国际标准

ISO 28000

第二版
2022-03

ISO28000:2022

安全和韧性—安全管理体系—要求

Security and resilience-Security management systems-Requirements

参考编号
ISO28000:2022(E)

目录

前言

ISO(国际标准化组织）是一个由国家标准机构 （ISO成员团体）组成的全球联合会。制定国际标准的工作通常是通过ISO技术委员会进行的。每个对某一主题感兴趣的成员机构都有权在该技术委员会中任职。与国际标准化组织联络的国际组织、政府和非政府组织也参与这项工作。国际标准化组织与国际电工委员会(IEC)在所有电工标准化问题上紧密合作。

用于制定本标准的程序和打算进一步维护本标准的程序在ISO/IEC指令第1部分中有描述。特别要注意的是，不同类型的ISO文件需要不同的批准标准。本标准是根据ISO/IEC指令第2部分的编辑规则起草的（见www.iso.or/directives)。

请注意，本标准中的某些内容可能是专利权的对象。ISO不负责识别任何或所有此类专利权。在文件制定过程中发现的任何专利权的细节将在导言中和 / 或在ISO收到的专利声明列表中（见www.iso.or/patents)。

本标准中使用的任何商品名称是为方便用户而提供的信息，不构成对其的认可。

关于标准的自愿性质的解释，与合格评定有关的ISO特定术语和表达方式的含义，以及关于ISO在技术性贸易壁垒(TBT)中遵守世界贸易组织(WTO)原则的信息，见www.iso.org/iso/foreword.html。

本标准由ISO/TC292技术委员会（安全和复原力）编写。

第二版取代了经过技术修订的第一版（ISO 28000:2007），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 章中增加了关于原则的建议，以更好地与 ISO 31000 协调；
- 在第 8 章中增加了建议，以更好地与 ISO 22301 保持一致，便于整合，包括：
    - 安全策略、程序、过程和处理措施；
    - 安全计划。

对本标准的任何反馈或问题应直接向用户的国家标准机构提出。这些机构的完整名单可在www.iso.org/members.html。

简介

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中体系地解决这些问题。正式的安全管理方法可以直接促进组织的业务能力和可信度。

本标准规定了对安全管理体系的要求，包括对供应链安全保障至关重要的那些方面。它要求组织做到评估其运行的安全环境，包括其供应链（包括依赖性和相互依赖性）。

确定是否有足够的安全措施来有效管理与安全有关的风险。管理对组织所认同的法定、监管和自愿义务的遵守情况。

调整安全流程和控制，包括供应链的相关上游和下游流程和控制，以满足组织的目标。

安全管理与企业管理的许多方面相关联。它们包括由组织控制或影响的所有活动，包括但不限于对供应链有影响的活动。应考虑对组织的安全管理有影响的所有活动、功能和操作，包括（但不限于）其供应链。

关于供应链，必须考虑到供应链在本质上是动态的。因此，一些管理多个供应链的组织可能希望其供应商达到相关的安全标准，作为被纳入该供应链的一个条件，以满足安全管理的要求。

本标准将策划－实施－检查－处置(POCA)模式应用于组织的安全管理体系的策划、建立、实施、运行、监控、评审、维护和持续改进其有效性，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，以交付与组织总体方针和目标相一致的结果。
实施 （实施和操作）	实施并运行安全方针、控制措施、过程和程序。
检查 （监视和评审）	对照安全方针和目标监视并评审绩效，向管理层报告结果以供评审，并确定和授权采取整改和改进措施。
处置 （保持和改进）	基于管理评审结果，采取纠正措施，并重新评估安全管理体系的范围以及安全方针和目标，以保持和改进安全管理体系。

