反应：**安全计划还包括如何监视组织对这些威胁和违规行为的反应。这包括评估应对措施的有效性，及时调整策略以更好地应对变化的情况，以及确保所有相关方都能够了解并遵循最新的安全指南和程序。

(b)参照预设的阈值和启动反应的过程；

——**预设的阈值：**组织应设定一系列预设的阈值，这些阈值是用于评估安全威胁、漏洞或违规行为的性质和程度及其潜在影响的标准。当安全事件达到或超过这些阈值时，组织将启动相应的安全响应程序。预设的阈值应基于组织的特定情况、风险评估结果以及可接受的风险水平来制定；

——**启动反应的过程：**安全计划应详细描述当达到预设阈值时启动反应的具体过程。这包括确定启动反应的标准、启动安全响应的授权机制、如何通知相关团队和人员、以及应急响应团队的行动指南等。启动反应的过程应确保快速、准确和有效地响应安全事件，最大程度地减少潜在的损害和损失。

(c)恢复组织安全的程序；

(a)**程序的重要性：**恢复组织安全的程序是安全计划中不可或缺的一部分。它规定了组织在遭受安全威胁、漏洞或违规行为后应采取的具体步骤和措施，以确保在最短时间内恢复关键服务和功能，减少业务中断和潜在损失；

(b)**程序的内容：**恢复组织安全的程序应详细列出在发生安全事件后需要采取的所有必要步骤。这包括但不限于：

——**评估损失和影响：**组织应评估安全事件对业务、资产和声誉造成的具体损失和影响，以便制定有效的恢复计划；

——**制定恢复策略：**基于评估结果，组织应制定详细的恢复策略，明确恢复的目标、优先级、时间表和所需资源；

——**实施恢复措施：**组织应按照恢复策略，逐步实施各项恢复措施，包括恢复关键服务和功能、修复受损系统和设备、更新安全策略等；

——**验证和测试：**在恢复过程中，组织应对已实施的恢复措施进行验证和测试，确保其有效性和可行性；

——**持续改进：**组织应根据恢复过程中的经验和教训，对恢复程序进行持续改进和优化，以提高未来应对类似事件的能力。

(c)**程序的灵活性和适应性：**恢复组织安全的程序应具有足够的灵活性和适应性，以便在应对不同类型、规模和复杂度的安全事件时能够根据实际情况进行调整和优化。

(d)管理安全漏洞和威胁或实际或即将发生的安全侵犯行为的直接后果的细节，并适当考虑到：

——**直接后果的管理：**安全计划必须包含详细的管理策略，用于应对安全事件带来的直接后果。这些后果可能包括财务损失、声誉损害、业务中断、人员伤亡等；

——考虑因素。

- **个人的福利：**在安全事件处理过程中，组织应首先确保受影响的个人（如员工、客户等）的安全和福利。这可能包括提供紧急援助、医疗救助和心理支持等；
- **资产、信息和人员的价值：**组织应评估并考虑可能受到损害的资产（如物理资产、知识产权等）、信息的价值以及人员的重要性。这有助于确定资源分配和恢复工作的优先级；

- **防止核心活动的损失或不可用：**核心活动的连续性和可用性对组织的运营至关重要。因此，安全计划应着重考虑如何快速恢复关键业务功能，减少因安全事件导致的业务中断时间。

(3)每个计划都应包括：

(a)目的、范围和目标；

——**目的：**明确该安全计划的主要意图，即为了应对何种类型的安全事件；

——**范围：**界定安全计划适用的具体领域、部门或过程；

——**目标：**设定实施该计划后期望达到的具体结果或成效。

(b)实施团队的作用和责任：

——**作用：**阐述实施该计划的团队在响应和恢复过程中的主要功能和角色；

——**责任：**分配给每个团队成员或小组的具体职责和任务。

(c)**实施解决方案的措施：**详细描述为实现安全计划目标所采取的具体措施和方法，包括步骤、策略、工具等；

(d)启动、运行、协调和沟通所需的信息；

——**启动：**包括启动计划的标准和条件；

——**运行：**描述计划实施过程中的关键步骤和流程；

——**协调：**明确不同团队或部门之间的协作和配合机制；

——**沟通：**规定计划实施过程中的内外部沟通渠道和方式。

(e)**内部和外部的相互依存关系：**分析计划实施过程中可能涉及的内部和外部实体（如供应商、合作伙伴、政府部门等）之间的依存关系，并明确各自的职责和角色；

(f)**资源需求：**列出实施计划所需的所有资源，包括人力、物力、财力、时间等，并明确资源的来源和分配方式；

(g)**报告要求：**规定计划执行过程中的报告频率、内容、格式和提交对象，确保管理层和相关方能够及时了解计划执行情况和效果；

(h)**退出过程：**描述安全事件得到妥善处理、组织恢复正常运营后，如何有序地退出安全计划实施阶段，并进行总结和评估。

(4)每个计划都应是可用的，并在需要的时间和地点提供。

(a)每个计划都应是可用的；

——**可用性定义：**安全计划应当处于随时可用的状态，计划应当是完整、最新且易于获取的。组织应确保其安全计划随时处于准备状态，以便在需要时能够迅速实施；

——**计划维护：**组织应定期对安全计划进行审查和更新，以确保其内容与组织的当前环境、需求和目标保持一致。同时，组织还应确保所有相关人员都了解并熟悉安全计划的内容。

(b)在需要的时间和地点提供。

——**在需要的时间提供：**安全计划的实施往往具有时间敏感性，因此组织应确保计划能够在需要的时间点迅速启动。这要求组织在计划中明确规定启动条件、响应时间和紧急情况下的决策流程；

——**在需要的地点提供：**考虑到组织可能面临的各种安全事件可能发生在不同的地点，组织应确保安全计划能够适应不同的场景和地点。这包括制定适应不同地域、设施和业务部门的定制化计划，以及确保计划所需的资源能够在所需地点及时提供。

ISO 28000-2022 《安全与韧性—安全管理体系要求》

8.6 安全计划

8.6.5 恢复

组织应具有文件化的过程，以从安全违规之前、期间和之后采取的任何临时措施中恢复组织的安全。

8.6.5 恢复

(1)组织应具有文件化的恢复过程；

(a)**文件化的必要性：**为了确保恢复工作的有序性和可重复性，组织必须制定并文件化其恢复过程。这意味着恢复工作不应仅依赖于个人经验或口头指导，而应有一个明确、详细的文件作为指导和参考；

(b)**恢复过程的内容：**恢复过程应涵盖从安全违规事件发生前、发生时到发生后的所有阶段。它应包括在事件发生前采取的预防措施、事件发生时采取的紧急响应措施，以及事件发生后进行的恢复和重建措施。

(2)恢复组织的安全；

(a)**恢复的目标：**恢复过程的核心目标是使组织的安全状态恢复到事件发生前的水平，甚至更好。这意味着组织需要全面评估安全违规事件对组织安全的影响，并采取适当的措施来消除这些影响，恢复组织的正常运营和安全状态；

(b)**采取的措施：**为了实现这一目标，组织可能需要采取一系列的措施，如修复受损的设备、更新安全系统、加强内部控制、重新评估风险管理策略等。这些措施应根据组织的具体情况和事件的影响程度来确定。

(3)临时措施的处理：

(a)**临时措施的定义：**在安全违规事件发生前、期间和之后，组织可能会采取一些临时措施来应对紧急情况或减轻损失。这些措施可能是临时的、短期的，但同样对组织的恢复和安全至关重要；

(b)**从临时措施中恢复：**组织需要确保在采取临时措施后，能够有序地从这些措施中恢复过来，使组织的安全状态重新回到正常轨道。这可能需要组织在事件后进行全面的审查和评估，以确定哪些临时措施是有效的、哪些需要改进或替换。

ISO 28000-2022 《安全与韧性—安全管理体系要求》

9 绩效评价

9.1 监视、测量、分析和评价

组织应确定：

——需要监视和测量什么；

——需要用什么方法进行监视、测量、分析和评价（如适用），以确保结果有效；

——何时实施监视和测量；

——何时对监视和测量的结果进行分析和评价。

组织应保留适当的成文信息，以作为结果的证据。

组织应评价安全管理体系的绩效和有效性。

9 绩效评价

9.1 监视、测量、分析和评价

(1)与监视、测量、分析和评价有关的术语；

(a)监视

确定体系、过程或活动的状态。

——**监视定义：**指确定安全管理体系、安全相关的过程或活动的状态，以确保这些体系、过程或活动是否达到了预期或规定的绩效和安全水平；

——**目的：**在于识别安全管理体系、过程或活动状态的变化，及时发现与安全相关的潜在问题或偏离安全目标的情况，从而及时采取措施进行纠正或改进，以保障组织的安全；

——**监视可以通过多种方法实现，**包括但不限于：

- **持续的检查：**对安全管理体系、过程和活动的日常或定期评估，以确保其状态符合预期；
- **监督：**通过特定的监控机制或系统，实时跟踪安全管理体系的运行情况；
- **严格观察：**对特定活动或过程进行详细观察，以获取其运行状态的第一手资料；
- **确定状态：**使用测量工具或技术，对安全管理体系、过程或活动的关键绩效指标进行测量和评估。

