国际标准

ISO

28000

第2版

2022-03

安全与韧性 安全管理体系 要求

Security and resilience —

Security management systems — Requirements

ISO 28000：2022

目次

前言

国际标准化组织（ISO）是由各国标准化团体（ISO成员团体）组成的世界性的联合会。制定国际标准工作通常由ISO的技术委员会完成。各成员团体若对某技术委员会确定的项目感兴趣，均有权参加该委员会的工作。与ISO保持联系的各国际组织（官方的或非官方的）也可参加有关工作。ISO与国际电工委员会（IEC）在电工技术标准化方面保持密切合作的关系。

制定本标准及其后续标准维护的程序在ISO/IEC指引 第1部分均有描述。应特别注意用于各不同类别ISO文件批准准则。本标准根据ISO/IEC导则第2部分的规则起草（见www.iso.org/directives）。

本标准中的某些内容有可能涉及一些专利权问题，对此应引起注意。ISO不负责识别任何这样的专利权问题。在标准制定期间识别的专利权细节将出现在引言/或收到的ISO专利权声明清单中（www.iso.org/patents）。

ISO与合格评定相关的特定术语和表述含义的解释以及ISO遵循的世界贸易组织（WTO）贸易技术壁垒（TBT）原则相关信息访问以下URLL：www.iso.org/iso/foreword.html.

本标准由ISO/TC 292安全与韧性分委员会制定。

第二版取消并取代了第一版（ISO 28000:2007），第一版在技术上进行了修订，但保留了现有的要求，为使用前一版的组织提供连续性。主要变化如下：

——在第 4 章中加入了关于原则的建议，以便与 ISO31000 更好地协调；

——在第 8 章中增加了建议，以便与 ISO22301 更好地保持一致，促进整合，包括：

- 安全策略、程序、过程和应对；
- 安全计划。

有关本标准的任何反馈应直接向用户所在国家标准机构提出，这些机构的完整名单可以www.iso.org/members.html中找到。

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。

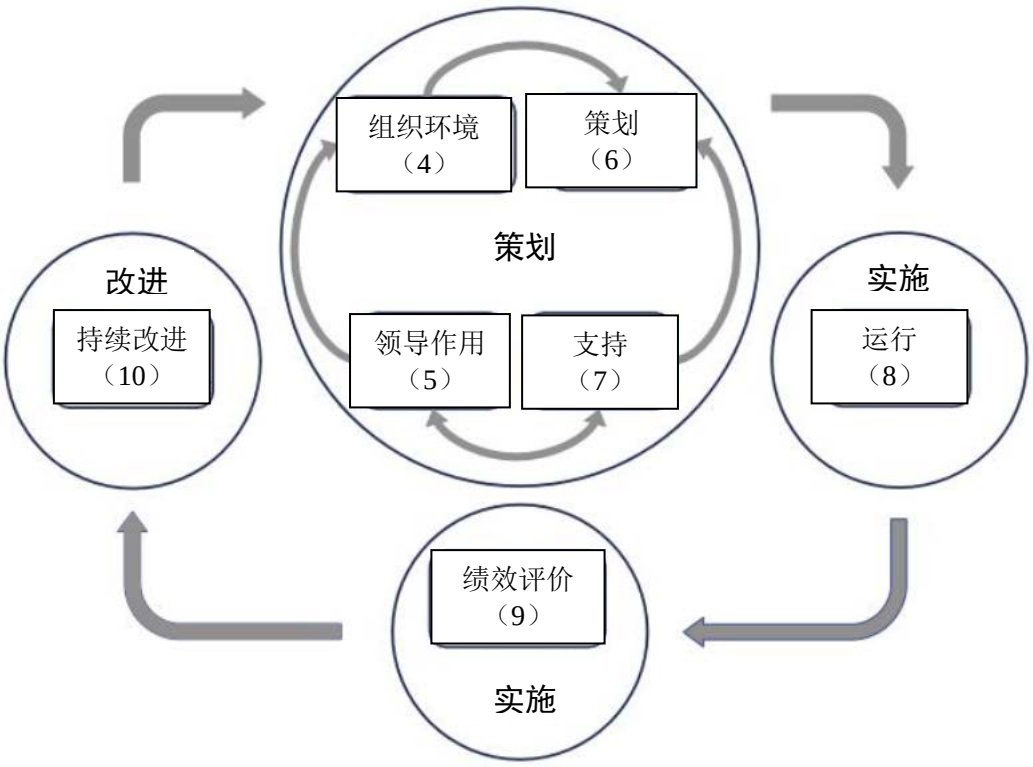

图1：应用于安全管理体系的PDCA模式

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。

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。

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

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