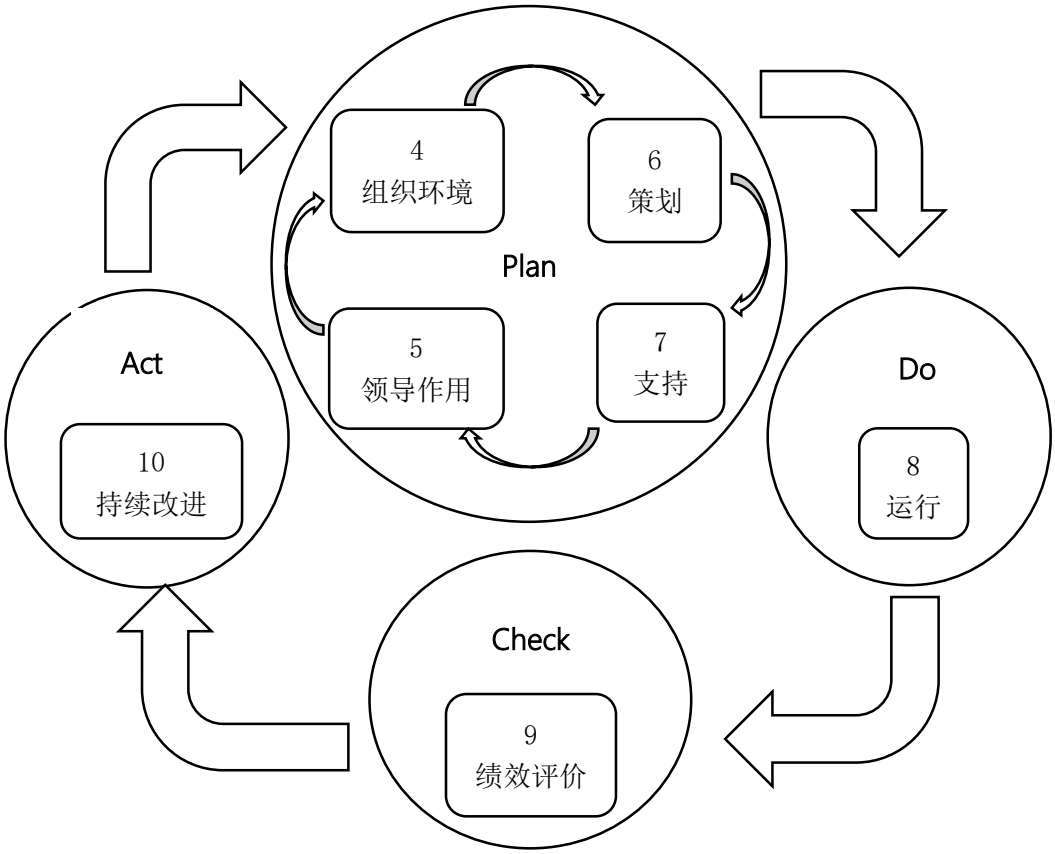

图1-PDCA 模型应用于安全管理体系

这确保了与其他管理体系标准，如ISO9001、ISO14001、ISO22301、1SO/IEC27001、ISO45001等的一定程度的一致性，从而支持与相关管理体系的一致和综合实施和运行。

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。

安全和韧性－安全管理体系－要求

1.范围

本标准规定了安全管理体系的要求，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（例如商业企业、政府或其他公共机构以及非营利组织），这些组织有意建立、实施、保持和改进安全管理体系。本标准提供了一种整体的、通用的方法，不针对特定行业或领域。

本标准可在组织的整个存续期间使用，并适用于任何内部或外部、各个层面的活动。

2.规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该注日期对应的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本标准。

ISO 22300《安全与韧性——词汇》

3.术语和定义

在本标准中，适用ISO22300和下列术语和定义。国际标准化组织和国际电工委员会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：可在https://www.iso.or/obp