——**应用范围：**监视的应用范围广泛，可以适用于整个安全管理体系，也可以针对特定的安全相关过程或控制活动进行。通过全面的监视，组织可以及时了解其安全管理体系的运行状态，确保其始终处于受控状态，从而有效管理和降低安全风险。

(b)测量

确定数值的过程

——**测量的定义：**测量被定义为确定数值的过程。这个数值通常是量值，用于描述安全管理体系、安全相关的过程或活动的具体特性或状态。测量活动是获取定量数据的基础，对于确保安全管理体系的有效性和符合性至关重要。

——**测量的应用场景：**测量在安全管理体系的多个环节中发挥着重要作用。它有助于组织量化安全风险、监控关键安全参数、确保符合安全标准或要求，并评估控制措施的有效性。通过测量，组织可以更加准确地了解安全管理体系的运行状态，从而及时采取必要的纠正措施或改进策略；

——**测量的类型：**测量可以分为定量测量和定性测量两种类型：

- **定量测量：**使用数值来描述安全管理体系、过程或活动的具体特征或状态。例如，使用经校准或验证的设备来测量有害物质的暴露量、安全设施的性能参数等。定量测量能够提供准确、可比较的数据，有助于组织做出基于事实的决策；
- **定性测量：**通过描述性信息来评估安全管理体系、过程或活动的状态。虽然定性测量不直接使用数值，但它仍然是一种重要的数据收集方法。例如，通过对安全文化的问卷调查、对安全事件的描述性分析等，组织可以了解员工对安全管理的态度、安全事件的影响等方面的信息。

——**测量与监视的区别：**虽然监视和测量都涉及对安全管理体系、过程或活动的状态的检查，但二者之间存在明显的区别。

- 监视主要关注对状态的观察或检查，以确定是否达到预期或规定的绩效和安全水平。监视可能涉及对控制措施执行情况的检查、对关键活动的观察等；
- 测量则涉及确定具体的数值或量值，用于描述安全管理体系、过程或活动的具体特征或状态。测量能够提供更精确、可量化的数据，有助于组织进行更深入的分析和决策。

监视与测量的区别说明表

特征	监视	测量
定义	确定安全管理体系、安全相关的过程或活动的状态，以确保其达到预期或规定的绩效和安全水平。	确定数值的过程，这个数值通常是量值，用于描述安全管理体系、安全相关的过程或活动的具体特性或状态。
目的	识别体系、过程或活动状态的变化，及时发现与安全相关的潜在问题或偏离目标的情况，从而采取措施进行纠正或改进。	量化安全风险、监控关键安全参数、确保符合安全标准或要求，评估控制措施的有效性。
方法	- 持续的检查 - 监督 - 严格观察 - 确定状态（使用测量工具或技术）	- 定量测量：使用数值描述特征或状态 - 定性测量：通过描述性信息评估状态
应用场景	适用于整个安全管理体系或特定过程/控制活动。	在安全管理体系的多个环节发挥作用，尤其是在需要量化数据和评估状态的情况下。
主要关注	状态的变化和是否符合预期。	确定具体的数值或量值，提供可量化的数据。
数据类型	通常不涉及具体数值，关注整体状态和符合性。	提供定量或定性的数据，有助于深入分析和决策。
输出	对体系、过程或活动状态的观察结果和符合性判断。	具体的数值或描述性信息，用于量化评估和决策支持。

(c)分析

为提供有效的决策基础而对事实和数据的验证。

——**与监视和测量活动结果的关联：**在安全管理体系中，分析经常与监视和测量活动所获得的数据直接相关。这些数据为分析提供了基础和来源，帮助组织了解当前的安全状况、风险状况和绩效水平；

——**确定因果关系、模式和趋势：**分析的核心目的是通过仔细检查这些数据来揭示其中可能存在的因果关系、隐藏的规律或未来的发展趋势。这有助于组织更好地理解安全风险的本质，预测可能的安全事件，并据此制定有效的应对措施；

——**可能涉及统计运算：**为了从数据中得出更准确的结论，分析过程可能涉及复杂的统计运算。例如，回归分析可以帮助组织确定不同因素之间的影响关系；方差分析可以用于比较不同条件下的安全绩效差异。这些统计方法有助于提升分析的准确性和可靠性；

——**使用外部信息：**在分析过程中，组织可能会使用来自其他类似组织的信息或历史数据进行比较和参考。这种外部信息可以为组织提供宝贵的安全管理实践经验和行业最佳实践，有助于组织在构建和持续改进其安全管理体系时吸收和学习；

——**针对安全管理绩效的评价：**在安全管理体系中，分析是评价组织安全管理绩效的重要手段。通过分析监视和测量活动所收集的数据，组织可以评估当前的安全状况、风险状况和绩效水平，识别存在的问题和潜在的改进机会，并据此制定相应的改进措施和计划。

(d)评价

将评测结果与既定指标相对比，确定预期绩效与实际绩效之间差异的系统化过程

——**评价的定义：**评价涉及将实际的安全管理绩效与预定的安全标准或指标进行对比，以识别和量化两者之间的差异；

——**评价的目的：**通过评价，组织可以了解安全管理体系的实际运行效果，判断其是否达到了预期的安全目标，并识别出需要进一步关注和改进的领域；

——**评价的内容：**评价可以涵盖安全管理体系的各个方面，包括但不限于风险评估的准确性、安全策略的有效性、控制措施的执行情况、法律法规的遵守状况、供应链管理中的安全水平等；

——**评价的方法：**组织可以采用多种方法进行安全管理评价，如检查表、绩效指标监测、内部审核、管理评审等。这些方法可以帮助组织系统地收集和分析相关数据，从而做出客观、准确的评价；

——**绩效差异的作用：**绩效差异是评价过程中识别出的实际绩效与预期绩效之间的差距。这些差异为组织提供了宝贵的改进机会，组织可以基于这些差异制定针对性的改进措施，以提高安全管理绩效，确保组织的安全和韧性；

——**持续改进的依据：**绩效差异是组织实现持续改进的重要依据。通过评价，组织可以持续识别安全管理中的不足和潜力，不断寻求改进和创新，以确保安全管理体系的持续有效性和适应性。

(e)绩效评价

绩效评价是组织为确保其安全管理体系在实现所设定的安全方针和目标方面的适宜性、充分性和有效性而进行的一项综合性活动。

——**适宜性：**绩效评价首先关注安全管理体系是否与组织的特定环境、运营模式和业务需求相匹配，能否有效支撑组织实现其安全相关的目标和愿景；

——**充分性**：绩效评价进一步评估安全管理体系是否得到全面实施，各项控制措施是否充足且恰当，以确保体系能够充分发挥其在预防安全事故、减轻安全威胁和降低安全风险等方面的作用；

——**有效性**：绩效评价的核心在于评价安全管理体系是否正在实现其预期的安全绩效，这包括减少安全事故的发生、提高组织的安全响应能力、增强供应链的韧性等方面，以及组织在安全管理方面取得的持续改进成果。

(2)组织应建立、实施和保持用于监视、测量、分析和评价绩效的过程，包括：

(a)需要监视和测量什么；

——**监视与测量的内容确定**：组织应明确在安全管理体系运行过程中需要监视和测量的具体内容和指标。这包括但不限于：

- **安全方针的执行情况**：安全方针是组织安全管理的指导原则，组织应监视其成员是否严格遵循并执行安全方针，确保安全管理的一致性和有效性；
- **安全目标的达成情况**：组织应监视安全管理体系中设定的安全目标是否按时、按质达成，这是评价安全管理效果的重要指标；
- **法律法规的遵守情况**：组织应监视自身活动是否遵守了相关的法律法规和安全标准，确保组织运营的合规性；
- **供应链中的安全风险**：针对供应链中的各个环节，组织应监视和评估潜在的安全风险，包括供应商的安全状况、物流过程中的安全控制等；
- **安全事故和违规行为**：组织应密切关注安全事故的发生情况，包括事故发生的频率、原因以及造成的后果，同时也要监视和评估组织内部是否存在违反安全规定的行为；
- **安全培训和教育效果**：对于组织内部的安全培训和教育活动，组织应监视其效果，确保员工具备必要的安全知识和技能；
- **安全设备和设施的运行状态**：组织应定期检查和维护安全设备和设施，确保其处于良好的运行状态，能够有效预防和应对安全事故；
- **安全管理的持续改进情况**：组织应监视自身在安全管理方面的持续改进情况，包括改进措施的实施效果、是否存在新的改进机会等。

——**确定监视与测量的目的**：旨在实时获取安全管理体系运行的状况数据，确保安全管理活动的有效性和合规性；

——**设定具体指标**：为了量化监视和测量的结果，组织应设定具体的绩效指标，如安全事故率、安全培训覆盖率、安全设备完好率等。

(b)需要用什么方法进行监视、测量、分析和评价（如适用），以确保结果有效；

——**方法的适用性**：组织在选择监视、测量、分析和评价方法时，应确保其适用性。这意味着所选方法应能够准确反映安全管理体系的绩效，并提供可靠和有效的结果；

——**方法的多样性**：组织可以采用多种方法进行监视、测量、分析和评价，包括但不限于以下几种类型：

绩效监视、测量、分析和评价方法及其应用说明

项目	方法	监视、测量、分析和评价涵义	监视、测量、分析和评价方法应用说明
绩效监视	定期巡检	定期对组织的安全管理活动进行实地查看和检查，以确保各项措施得到有效执行	组织应制定巡检计划，明确巡检频率和覆盖范围，并对巡检结果进行记录和反馈
	关键控制点监控	对安全管理过程中的关键控制点进行实时监控，以确保关键活动的有效性和合规性	识别并确定关键控制点，建立监控机制，定期分析监控数据，及时采取措施解决问题
	安全事件日志分析	对安全事件日志进行分析，识别潜在的安全问题和风险	收集安全事件日志，建立分析流程，定期分析日志数据，提取有价值的信息，为安全决策提供支持
绩效测量	安全指标统计	收集和统计与安全相关的各种指标数据，如事故率、违规次数等，以量化评估安全管理绩效	确定关键的安全指标，建立数据收集和分析流程，定期报告统计结果，分析指标变化趋势
	关键绩效指标（KPI）跟踪	跟踪关键绩效指标的变化情况，以评估安全管理活动的成果和效果	设定具体的 KPI 指标，明确测量方法和标准，定期跟踪指标完成情况，分析影响因素，制定改进措施
绩效分析	根本原因分析（RCA）	对安全事故或问题进行深入分析，找出导致问题的根本原因	建立 RCA 流程，采用适当的分析工具和方法，对问题进行彻底分析，提出针对性的改进措施
	趋势分析	分析安全管理数据的变化趋势，预测未来可能出现的问题和风险	收集历史数据，运用统计方法和趋势分析工具，分析数据变化趋势，为安全管理提供预警和决策支持
	比较分析	将当前安全管理绩效与基准、历史数据或其他组织进行比较，以评估自身绩效水平	确定比较对象和比较指标，收集相关数据，进行对比分析，识别自身优势和不足，制定改进策略
绩效评价	内部审核	定期对组织的安全管理体系进行内部审核，评价其符合性和有效性	制定内部审核计划，明确审核范围、方法和要求，实施审核并出具审核报告，提出改进建议并跟踪验证
	管理评审	高层管理者定期对组织的安全管理体系进行评审，确保其持续的适宜性、充分性和有效性	设定管理评审的频率和议程，收集相关信息和数据，进行评审讨论并作出决策，制定改进计划和措施
	外部审核和认	邀请第三方机构对组织的安全管理体	选择合适的认证机构，准备认证材料，配

项目	方法	监视、测量、分析和评价涵义	监视、测量、分析和评价方法应用说明
	证	系进行审核和认证，评估其符合国际标准的要求	合审核工作，根据审核结果进行改进并获取认证证书

——**方法的组合使用：**在实际操作中，组织可能需要根据具体情况组合使用多种方法，以确保监视、测量、分析和评价结果的全面性和准确性。

——**结果的有效性验证：**组织应对采用的方法进行验证，确保其能够提供准确、可靠和有效的结果。这包括定期评估方法的适用性、准确性和一致性，并根据需要进行调整和改进。

(c)何时实施监视和测量；

——**定期实施：**组织应设定明确的周期，如季度、半年或年度，定期对安全管理体系的绩效进行监视和测量。这有助于确保安全管理活动的连续性和一致性，及时发现并解决潜在问题；

——**基于事件驱动：**除了定期监视和测量外，组织还应根据特定事件或情况进行绩效监视和测量。例如，当发生安全事故、违规行为或发现潜在风险时，应立即进行绩效监视和测量，以评估安全管理措施的有效性和及时采取纠正措施；

——**与其他管理活动相协调：**绩效监视和测量的实施时机应与组织的其他管理活动相协调，如内部审核、管理评审等。这有助于确保绩效监视和测量结果的准确性和有效性，并为组织的安全管理体系提供全面的反馈和持续改进的机会。

(d)何时对监视和测量的结果进行分析和评价。

——**与监视测量周期同步：**组织应将绩效分析与评价活动与监视测量的实施周期同步进行。例如，如果绩效监视和测量是每季度执行一次，那么对绩效结果的分析和评价也应在该季度末进行。这样可以确保及时发现问题、总结经验和提出改进措施；

——**基于特定事件：**在某些情况下，如发生安全事故、发现严重违规行为或接收到外部投诉时，组织应立即对相关的绩效监视和测量结果进行分析和评价。这种基于事件的及时分析有助于组织迅速识别问题根源，采取有效措施防止类似事件再次发生；

——**与管理评审周期协调：**管理评审是组织对安全管理体系进行全面、系统评估的重要环节。组织应将绩效分析与评价活动与管理评审周期相协调，确保将绩效监视和测量的结果作为管理评审的重要输入之一。这样有助于管理层全面了解安全管理体系的运行状况，做出更准确的决策；

——**定期总结与反馈：**除了与监视测量周期同步和管理评审周期协调外，组织还应定期对绩效监视和测量的结果进行总结和反馈。这种定期总结有助于组织识别长期趋势、评估整体绩效并持续改进安全管理体系。同时，将结果反馈给相关人员也能促进其对安全管理工作的重视和参与。

(3)组织应评价安全管理体系的绩效和有效性。

(a)评价安全绩效：

——组织应定期或不定期地评估其职业健康安全绩效，以量化或定性地展现安全管理活动的成果；

——绩效评价应涵盖安全事故率、违规情况、预防措施的成效等方面，确保评价内容的全面性和准确性；

——评价结果应作为改进安全管理活动的依据，指导组织进一步提升职业健康安全绩效。

(b)确定安全管理体系的有效性：

——有效性评价旨在确认安全管理体系是否达到了预期的安全管理目标和要求；

——评价应包括体系运行的有效性、目标的达成情况、控制措施的有效性等方面；

——组织应通过内部审核、管理评审等方式收集和分析体系运行的数据和信息，以评估体系的有效性；

——评价结果应作为改进安全管理体系的依据，推动组织不断完善和提升安全管理体系的运行效果。

(4)组织应保留适当的成文信息，以作为结果的证据。

——**监视和测量目标及指标清单：**详细描述需要监视和测量的具体安全绩效目标及指标；

——**监视和测量方法说明：**说明用于监视和测量的具体方法，包括定量和定性的工具、技术和流程；

——**监视和测量实施计划：**列出实施监视和测量的具体时间和频率，如季度、年度等；

——**监视和测量记录：**记录实际执行的监视和测量活动，包括收集的原始数据、观察结果等；

——分析和评价报告；

- 对监视和测量结果的分析报告，包括数据解读、趋势分析、问题识别等；
- 对安全管理体系绩效和有效性的评价报告，说明体系运行的状态、目标的达成情况等；

——**不符合与纠正措施记录：**记录任何不符合安全管理体系要求的情况，以及采取的纠正措施和结果；

——**内部审核报告：**记录内部审核活动的结果，包括审核发现、结论和建议等；

——**管理评审记录：**记录管理评审会议的内容、决策和改进措施等；

——**持续改进计划：**基于绩效监视、测量、分析和评价的结果，制定的持续改进计划。

ISO 28000-2022 《安全与韧性—安全管理体系要求》

9 绩效评价

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 内部审核

9.2.1 总则

(1)有关内部审核术语

(a) 审核

为获得审核证据并对其进行客观评价，以确定组织的安全管理体系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。

——**审核目的：**通过系统的审核流程，收集和分析审核证据，以确认组织的安全管理体系是否满足预定的准则和要求，包括相关法规、标准以及组织自身的安全方针和目标。

——审核的用途；

- 内部审核结果可作为组织自我评估和改进的基础，帮助识别管理体系中的强项和改进点；
- 作为管理评审的输入，为管理层提供决策依据，推动安全管理体系的持续改进。

——审核类型；

- 内部（第一方）审核：由组织内部进行，旨在自我检查和改进安全管理体系；
- 外部（第二方或第三方）审核：由组织外部进行，如客户、监管机构或其他认证机构对组织安全管理体系的审核；
- 结合审核：涵盖两个或多个管理体系领域的审核，如同时审核质量管理体系、环境管理体系和安全管理体系。

——审核特性；

- 系统性：内部审核按照预定的计划和程序进行，确保全面覆盖安全管理体系的所有相关要素；
- 独立性：审核员应与被审核的活动无直接责任关系，保持客观立场，以确保审核结果的公正性和准确性；
- 文件化：审核过程和结果应详细记录成文件，以便于后续跟踪、参考和改进。

——**实施方式：**内部审核可以由组织自己实施，或由外部专家代表组织实施，但始终以组织的名义进行，确保审核的权威性和有效性。

(b)公正性

存在的客观性。

——**客观性的重要性：**客观性是确保内部审核结果可信度和有效性的基础。它要求审核过程应基于事实和证据，不受外部利益或个人偏见的影响；

——**利益冲突的解决：**在启动内部安全管理体系审核之前，识别并妥善处理一切潜在的利益冲突至关重要。这要求确保参与审核的人员与被审核的安全管理流程或实践没有直接的利害关系，从而避免任何可能的偏见或利益影响判断；

——**公正性的表现：**公正性应贯穿于审核的全过程，并在审核报告和记录中得到明确体现。审核人员需保持中立，对所有收集到的安全管理证据进行无偏见的评估，并仅基于事实和数据进行决策；

——**其他相关术语：**与公正性紧密相关的概念包括独立性、无利益纠葛、无预设观点、中立性、公平性、开放思维以及不受外部影响等。这些理念共同构成了内部安全管理体系审核中公正性的多维内涵；