-IEC Electropedia:可在https://www.electropedia.org/

3.1

组织

为实现其目标（3.7）而具有自身职能、职责、权限和关系的人员或一组人。

注1： 组织的概念包括但不限于个体工商户、公司、集团公司、商行、企业、行政机关、合伙企业、慈善机构或研究机构，或其部分或组合，无论是否注册、公有还是私有。

注2： 如果该组织是一个更大实体的一部分，则“组织”一词仅指该更大实体中处于安全管理体系（3.5）范围之内的那部分。

3.2

相关方（首选术语）

利益相关方（允许使用术语）

能够影响某项决策或活动、受其影响，或自认为受其影响的个人或组织（3.1）。

3.3

最高管理者

在最高层指挥和控制组织（3.1）的一个人或一组人

注1：最高管理者在组织内有授权和提供资源的权力。

注2：如果管理体系（3.4）的范围仅覆盖组织的一部分，在这种情况下，最高管理者是指管理和控制组织的这部分一个人或一组人。

3.4

管理体系

组织（3.1）中相互关联或相互作用的一组要素，用于制定方针（3.6）和目标（3.7），以及实现这些目标的过程（3.9）

注1：一个管理体系可以针对单个或多个学科领域。

注2：管理体系要素包括组织的结构、岗位和职责、策划和运行。

3.5

安全管理体系

一系列协调一致的方针（3.6）、过程（3.9）和实践，组织通过其管理安全目标（3.7）

3.6

方针

由组织（3.1）的最高管理者（3.3）正式表述的组织意图和方向

3.7

目标

要取得的结果

注1：目标可以是战略性的、战术性的或操作性的。

注2：目标可涉及不同学科（如财务、健康安全、环境）。例如，它们可以是组织整体层面的，或针对特定项目、产品和过程（3.9）的。

注3：目标可以用其他方式表达，例如预期的结果、宗旨、操作准则、安全目标，或使用其他含义相近的词（如目的、指标或靶向）。

注4：在安全管理体系（3.5）的语境下，安全目标由组织（3.1）依据安全方针（3.6）设定，以实现特定结果。

3.8

风险

不确定性对目标（3.7）的影响

注1：影响是指偏离预期。它可以是正面的、负面的或两者兼有，并可产生、带来或导致机会与威胁。

注2：目标可以有不同方面和类别，并可在不同层面应用。

注3：风险通常用风险源、潜在事件、其后果及其可能性来表达。

3.9

过程

一组相互关联或相互作用的活动，使用或转换输入以交付结果

注1：过程的结果称为输出、产品或服务，取决于引用的语境。

3.10

能力

应用知识和技能以实现预期结果的本领

3.11

成文信息

组织（3.1）需要控制和维护的信息及其载体

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（3.4），包括相关过程（3.9）；

——为组织运行而产生的信息（成文信息）；

——结果实现的证据（记录）。

3.12

绩效

可测量的结果

注1：绩效可涉及定量或定性的发现。

注2：绩效可涉及活动、过程（3.9）、产品、服务、体系或组织（3.1）的管理。

3.13

持续改进

提升绩效（3.12）的循环活动

3.14

有效性

实现策划的活动和取得策划的结果的程度

3.15

要求

明示的、通常隐含的或强制性的需要或期望

注1：“通常隐含”是指对组织（3.1）和相关方（3.2）而言，考虑中的需要或期望按惯例或常见做法是隐含的。

注2：规定的要求是已明示的要求，例如在成文信息（3.11）中阐明。