——**确保公正性的措施：**为确保内部安全管理体系审核的公正性，组织应采取一系列措施，包括但不限于：精心挑选具备专业资质和经验的审核人员，制定并执行严格的审核规程，以及对审核人员进行系统的培训和监督。此外，可以引入外部监督机构或第三方认证来进一步验证内部审核的公正与有效；

——**公正性与客观性的关系：**公正性是客观性的外在表现，而客观性则是实现公正性的基础。只有建立在客观事实和数据分析基础上的审核，才能产生公正且可信的审核结果。因此，在进行内部安全管理体系审核时，必须始终坚守客观性和公正性的原则。

(c)审核方案

针对特定时间段所策划并具有特定目标的一组一次或多次审核安排。

——**特定时间段：**审核方案的策划应在预定的时间段内进行，以确保所有的安全管理体系审核活动能够有序、系统地展开，从而满足 ISO 28000 标准的要求；

——**特定目标：**审核方案必须设定清晰的目标，这些目标通常与评估、改进组织的安全管理体系，确保其符合相关法规要求，或满足组织设定的其他特定标准紧密相关；

——**一次或多次审核：**根据安全管理体系的复杂性及审核需求，审核方案可以包含一个或多个审核活动。这些活动的数量和范围将根据实际情况进行灵活调整；

——**审核策划：**一个完善的审核方案应包含周密的策划，明确审核的目的、范围、所依据的准则、采用的方法、实施的时间表、所需的资源、参与人员的角色与职责等核心要素；

——**详略程度：**审核方案的详细程度应根据组织的安全管理体系的复杂性、潜在风险的高低以及管理体系的成熟度来定制。对于那些复杂且风险较高的管理体系，审核方案需要设计得更加详尽和全面，以确保所有关键领域都能得到充分的审查。

(d)审核计划

对审核活动和安排的描述。

——**活动的描述：**审核计划需要全面而详细地阐述在审核过程中所要执行的各项活动。这涵盖了从审核的启动、前期的准备工作、实际的审核执行、审核结果的报告，以及后续的跟踪和验证等所有关键阶段；

——**安排的明确性：**为确保内部安全管理体系审核能够有条不紊地进行，审核计划必须清晰地指出审核的具体时间、地点、预期的参与人员，以及必要的资源需求等核心安排。这样的明确性有助于所有相关人员对审核流程有一个统一的认识，从而确保活动的顺利进行；

——**与审核方案的关系：**审核计划是审核方案的一个重要组成部分，它根据审核方案所设定的目标和要求，进一步细化了审核过程中应执行的具体活动和操作步骤。简而言之，审核方案为审核活动提供了宏观的指导，而审核计划则是这一指导下的具体执行蓝图。

(e)审核准则

用于与客观证据进行比较的一组要求。

——**比较基准：**审核准则起到了一个关键的参照作用，它帮助审核人员判断组织的安全管理体系运行状况是否达到了既定的要求和标准；

——**客观性**：为确保审核的有效性和公正性，审核准则必须具有客观性，即它们应能真实、准确地反映出组织安全管理体系的实际运作情况；

——**合规性的判定**：当审核准则涉及法律或法规的强制性要求时，审核结果中应明确使用“合规”或“不合规”来描述组织的安全管理体系与这些法定准则的符合程度；

——**准则类型**：审核准则不仅限于法律法规，还可以包括组织的安全方针、操作程序、工作指导手册、合同条款等。这些多元化的准则共同为审核过程提供了坚实的基础和明确的依据。

(f)审核证据

与审核准则有关并能够证实的记录、事实陈述或其他信息。

——**与审核准则的关联**：为确保审核的有效性和准确性，所收集的审核证据必须明确指向并对应相关的审核准则。这种关联性是评估组织的安全管理体系是否满足既定要求的基础；

——**证实性**：审核证据必须具有高度的真实性和可靠性，无论是书面记录、实际事实的陈述，还是其他形式的信息，都必须能够被独立验证，确保其所反映的情况是准确无误的；

——**来源多样性**：在收集审核证据时，应考虑到信息的多样性。这不仅包括组织内部的文件和记录，还涵盖现场的直接观察结果、员工及管理层的陈述，以及通过监测和测量获得的数据等。这种多元化的证据收集方法有助于更全面地评估组织的安全管理体系。

(g)审核发现

将收集的审核证据对照审核准则进行评价的结果。

——**审核发现定义**：指在内部审核过程中，将收集的审核证据与审核准则进行对照评价后所得出的结果；

——**结果的性质**：审核发现能够清晰地反映出组织在安全管理体系方面是否符合预设的审核准则。当审核证据与准则相符时，表明组织在该方面已经达到了标准的要求；反之，则意味着组织在某些特定环节还未达到标准，需要采取相应的改进措施；

——**改进与良好实践**：除了作为符合性评判的依据，审核发现还能为组织指明改进的方向，推动安全管理体系的持续完善。同时，审核过程中记录下的优秀实践案例，可以成为组织内部推广和学习的典范；

——**合规性评价**：如果审核准则是基于法律法规制定的，那么审核发现就直接关系到组织的法律合规性。符合审核准则的审核发现意味着组织的行为符合相关法律法规的要求，是合规的；而不符合则暗示组织可能面临违规的风险，需要迅速采取纠正措施以确保合规。

(h)审核结论

考虑了审核目标和所有审核发现后得出的审核结果。

——**定义**：指在内部审核过程中，经过全面考虑审核目标以及所有审核发现后得出的最终审核结果；

——**形成审核结论的关键因素**，审核结论的形成需要基于两个核心要素：

- **明确的审核目标**：这是审核活动的基石和导向，确保整个审核过程有的放矢，提高审核的效率和效果。

- **审核发现：**这是通过将审核证据与审核准则对比评价后得出的结果，它真实反映了组织在安全管理体系实施中的现状。

——审核结论的内容：

- 审核结论需要详尽且具体地展现组织在安全管理体系上的综合表现，这包括哪些方面达标、哪些方面未达标、存在哪些核心问题，以及有哪些潜在的改进空间；
- 审核结论应对组织在安全管理体系实施中的优秀做法给予认可，并针对存在的问题提出切实可行的改进意见，以推动体系的不断优化和完善。

(2)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)安全管理体系的符合性：

——**组织自身安全管理体系要求的符合性：**内部审核应首先评价组织是否按照其自己制定的安全管理体系要求进行运行。这包括检查组织的安全方针、目标、控制措施、过程和程序是否得到了有效执行。

——**ISO 28000一标准要求的符合性：**内部审核应检查组织是否遵守了 ISO 28000 标准中的各项规定。

(b)安全管理体系的有效实施和保持：

——内部审核应评估价安全管理体系是否得到了有效的实施和保持。这包括检查组织是否按照策划的要求和程序进行了安全管理体系的运行，以及是否采取了必要的措施来保持其持续有效性；

——审核还应关注组织在安全管理方面的持续改进能力，包括是否对不符合进行了及时纠正，并采取了预防措施来防止类似问题再次发生。

ISO 28000-2022 《安全与韧性—安全管理体系要求》

9.2 内部审核

9.2.2 内部审核方案

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。

组织应：

a) 规定每次审核的审核目标、准则和范围；

b) 选择审核员实施审核，以确保审核过程客观公正；

c) 确保将审核结果报告给相关管理者。

d) 验证安全设备和人员是否得到适当的部署；

e) 确保采取任何必要的纠正措施，不做无谓的拖延，以消除发现的不符合及其原因；

f) 确保后续审核措施包括验证所采取的措施和报告验证结果。

保留成文信息，作为实施审核方案以及审核结果的证据。

审核程序（包括任何时间表），应基于对组织活动的风险评估结果和以往审核的结果。审核程序应涵

盖范围、频率、方法和能力，以及进行审核和报告结果的职责和要求。

9.2.2 内部审核方案

(1)策划与实施内部安全审核方案告。

(a)审核方案的策划与制定；

——依据；

- **相关过程的重要性：**在制定审核方案时，首要考虑的是组织内各个过程对安全管理的关键性。重要的或高风险的过程应更频繁地进行审核；
- **对组织产生影响的变化：**组织内外部环境的变化（如政策更新、技术进步、市场动态等）也是制定审核方案的参考因素，以确保安全管理体系的持续有效性和适应性；
- **以往的审核结果：**过去的审核发现应作为改进和未来审核方案制定的依据，特别是针对以往发现的问题区域进行重点关注。

——审核方案内容；

- **频次：**根据过程的重要性和风险等级设定审核的频率，确保关键和高风险过程得到足够的关注；
- **方法：**明确审核的具体方法和流程，可能包括文件审查、现场观察、员工访谈等，以保证审核的全面性和有效性；
- **职责：**清晰界定审核团队中各成员的职责，确保审核活动的顺利进行；
- **策划要求：**对审核活动的具体规划，包括审核范围、资源分配、时间安排等，以指导审核的实施。
- 报告：规定审核结果报告的格式和内容，以便管理层了解审核发现，并采取相应措施。

(b)**实施与保持：**审核方案不仅要有详尽的计划，还需要确保其实施与持续维护。这包括定期对审核方案进行评审和更新，以确保其始终与组织的安全管理需求相匹配。

(2)基于对组织活动的风险评估结果和以往审核的结果建立内部审核程序；

(a)建立审核程序的基础；

——**风险评估结果：**审核程序的建立应考虑组织活动的风险评估结果。对于风险较高的活动或流程，审核应更加严格和频繁；

——**以往审核结果：**过去的审核发现和经验应被纳入考虑，特别是那些曾出现问题或需要改进的领域，应在审核程序中给予重点关注。

(b)审核程序的关键要素；

——**范围：**明确界定每次审核的具体内容和边界，确保所有关键的安全管理活动和流程都被纳入审核范围；

——**频率：**基于风险评估结果确定审核的频率，高风险活动需要更频繁的审核以确保安全；

——**方法：**详细描述进行审核的具体方法和步骤，可能包括但不限于文件审查、现场检查、员工访谈等，确保审核的全面性和有效性；

——**能力：**审核团队或人员应具备相应的专业知识和技能，以确保审核的准确性和权威性。

(c)审核与报告职责：

——**进行审核的职责：**明确指定负责进行审核的人员或团队，并确保他们了解并遵循审核程序；

——**报告结果的职责：**审核完成后，应有人负责整理和报告审核结果，包括发现的问题和改进建议。

(3)组织应：

(a)规定每次审核的审核目标、准则和范围；

——**审核目标：**组织应明确每次内部审核的具体目标。这些目标应当与提升安全管理体系的效能、确保体系符合相关标准和要求，以及识别潜在的安全风险和改进机会紧密相关。通过设定明确的审核目标，组织能够有针对性地评估安全管理体系的运行状况，从而确保审核活动的有效性和针对性；

——**审核准则：**审核准则是进行审核的依据和标准，组织应明确并遵循这些准则来评估安全管理体系的符合性和有效性。这些准则可能包括法律法规要求、行业标准、组织内部的安全管理政策等。通过确立清晰的审核准则，组织能够确保审核过程的公正性、客观性和一致性。

——**审核范围：**组织需要界定每次审核的具体范围，这包括受审核的部门、流程、活动以及相关的安全管理体系要素。明确审核范围有助于确保审核的全面性和深度，避免遗漏关键的安全管理环节。同时，通过合理划定审核范围，组织可以更加高效地分配审核资源，提高审核工作的效率和效果。

(b)选择审核员实施审核，以确保审核过程客观公正；

——**选择审核员：**组织在进行内部安全审核时，应慎重选择审核员。审核员的选择直接关系到审核结果的客观性和公正性，因此，这一步骤至关重要；

——**确保审核过程的客观性：**客观性意味着审核员在审核过程中应保持中立，不受个人偏见、情感或其他外部因素的影响。为实现这一点，组织需确保所选的审核员具备专业素养，能够基于事实和证据做出判断，而非个人主观意见；

——**确保审核过程的公正性：**公正性要求审核员在审核时对所有被审核对象一视同仁，不偏不倚。组织应通过选择具有高尚职业道德和诚信度的审核员，以及建立有效的监督机制，来保障审核的公正性。同时，审核员应避免与被审核部门存在利益冲突，以确保审核结果的公正无私。

(c)确保将审核结果报告给相关管理者。

——**审核结果的及时报告：**完成内部安全审核后，应确保审核结果能够迅速且准确地报告给相关的管理者；

——**报告的内容：**审核结果报告应全面反映审核过程中发现的问题、潜在风险以及改进建议；

——**报告的目的：**向管理者报告审核结果不仅是为了让其了解现状，更是为了推动改进措施的落实。管理者在接收到报告后，应组织相关部门进行整改，并监督改进措施的执行情况，以确保安全管理体系不断完善和提升。

(d)验证安全设备和人员是否得到适当的部署；

——**验证安全设备的部署：**在内部审核过程中，需要对组织内部的安全设备进行全面的检查和验证。这包括确认安全设备是否按照既定的安全标准和要求进行了正确的安装和配置，设备是否处于良好的工作状态，以及是否能够有效地发挥其应有的安全防护功能；

——**验证安全人员的部署**：除了对安全设备的验证，内部审核还需要检查安全人员的配置情况。这包括确认安全人员是否足够，并且是否具备必要的专业知识和技能来执行他们的职责。同时，还要验证安全人员是否被合理地分配到各个关键的安全管理岗位上，以确保组织的安全管理体系能够得到有效的执行和维护。

(e)确保采取任何必要的纠正措施，不做无谓的拖延，以消除发现的不符合及其原因；

——**及时采取纠正措施**：一旦内部审核发现任何不符合安全管理体系要求的问题，组织应立即着手制定并实施相应的纠正措施。这些措施应旨在迅速而有效地解决问题，避免问题进一步恶化或产生更严重的后果；

——**消除不符合及其原因**：纠正措施不仅要解决当前发现的具体问题，还要深入分析问题产生的原因，并从根本上加以解决。这样做可以防止类似问题在未来再次发生，从而提高安全管理体系的持续性和稳定性；

——**不做无谓的拖延**：在处理不符合时，组织应秉持迅速响应的原则，避免任何不必要的拖延。及时的行动有助于减少潜在的安全风险，并维护组织的声誉和利益相关者的信任。

(f)确保后续审核措施包括验证所采取的措施和报告验证结果。

——**后续审核措施的实施**：在完成内部安全审核并采取了必要的纠正措施后，组织需要确保实施有效的后续审核措施。这些措施应包括对所采取的纠正措施进行验证，以确认其是否按照计划执行，并达到了预期的效果；

——**验证所采取的措施**：验证过程应包括对纠正措施实施情况的详细检查和评估。组织需要确保这些措施不仅得到了执行，而且真正解决了先前审核中发现的问题。验证可以通过多种方式进行，如现场检查、文件审查或与相关人员进行沟通等；

——**报告验证结果**：完成验证后，组织应编制详细的验证结果报告。这份报告应清晰地说明纠正措施的执行情况，以及这些措施是否有效解决了先前发现的问题。报告还应包括任何必要的改进建议，以便组织进一步优化其安全管理体系。

(4)保留成文信息，作为实施审核方案以及审核结果的证据。

(a)**内部审核策划文件**：包含策划的时间间隔、频次、方法、职责分配、策划要求、报告程序等详细信息的内部审核策划文档；

(b)**审核准则和范围定义**：每次内部审核的详细准则和范围说明，确保审核活动覆盖组织安全管理体系的关键过程和要素；

(c)**审核员选择和资质证明**：记录审核员的选择过程，包括其资质、经验和独立性的评估结果；

(d)**内部审核实施记录**：记录内部审核活动的详细过程，包括审核日期、参与人员、审核范围、发现的问题、观察结果等；

(e)**不符合记录**：详细记录审核过程中发现的不符合，包括不符合的描述、涉及的条款、位置或过程、不符合的严重性和可能的后果等；

(f)**根本原因分析和纠正措施记录：**对于识别出的不符合，记录其根本原因分析的结果和采取的纠正措施，以及纠正措施的实施情况和效果评估；

(g)**内部审核结果报告：**向相关管理者提交的详细审核结果报告，包括符合性评估、有效性评估、不符合及纠正措施、改进建议等；

(h)**持续改进措施记录：**记录组织基于内部审核结果所采取的持续改进措施，包括措施的具体内容、实施计划、实施进展和效果评估等。

ISO 28000-2022 《安全与韧性—安全管理体系要求》

9 绩效评价

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。

组织应考虑分析和评价的结果以及管理评审的结果，以确定是否存在与业务或安全管理体系有关的需求或机会，并作为持续改进的一部分加以解决。

注：组织可以使用安全管理体系过程，如领导作用、策划和绩效评价，以实现改进。

9.3 管理评审

9.3.1 总则

(1)管理评审的定义；

最高管理者根据方针目标对管理体系适宜性、充分性和有效性进行的定期的、系统的评价。

(a)**主体与职责：**管理评审由最高管理者执行，他们负责对安全管理体系进行全面评价；

(b)**评审内容：**评审的内容聚焦于安全管理体系的“适宜性”“充分性”和“有效性”；

——**适宜性：**指的是安全管理体系与组织、其运营方式、组织文化和业务系统的匹配程度。简而言之，就是体系是否适合组织的实际需求和特点；

——**充分性：**反映安全管理体系是否得到了适当的执行和实施。这涉及到体系的各项要求是否被完全、准确地落实；

——**有效性：**衡量安全管理体系是否正在达到预期的目标和结果。这包括体系运行后，组织的安全状况是否有所改善，安全风险是否得到了有效控制等。

(c)**定期与系统评价：**管理评审不是一次性的活动，而是需要定期进行，确保安全管理体系的持续改进和适应性。同时，评审过程应该是系统的，涵盖安全管理体系的所有关键方面，以确保全面、准确地评估体系的状态和绩效。

(2)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。

(a)**最高管理者的责任：**最高管理者负有对组织安全管理体系进行定期评审的责任。这是确保体系能够适应组织变化、满足安全需求和持续改进的关键环节。

(b)**策划的时间间隔：**评审应按照预先策划的时间间隔进行。这意味着组织需要有一个明确的计划，规定了何时进行安全管理体系的评审，以确保这一活动的规律性和及时性。