3.16

符合

满足要求（3.15）

3.17

不符合

不满足要求（3.15）

3.18

纠正措施

为消除不符合（3.17）的原因并防止再发生而采取的措施

3.19

审核

获取证据并客观评价，以确定审核准则满足程度的系统的、独立的、过程（3.9）

注1：审核可以是内部审核（第一方）或外部审核（第二方或第三方），也可以是结合审核（结合两个或多个学科）。

注2：内部审核由组织（3.1）自行实施，或由外部方代表其实施。

注3：“审核证据”和“审核准则”在ISO 19011中定义。

3.20

测量

确定数值的过程（3.9）

3.21

监视

确定体系、过程（3.9）或活动的状态

注1：确定状态可能需要检查、监督或密切观察。

4 组织环境

4.1理解组织及其环境

组织应确定与其目的相关的、影响其实现安全管理体系预期结果能力的外部和内部环境，包括其供应链的要求。

4.2 理解相关方的需求和期望

4.2.1 总则

组织应确定：

a)与安全管理体系有关的相关方；

b)这些相关方的需求和期望；

c)这些要求中的哪些将通过安全管理体系予以解决。

4.2.2 法律法规和其他要求

组织应：

a)实施和保持一个过程，以确定、获取和评估与其安全有关的适用法律法规和其他要求；

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法律法规和其他要求；

c)将此信息形成文件并保持更新；

d)酌情将此信息传达有关相关方。

4.2.3 原则

4.2.3.1 总则

组织内安全管理的目的是创造，特别是保护价值。

组织应采用图2中给出的、4.2.3.2至4.2.3.9中描述的原则。

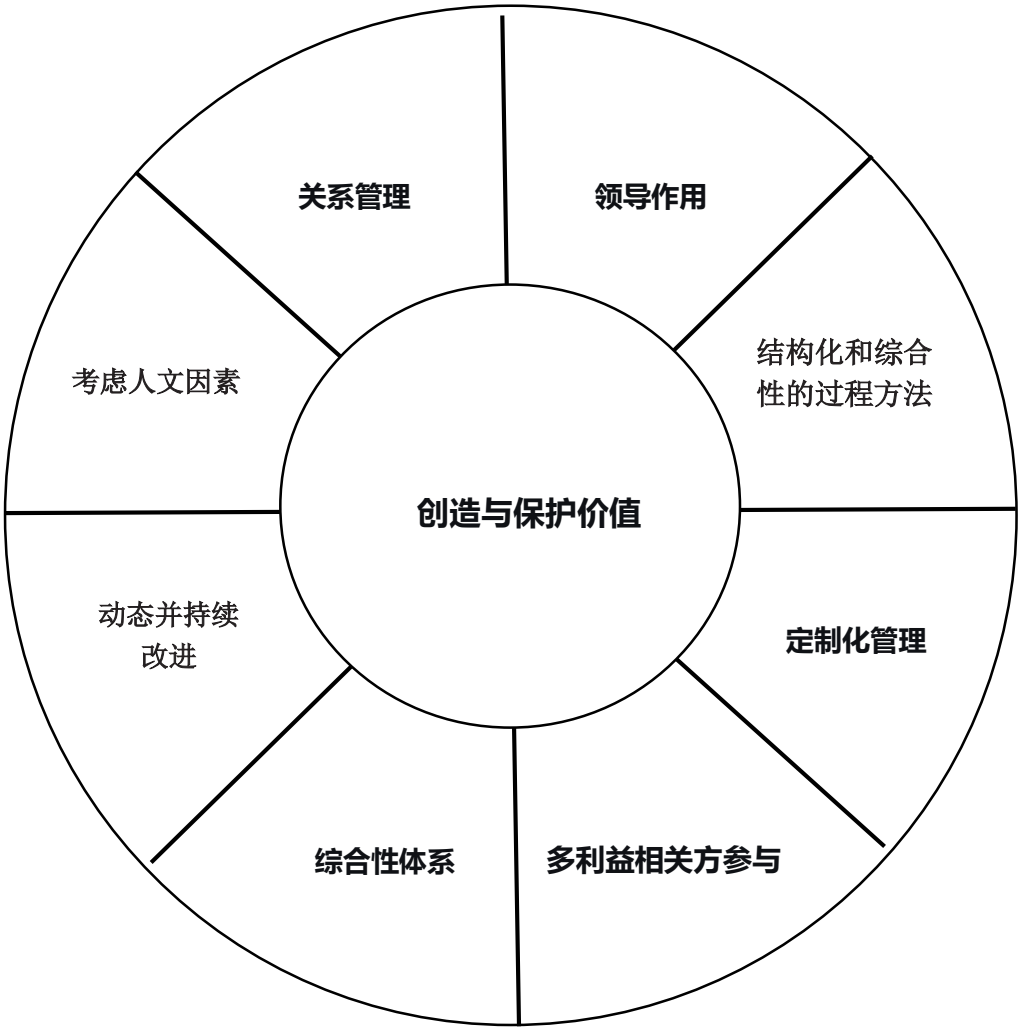

图 2-原则

4.2.3.2 领导作用

各级领导者应建立统一的宗旨和方向。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。第 5 章阐述了此原则相关的要求。

4.2.3.3 基于现有最佳信息的结构化和综合性的过程方法

包括供应链在内的结构化和综合性的安全管理方法应有助于取得一致且可比的结果，当活动被理解并作为构成一个连贯系统的相互关联的过程进行管理时，能够更有效和高效地实现这些结果。

4.2.3.4 定制化管理

安全管理体系应根据组织的外部和内部环境及需求进行定制并与之相称。它应与其目标相关联。

4.2.3.5 多利益相关方参与

组织应适当地、适时地让有关相关方参与。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。组织应确保各层次的所有人员都得到尊重和参与。

4.2.3.6 综合性体系

安全管理是所有组织活动的一个组成部分。它应与组织的所有其他管理体系相整合。组织的风险管理——无论是正式的、非正式的还是直观的——都应整合到安全管理体系中。

4.2.3.7 动态并持续改进

随着组织外部和内部环境的变化，组织应持续关注通过学习与经验进行改进，以保持绩效水平、应对变化并创造新的机会。

4.2.3.8 考虑人文因素

人的行为和文化对安全管理的所有方面都有很大的影响，应在每个层次和阶段予以考虑。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，可信，并更有可能产生预期的结果。应考虑个体的感知。