(c)增加管理评审频次或临时开展专项管理评审的情形通常包括以下几种情况：

——**组织战略目标变化：**当组织的战略目标发生变化时，需要对安全管理体系进行评审，确保其与新的战略目标保持一致，支持组织目标的实现；

——**重大变更：**当组织经历重大结构或运营变更时，如合并、收购、重组等，需要对安全管理体系进行额外的评审，以确保其仍然适用于新的组织结构和运营环境；

——**安全事件：**发生重大安全事故或安全漏洞后，应立即启动专项管理评审，分析事故原因，评估安全管理体系的有效性，并提出改进措施，防止类似事件再次发生；

——**监管要求变化：**当相关法律法规、行业标准和监管要求发生变化时，需要对安全管理体系进行评审，以确保体系符合最新的监管要求；

——**内部审核结果：**如果内部审核发现重大不符合或潜在的高风险问题，可能需要增加管理评审频次，对这些问题进行深入分析和解决；

——**相关方要求：**当重要相关方（如客户、合作伙伴、投资者等）对组织的安全管理提出特别关注或要求时，可能需要临时开展专项管理评审，以满足利益相关方的期望和要求；

——**风险评估结果：**如果风险评估发现新的重大风险或现有风险的严重性增加，可能需要增加管理评审频次，对风险应对策略进行审查和更新；

——**持续改进计划：**为了推动安全管理体系的持续改进，可以根据组织的改进计划，定期或不定期地开展专项管理评审，评估改进计划的实施情况，调整优化改进措施。

(d)**评审的目的：**评审的目的是确保安全管理体系的适宜性、充分性和有效性。这包括评估体系是否仍然适合组织的当前需求和状况（适宜性），是否已全面实施且没有遗漏（充分性），以及是否正在达到预期的安全管理效果（有效性）。

(3)组织应考虑分析和评价的结果以及管理评审的结果，以确定是否存在与业务或安全管理体系有关的需求或机会，并作为持续改进的一部分加以解决。

(a)**分析和评价结果的考虑：**在管理评审过程中，组织应全面考虑和分析已收集的数据、信息、评估结果等，包括但不限于安全绩效监测数据、内部审核结果、纠正措施执行情况等；

(b)**管理评审结果的利用：**管理评审的结果是组织评估安全管理体系状态的重要依据。组织应仔细分析这些结果，以确定安全管理体系是否仍然有效、是否满足了组织的业务和安全需求；

(c)**识别需求或机会：**通过分析评价结果和管理评审结果，组织应识别出与业务或安全管理体系相关的潜在需求或机会。这些需求或机会可能涉及体系的改进、资源的重新分配、新的安全策略或措施等；

(d)**持续改进的整合：**识别出的需求或机会应被组织纳入持续改进的框架中加以解决。这包括制定行动计划、分配资源、设定优先级、监控实施情况等，以确保组织能够不断地优化安全管理体系，提高其效能

和适应性；

(e)**业务与安全管理体系的关联：**在进行管理评审时，组织应关注业务与安全管理体系之间的关联。这意味着组织需要确保安全管理体系不仅符合法规要求，而且能够有效地支持组织的业务发展和战略目标的实现。

(4)组织可以使用安全管理体系过程，如领导作用、策划和绩效评价，以实现改进。

利用安全管理体系过程：组织可以充分利用安全管理体系中的各个过程来实现改进。例如，领导作用过程可以确保最高管理者在推动改进方面的领导力和承诺；策划过程可以帮助组织系统地识别改进需求，并制定相应的改进措施；绩效评价过程则可以通过收集和分析数据来评估改进措施的有效性。

(a)**领导作用在改进中的作用：**最高管理者应通过领导作用展示对持续改进的承诺，确保资源、政策和目标的协调一致，并鼓励组织内的各级人员积极参与改进活动。

(b)**策划过程的改进应用：**在策划过程中，组织应识别与业务或安全管理体系相关的需求或机会，并将其纳入改进行动计划中。这包括确定改进的目标、措施、责任人、时间表和预期的成果。

(c)**绩效评价与改进的结合：**绩效评价不仅是对过去绩效的回顾和总结，更是识别改进机会的重要工具。组织应定期评估安全管理体系的绩效，包括监测结果、审核结果和纠正措施的执行情况等，以便及时发现并解决问题。

ISO 28000-2022 《安全与韧性—安全管理体系要求》

9.3 管理评审

9.3.2 管理评审输入

管理评审应包括：

a) 以往管理评审所采取措施的状况；

b) 与安全管理体系相关的内外部因素的变化；

c) 与安全管理体系有关的相关方的需求和期望的变化；

d) 下列有关安全绩效的信息，包括其趋势：

1) 不符合和纠正措施；

2) 监视和测量结果；

3) 审核结果；

e) 持续改进机会；

f) 对遵守法律要求和本组织同意的其他要求的审核和评估结果；

g) 来自外部相关方的沟通，包括投诉；

h) 组织的安全绩效；

i) 目标和指标的实现程度；

j) 纠正措施的状况；

k) 以往管理评审的后续措施；

l）不断变化的环境，包括与安全方面有关的合规义务（见4.2.2）的发展；

m) 改进的建议。

9.3.2 管理评审输入

管理评审应包括：

(1)**以往管理评审所采取措施的状况：**管理评审应包括对以往管理评审中所采取措施的执行情况进行回顾和评估；

——**以往措施的执行情况：**组织应关注之前管理评审中提出的改进措施的执行进度和完成情况；

——**措施的有效性：**评估以往措施是否达到预期的效果，通过效果评估可以判断措施的有效性和适用性；

——**未执行或未达到预期效果措施的原因分析：**对于未能执行或未达到预期效果的措施，应进行深入的原因分析，找出问题所在，以便制定更有效的改进措施。

(2)与安全管理体系相关的内外部因素的变化；

——**内部因素的变化：**内部因素可能包括组织结构、人员变动、资源配置、技术更新等。管理评审需要关注这些内部因素的变化如何影响安全管理体系的有效性和效率；

——**外部因素的变化：**外部因素可能涉及市场环境、客户需求、法律法规变动、行业动态等。评审应分析这些外部变化对安全管理体系的挑战和机遇。

(3)与安全管理体系有关的相关方的需求和期望的变化：

——**相关方需求和期望变化的影响：**相关方需求和期望的变化可能对组织的安全管理体系产生显著影响。因此，这些变化必须作为管理评审的重要输入，以便及时调整策略和实践；

——**及时响应：**将这些变化纳入评审输入，有助于组织及时响应并满足相关方的新需求和期望，从而提升客户满意度、维护品牌声誉并减少潜在风险。

(4)下列有关安全绩效的信息，包括其趋势：

(a)**不符合与纠正措施；**

——**评估纠正措施的有效性：**管理评审不仅需要了解纠正措施的实施情况，还要评估这些措施是否真正解决了不符合，并带来了安全绩效的改进。这包括对纠正措施实施后的结果进行监测和验证；

——**趋势分析：**管理评审应分析这些不符合出现的趋势，以便识别潜在的系统性问题或管理漏洞，并采取预防措施。

(b)**监视和测量结果；**

——**趋势的识别与评估：**管理评审应关注监视和测量结果的趋势变化，包括长期趋势和短期波动。通过趋势分析，可以预测未来可能的安全问题，并提前采取相应的预防措施；

——**与安全绩效的关联：**监视和测量的结果及其趋势应与安全绩效紧密关联。通过对比历史数据和行业标杆，可以评估组织的安全绩效是否达到预期目标，以及是否需要调整安全管理策略和方法；

——**决策支持的依据：**这些监视和测量的结果及其趋势分析将为管理评审提供重要的决策支持。基于这些数据和分析，管理层可以做出更加明智和有针对性的决策，以持续提升组织的安全绩效。

(c)**审核结果。**

——**符合性与不符合的识别：**审核结果应明确指出哪些方面符合安全管理体系的要求，哪些方面存在不符合。这些不符合可能包括未遵循的安全程序、未达到的安全目标等；

——**趋势分析的重要性：**管理评审应关注审核结果的趋势。这包括对历史审核数据的分析，以识别安全绩效的改进或恶化趋势，从而预测未来可能出现的问题；

——**与以往审核的对比：**通过对比当前的审核结果与以往的审核结果，可以评估安全管理体系的持续改进情况，识别出长期存在的问题和新的挑战；

——**对决策的支持作用：**审核结果及其趋势分析为管理层提供了宝贵的信息，支持其做出关于安全管理体系改进和资源配置的明智决策。

(5)持续改进机会；

——**机会的识别与评估：**管理评审应包括对当前安全管理体系中潜在的改进点的识别和评估。这可能涉及对现有流程、政策、资源分配等方面的重新审视，以发现可以优化的空间；

——**数据驱动的分析：**识别持续改进机会时，应基于实际的数据和事实进行分析。这可能包括安全绩效数据、事故统计、员工反馈等，以确保所提出的改进点是具体、可行的；

——**与战略目标的对齐：**持续改进的机会应与组织的长远战略目标相一致。在管理评审中，需要评估这些机会如何有助于实现组织的整体安全愿景和目标；

(6)对遵守法律要求和本组织同意的其他要求的审核和评估结果；

——**法律要求的遵守情况：**管理评审的输入应包含组织对各项安全相关法律、法规和标准遵守情况的审核和评估结果；

——**其他同意的要求：**管理评审的输入应包括对组织同意遵守的其他要求的审核和评估。

(7)来自外部相关方的沟通，包括投诉；

——**数据收集与分析：**为了确保管理评审的全面性和有效性，组织需要系统地收集、整理和分析这些来自外部相关方的沟通和投诉数据；

——**对决策的影响：**这些外部沟通和投诉应作为管理评审的重要输入，影响组织在安全管理策略、资源配置、流程优化等方面的决策。

(8) 组织的安全绩效；

——**绩效分析：**对收集到的安全绩效数据进行深入分析，识别出安全管理的强项和弱项，以及需要改进的领域；

——**与安全目标的对比：**将实际的安全绩效与组织设定的安全目标进行对比，评估目标的达成情况，并找出差距和原因；

——**对管理决策的支持：**安全绩效数据和分析结果应作为管理评审的重要参考，为管理层提供决策支持，帮助确定未来的安全管理重点和改进方向。

(9)目标和指标的实现程度；

——**实现程度的评估：**管理评审的输入应包括对这些安全管理目标和指标实现程度的详细评估。这涉及对各项指标完成情况的量化和定性分析；

——**数据支持与证据：**为确保评审的准确性和客观性，输入应包含实际数据、统计分析和相关证据，以展示目标和指标的实现情况；

——**偏差分析：**如果目标和指标未完全实现，输入中应包含对偏差的详细分析，包括原因识别、影响评估和纠正措施的建议。

(10)纠正措施的状况；

——**管理评审输入的必要性：**在管理评审过程中，应考虑纠正措施的实施状况和效果。这是因为纠正措施的执行情况直接关系到组织安全管理体系的持续改进和有效性；

——**纠正措施的实施状况：**管理评审应审查已采取的纠正措施是否按计划进行，是否遇到了障碍，以及是否需要额外的资源或支持来确保措施的有效实施；

——**纠正措施的效果评估：**管理评审应评估纠正措施的实际效果。这包括措施是否成功解决了问题，是否减少了类似问题的再次发生，以及是否提升了整体的安全管理水平。

(11)以往管理评审的后续措施；

——**以往管理评审的回顾：**在进行新的管理评审时，必须考虑以往管理评审中提出的建议和决定，以及针对这些建议和决定所采取的后续措施；

——**后续措施的执行情况：**管理评审应审查上一次评审后制定的改进措施是否已得到有效执行，这包括各项措施的完成情况、遇到的问题以及解决方案；

——**效果评估：**除了关注措施的执行情况，还需要评估这些后续措施的实际效果，判断其是否达到了预期的目标，是否提升了组织的安全与韧性。

(12)不断变化的环境，包括与安全方面有关的合规义务（见 4.2.2）的发展；

——**环境变化的监测：**管理评审的输入应包括对组织运营环境的持续监测结果，特别是那些与安全与韧性相关的环境变化。这包括但不限于市场需求、技术发展、法律法规更新等；

——**合规义务的发展：**评审过程中应特别注意与安全方面相关的合规义务（见 4.2.2）的最新发展。这意味着组织需要时刻关注并理解影响其安全管理的法律、法规和标准的变化。

(13)改进的建议。

——**改进建议的重要性：**管理评审的输入应当包含关于安全管理体系的改进建议。这些建议可能来源于内部审核、风险评估、员工反馈或其他相关活动，旨在提升安全管理的效果和效率；

——**针对性和实施性：**提出的改进建议需要具有明确的针对性和实施性，能够直接针对现有安全管理体系中存在的问题或不足，提出切实可行的解决方案。

9.3 管理评审

9.3.3 管理评审输出

管理评审的结果应包括与持续改进机会有关的决定和对安全管理体系的任何变更需求。

组织应保留成文信息，作为管理评审结果的证据。

9.3.3 管理评审输出

(1)管理评审的结果应包括与持续改进机会有关的决定和对安全管理体系的任何变更需求。

(a)**管理评审的结果内容：**管理评审结束后，应产生一份明确的结果报告。这份报告是评审过程的总结，也是后续改进和实施的依据；

(b)**持续改进机会的决定：**评审结果中应包含与持续改进机会相关的决定。在评审过程中识别出的可优化、可改进的方面，应作为结果的一部分被明确提出，并决定相应的改进措施；

(c)**安全管理体系变更需求：**如果评审中发现现有的安全管理体系存在不足或需要适应新的环境和要求，结果中应明确对安全管理体系的任何变更需求。这些变更可能涉及流程、政策、组织结构等方面；

(d)**后续行动计划：**评审结果不仅仅是一份报告，它还应作为后续行动计划的指导。根据评审中发现的持续改进机会和体系变更需求，组织应制定具体的实施计划和时间表。

(2)组织应保留成文信息，作为管理评审结果的证据。

——管理评审计划：记录所针对的主题，参加人员、时间和地点，参与者在评审过程中承担的职责和作用，评审所需收集和确认的相关信息；

——管理评审输入信息；

——管理评审输出决定：管理评审报告、—管理评审决议的跟踪和验证结果；

——管理评审会议记录：包括日期、地点、参与人员、讨论的内容、决策事项和结论；

——沟通记录：记录最高管理者与工作人员及其代表（若有）就管理评审输出进行的沟通内容、方式和结果，确保沟通的有效性和可追溯性。

ISO 28000-2022 《安全与韧性—安全管理体系要求》

10 改进

10.1 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。组织应积极寻求改进的机会，即使不是因为与安全有关的漏洞和迫在眉睫的安全威胁或正在发生的安全违规行为而促使相关的有关方面改进。

10 改进

10.1 持续改进

(1)持续改进的定义；

提高绩效的循环活动。

(a)**持续改进的定义：**持续改进是一种循环活动，其核心目的是提高组织的绩效，特别是在安全管理领域。这种提升涉及整个安全管理体系的各个方面，确保其与组织的安全方针和安全目标保持一致；

(b)**与安全方针和目标的关联性：**持续改进不是孤立的行动，而是与组织的安全方针和安全目标紧密相连。通过持续改进，组织可以确保其安全管理体系在不断进步，从而更好地实现既定的安全方针和目标。

(c)**循环活动的特性：**持续改进是一个循环过程，意味着它不是一次性的活动，而是需要不断地进行；这个循环包括识别改进机会、制定改进措施、实施改进措施、评估改进效果等多个阶段，形成一个闭环系统；

(d)**提升整体安全绩效：**持续改进的最终目标是提升组织的整体安全绩效。这包括减少安全事故的发生、提高安全管理效率、增强组织应对风险的能力等多个方面。通过持续改进，组织可以不断提升其安全管理体系的有效性，确保组织的可持续发展；

(e)**持续而非不间断：**虽然持续改进是一个持续进行的过程，但并不意味着所有改进活动都需要同时在所有领域发生。组织可以根据自身的实际情况和需要，有针对性地选择和改进特定的领域或方面，以实现整体安全绩效的提升。

(2)组织应持续改进安全管理体系的适宜性、充分性和有效性。

——**持续改进的必要性：**组织应当不断地评估并优化其安全管理体系，确保该体系能够持续适应不断变化的组织环境、业务需求以及外部威胁，进而维持和提升组织的安全性和韧性；

——**持续改进的三个维度；**

- **适宜性：**安全管理体系需要与实际运行的组织环境、业务需求和外部法律法规保持一致性，确保体系的设计和实施能够充分满足组织的特定需求；
- **充分性：**安全管理体系应确保资源充足、过程完善、控制有效，覆盖所有与安全管理相关的关键活动和领域，没有重大遗漏；
- **有效性：**安全管理体系应能够实现预定的安全管理目标，确保组织在安全方面的承诺得到实际履行，并通过定期评估和审查来验证其有效性。

(3)组织应积极寻求改进的机会，即使不是因为与安全有关的漏洞和迫在眉睫的安全威胁或正在发生的安全违规行为而促使相关的有关方面改进。

——**持续性的改进过程：**持续改进是一个长期、持续的过程，需要组织不断审视当前的安全管理体系，识别存在的问题和潜在的风险，制定并实施相应的改进措施，并通过定期评估和审查来验证改进的效果；

——**持续改进的主动性：**组织应展现出积极主动的态度，不断寻求并把握安全管理体系改进的机会，而不仅仅是在面临具体的安全问题或威胁时才采取行动；

——**主动性的重要性：**组织在安全管理方面应展现出积极主动的态度，即使在没有直接面临与安全有关的漏洞、迫在眉睫的安全威胁或正在发生的安全违规行为的情况下，也应积极寻求并推进管理改进。

——**预防而非仅响应：**持续改进不仅仅是对已有问题或威胁的被动响应，更重要的是对未来的潜在风险进行前瞻性管理和预防。组织应能提前识别可能的安全隐患，并采取措施避免其发生。

——**持续改进的常态化：**安全管理体系的改进不应局限于特定事件或特定时期，而应成为组织日常管理和运营的一部分。组织应建立一种常态化的改进机制，确保安全管理体系始终处于最佳状态；

——**机会与风险的平衡：**在寻求改进的过程中，组织应平衡对机会和风险的考虑。不仅要关注可能带来的改进机会，也要充分评估实施改进措施可能带来的风险，确保改进举措的可行性和有效性；

——**把握各类改进机会：**组织应时刻关注外部环境和内部条件的变化，从中发现可能带来的安全管理挑战和机遇。这些机会可能来源于技术发展、法律法规的更新、业务模式的变革等。