4.2.3.9 关系管理

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

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提及的外部和内部环境。

--4.2中提及的要求。

该范围应作为成文信息可获取。

如果组织选择将影响其安全管理体系符合性的任何过程进行外部提供，则应确保这些过程得到控制。此类外部提供过程的必要控制措施和责任应在安全管理体系内予以明确。

4.4 安全管理体系

组织应根据本标准的要求建立、实施、保持并持续改进安全管理体系，包括所需的过程及其相互作用。

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面，证实其对安全管理体系的领导作用和承诺：

a）确保制定安全方针和安全目标，并与组织的策略方向相一致。

b）确保识别和监视组织相关方的要求和期望，并及时采取适当措施管理这些期望，以确保将安全管理体系要求融入组织的业务过程。

c）确保安全管理体系要求融入组织的业务过程。

d）确保安全管理体系所需的资源是可获得的。

e）沟通有效的安全管理和符合安全管理体系要求的重要性；

f）确保安全管理体系实现其预期结果；

g）确保安全管理目标、指标和方案的可行性；

h）确保组织的其他部门产生的任何安全方案与安全管理体系互补；

i）指导和支持人员为安全管理体系的有效性作出贡献。

j）促进组织安全管理体系的持续改进。

k）支持其他相关管理者在其职责范围内发挥其领导作用。

注：本标准使用的＂业务”一词，可广义地解释为涉及组织存在的目的具有核心意义的那些活动。

5.2 安全方针

5.2.1 制定安全方针

最高管理者应制定安全方针，以便：

a)适应组织的宗旨。

b)为建立安全目标提供框架。

c)包括满足适用要求的承诺。

d)包括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：

-与组织的其他方针相一致；

-与组织的总体安全风险评估相一致；

-规定在收购或与其他组织合并，或在组织的业务范围发生可能影响安全管理体系的连续性或相关性的变更时，应对其进行评审；

-描述并分配对结果的总体责任和职责；

-作为成文信息可获取；

-在组织内部得到沟通；

-适用时，可为相关方所获取。情向有关方面提供。

注：组织可选择制定内部使用的详细的安全管理方针，以提供足够的信息和方向来驱动安全管理体系（其中部分可以是保密的），并编制简化的（非保密的）版本，包含总体目标，以分发给其相关方。

5.3 岗位、职责和权限

最高管理者应确保组织相关岗位的责任和权限在组织内得到分配和沟通。

最高管理者应分配以下责任和权限，以：

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。

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；

-防止或减少非预期影响；

-实现持续的改进。

组织应策划：

a)应对这些风险和机遇的措施；

b)如何：

1）在安全管理体系过程中整合并实施这些措施；

2）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。风险管理应融入安全管理体系。与组织及其相关方的安全有关的风险见8.3。

6.1.2 确定安全相关的风险和机遇

确定安全有关的风险以及识别和利用机遇，需要进行积极主动的风险评估，该评估应包括但不限于考虑：

a)物理或功能故障以及恶意或犯罪行为。

b)环境、人类和文化因素以及其他内部或外部环境，包括组织控制范围之外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、知识和沟通管理。