——**持续学习与创新：**持续改进要求组织保持开放的学习态度，不断吸收新的安全管理理念、技术和方法。同时，鼓励创新，尝试新的解决方案，以提升安全管理体系的效能。

ISO 28000-2022 《安全与韧性—安全管理体系要求》

10 改进

10.2 不符合和纠正措施

当发生不符合时，组织应：

a）对不符合做出应对，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他场合发生：

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，变更安全管理体系。

纠正措施应与不符合所产生的影响相适应。

应保留成文信息，作为下列事项的证据：

——不符合的性质以及随后所采取的措施；

——任何纠正措施的结果；

——对安全方面的调查：

- 失败，包括近乎失误和错误警报；
- 事故和紧急情况；
- 不符合；

采取措施，减轻此类故障、事故或不符合所产生的任何后果。

程序应要求在实施之前，通过安全相关风险的评估过程对所有拟议的纠正措施进行评审，除非立即实施可以防止即将发生的生命或公共安全风险。

为消除实际和潜在不符合的原因而采取的任何纠正措施，应与问题的严重程度相适应，并与可能遇到的安全管理相关风险相适应。

10.2 不符合和纠正措施

(1)当发生不符合时，组织应：

(a)**对不符合做出应对：**组织一旦发现不符合，应立即采取行动以应对，确保不符合不会进一步恶化或对其他环节造成影响。应对措施包括但不限于对不合格项的直接控制和纠正，以及消除不符合产生的后果或影响。

(b)采取措施以控制和纠正不合格：

——控制措施旨在暂时限制不符合的影响范围，防止其进一步扩大或对其他方面产生连锁反应；

——纠正措施则专注于根本问题的解决，旨在消除导致不符合的根本原因，防止问题再次发生；

(c)**后果的处置：**

——对于不符合可能产生的后果，组织需进行妥善处置，包括但不限于对受损资源的修复、对相关方的通知和解释、对影响的评估和记录等。

——组织应采取措施，减轻此类故障、事故或不符合所产生的任何后果；

- 立即响应：当组织发生不符合，如故障、事故或违反安全规定时，应立即采取行动以减轻这些事件可能带来的后果。迅速响应有助于减少潜在损失，保障人员和财产的安全。
- ——后果评估：在采取措施之前，组织应首先评估不符合可能导致的后果，包括但不限于人员伤亡、财产损失、环境破坏、声誉损失等。通过全面的后果评估，组织可以确定优先处理的事项和所需的资源。
- 制定减轻措施：根据后果评估的结果，组织应制定相应的减轻措施。这些措施可能包括紧急疏散、救援行动、设备修复、替代方案实施等。制定措施时应充分考虑资源的可用性、响应时间和效果等因素。

(2)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他场合发生：

(a)评审不符合；

——当安全管理体系中出现不符合时，组织应进行评审，以全面理解不符合的性质、范围和影响；

——评审过程应基于事实和数据，确保对不符合有清晰、准确的认识。

(b)确定不符合的原因；

——通过对不符合的深入分析，组织应确定导致不符合的根本原因；

——原因分析应涉及所有可能的影响因素，包括人为因素、技术因素、管理因素等。

(c)确定是否存在或可能发生类似的不符合；

——在确定不符合原因的基础上，组织应进一步评估是否存在或可能发生类似的不符合；

——通过识别潜在的风险点，组织可以提前采取预防措施，避免类似问题再次发生。

(d)制定纠正措施：

——基于不符合的评审和原因分析，组织应制定具体的纠正措施；

——纠正措施应针对根本原因，确保能够彻底解决问题，防止不符合再次发生；

——纠正措施的适当性与风险匹配性。

- **纠正措施的适当性：**当组织识别出安全管理体系中的不符合时，所采取的纠正措施应与不符合的所产生的影响（或严重程度）相适应。在制定纠正措施前，组织应对不符合的影响进行全面评估。对于影响较大的不符合，应采取更为严格和全面的纠正措施；
- **风险匹配性：**在制定纠正措施时，组织还需要考虑这些措施可能遇到的安全管理相关风险。纠正措施应与可能的风险相匹配，确保在解决问题的同时，不会引入新的风险或加剧现有风险。

(3)实施所需的措施；

(a)纠正措施的风险评估与前置评审。

——风险评估的必要性；

- 在实施任何拟议的纠正措施之前，组织应通过一个与安全相关的风险评估过程来评估这些措施；
- 评估过程旨在确保所采取的纠正措施不仅针对当前的不符合，而且考虑到可能引发的其他安全风险和潜在影响。

——前置评审的要求；

- 纠正措施的评审是前置的，即在实施之前进行，以确保纠正措施的有效性、安全性和适用性。
- 除非立即实施可以防止即将发生的生命或公共安全风险，否则所有拟议的纠正措施都应经过此评审过程。

——例外情况处理。

- 当存在立即的生命或公共安全风险时，组织可以例外地跳过前置评审，直接实施纠正措施；
- 即使在这种情况下，组织也应在实施后尽快进行回顾和评估，以确保所采取的措施是适当的，并尽量减少任何潜在的负面影响。

(b)立即行动：

——当组织识别出安全管理体系中存在不符合时，应立即采取行动，不延误时机；

——迅速应对不符合有助于减少潜在风险，避免问题进一步恶化。

(c)实施必要措施：

——组织应根据不符合的性质和严重程度，实施必要的纠正措施；

——这些措施可能包括修复问题、更改流程、加强培训、改进技术等。

(d)确保措施的有效性。

——在实施纠正措施时，组织应确保这些措施能够切实解决不符合的根本原因。

——措施的有效性是保障安全管理体系持续稳定运行的关键。

(4)评审所采取的纠正措施的有效性；

(a)**纠正措施的实施：**组织应确保所采取的纠正措施已经得到实施，并且所有相关环节都已得到妥善处理；

(b)**措施效果的评估：**组织应对纠正措施的实施效果进行评估，以确定其是否充分控制了根本原因，防止了类似事件或不符合的再次发生；

(c)**评审结果的应用：**根据评审结果，组织可以对纠正措施的有效性进行判定。如果评审结果表明纠正措施未能充分控制根本原因，组织应重新评估并调整纠正措施，直至达到预期效果。

(5)需要时，变更安全管理体系。

(a)适应变化；

——当组织发生不符合，且该不符合揭示了安全管理体系的某些部分已不适应当前环境或运营需求时，组织应意识到安全管理体系的变革是必要的；

——这种变革旨在确保管理体系始终与组织的战略目标、运营环境以及风险管理要求保持一致。

(b)评估变更需求；

——在决定进行安全管理体系变更之前，组织应全面评估变更的必要性和可行性；

——评估内容应包括不符合的影响范围、潜在风险、资源需求以及预期变更带来的益处。

(c)制定变更计划；

——一旦确定需要进行变更，组织应制定详细的变更计划；

——变更计划应明确变更的目标、范围、步骤、时间表以及所需的资源。

(d)实施变更；

——组织应按照变更计划逐步实施安全管理体系的变更；

——在实施过程中，应确保所有相关部门和人员充分了解变更内容，并积极参与变革过程。

(6)应保留成文信息，作为下列事项的证据：

(a)不符合性质与采取措施的证据；

——组织应详细记录不符合的性质，包括不符合的具体情况、涉及的领域、发生的时间、地点等关键信息；

——组织应保留为应对不符合所采取的措施的详细记录，包括纠正措施的具体内容、实施时间、实施人员等。

(b)纠正措施结果的证据；

——对于所采取的纠正措施，组织应记录其实施后的结果，包括纠正措施是否有效解决了问题、是否产生了预期的效果等；

——这些结果可以通过数据、报告、评估结果等形式进行记录，以便后续分析和参考。

(c)安全方面调查的证据。

——组织应保留对安全方面进行调查的证据，包括失败、近乎失误、错误警报、事故和紧急情况等事件的详细记录；

——这些证据应涵盖事件发生的背景、原因、影响、应对措施等方面，以便组织对安全事件进行全面分析，找出潜在的问题和改进点。

参考文献

[1] ISO 9001 质量管理体系－要求

[2] ISO 14001 环境管理体系－要求与使用指南

[3] ISO 19011 管理体系审核指南

[4] ISO 22301 安全与韧性－业务连续性管理体系－要求

[5] ISO/IEC 27001 信息技术－安全技术－信息安全管理体系 - 要求

[6] ISO 28001 供应链安全管理体系 实施供应链安全、评估和计划的最佳实践 要求和指南

[7] ISO 28002 供应链安全管理体系　供应链韧性的开发－－要求及使用指南

[8] ISO 28003 供应链安全管理体系 对供应链安全管理体系审核认证机构的要求

[9] ISO 28004-1 供应链安全管理体系 ISO 28000 实施指南

[10] ISO 28004-3 供应链安全管理体系 ISO28000 实施指南第 3 部分：中小业务采用 ISO28000 的附加特定指南（海港除外）

[11] ISO 28004-4 供应链安全管理体系 ISO28000 实施指南第 4 部分：若以符合 ISO 28001 为管理目标实施 ISO28000 的附加特定指南

[12] ISO 31000 风险管理指南

[13] ISO 45001 职业健康和安全管理体系--要求与使用指南

[14] ISO 导则 73，风险管理 - 术语