e)与安全威胁和脆弱性有关的信息。

f)供应商之间的相互依存关系。

6.1.3 应对安全相关的风险和机遇

对已确定的安全相关风险的评价应提供以下投入，包括但不限于：

a)组织的整体风险管理。

b)风险处理。

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。

6.2 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级上建立安全目标。

安全目标应：

a)与安全方针保持一致；

b)可测量（如可行）；

c)考虑适用的要求；

d)予以监视；

e)予以沟通；

f)适时更新；

g)作为成文信息可获取。

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：

a)要做什么；

b)需要什么资源；

c)由谁负责；

d)何时完成；

e)如何评价结果。

在建立和评审安全目标时，组织应考虑：

a)技术、人力、行政和其他方案；

b)对有关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。

6.3 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)变更的目的及其潜在的后果。

b)安全管理体系的完整性。

c)资源的可获得性。

d)职责和权限的分配或重新分配。

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。

7.2 能力

组织应：

a)确定在其控制下工作的人员所需的能力，这些人员从事的工作影响安全绩效；

b)基于适当的教育、培训或经验，确保这些人员是胜任的，并获得适当的安全授权。

c)适用时，采取措施以获得所需的能力，并评价措施的有效性。

d)保留适当的成文信息，作为人员能力的证据。

注：适用的措施可包括对在职人员进行培训、辅导或重新分配工作；或聘用、外包胜任的人员。

7.3 意识

在组织应确保在其控制下工作的人员知晓：

a) 安全方针；

b) 他们对安全管理体系有效性的贡献，包括改进安全绩效的益处；

c) 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（包括应急准备和响应要求）方面的作用和职责。

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：

a)沟通什么；

b)何时沟通；

c)与谁沟通；

d)如何沟通；

e)信息在传播前的敏感性。

7.5 形成文件的信息

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。

成文信息应描述实现安全管理目标和指标的责任和权限，包括实现这些目标和指标的方法和时限。

注：对于不同组织，安全管理体系的成文信息可能因组织不同而有所差异，具体取决于：

1)组织的规模，及其活动、过程、产品和服务的类型；

2)过程及其相互作用的的复杂程度；

3)人员的能力；

组织应确定信息的价值，并确定所需的完整性级别，以及防止未授权访问的安全控制措施。

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：

a)识别和说明（如标题、日期、作者、索引编号）；

b)形式（如语言、软件版本、图表）和媒体（如纸质的、电子的）；

c)评审和批准，以保持适宜性和充分性。

7.5.3 成文信息的控制

7.5.3.1 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、不当使用或完整性缺失）；

c)定期评审并在必要时修订，且经授权人员批准其充分性；

d)过时的文件、数据和信息应及时从所有发放点和使用点移除，或以其他方式保证防止非预期使用；

e)为法律或知识保存目的(或两者)而保留的归档文件、数据和信息，应进行适当识别。

7.5.3.2 对于成文信息的控制，组织应酌情处理以下活动：

-分发、访问、检索和使用；

-储存和防护，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，或者意味着允许查查阅并授权修改。

8.运行

8.1 运行策划和控制

组织应通过以下方式，策划、实施和控制满足要求所需的过程，并实施第6章中确定的措施所需的过程：

--建立过程的准则；

--按照准则实施过程控制。

应提供成文信息，其程度应足以确信过程已按策划实施。

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)符合其安全方针；

b)符合法律、法规和规章的安全要求

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。

8.3 风险评估和处理

组织应实施并保持风险评估和处理过程。

注：风险评估和处理的过程在ISO31000。

组织应：

a)确定其与安全有关的风险，并根据其安全管理所需的资源确定优先次序。

b)分析和评估已确定的风险。

c)确定哪些风险需要处理。

d)选择并实施应对这些风险的方案。

e)编制并实施风险处理计划。

注：本条款中的风险涉及组织及其相关方的安全。与管理体系的有效性相关的风险和机遇（6.1）。

8.4 控制措施

本标准8.2条款中所列的过程应酌情包括对人力资源管理的控制措施，以及与安全相关设备、仪器和信息技术的设计、安装、运行、翻新和改造。当修订现有安排或引入可能对安全管理产生影响的新安排时，组织应在实施前考虑相关的安全相关风险。应考虑的新安排或修订安排应包括：

a)修订的组织结构、职责或权限；

b)培训、意识和人力资源管理；

c)修订的安全管理方针、目标、指标或方案；

d)修订的过程和程序；

e)引入新的基础设施、安全设备或技术（可能包括硬件和/或软件）；

f)酌情引入新的承包商、供应商或人员；

g)外部供应商的安全保证要求。

组织应控制计划中的变更，并评审非预期变更的后果，必要时采取措施以减轻任何不利影响。

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。

8.5 安全策略、程序、过程和处理

8.5.1 策略和处理措施的确定和选择

组织应实施并保持系统性的过程，以分析与安全相关的脆弱性和威胁。基于该脆弱性和威胁分析以及随之进行的风险评估，组织应确定并选择由一项或多项程序、过程和处理措施组成的安全策略。

确定应基于策略、程序、过程和处理措施在以下方面的程度：

a)保持组织的安全；

b)降低安全脆弱性的可能性；

c)降低威胁变为实现的可能性；

d)缩短任何安全处理措施的缺陷期并限制其影响；

e)提供充足资源的可获得性。

选择应基于策略、过程和处理措施在以下方面的程度：

--满足组织安全的要求。

--考虑组织可能或无法承担的风险的数量和类型。

--考虑相关的成本和效益。

8.5.2 资源需求

组织应确定并实施所选安全程序、过程和处理措施所需的资源需求。

8.5.3 实施处理

组织应实施并保持所选的安全处理措施。

8.6 安全计划

8.6.1 总则

组织应根据选定的策略和处理措施，建立并形成文件化的安全计划和程序。组织应实施并保护一个响应团队，能够就安全相关脆弱性、迫在眉睫的安全威胁或正在发生的安全违规行为，向相关相关方提供及时有效的预警和沟通。该响应团队应提供计划和程序，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对组织进行管理。

8.6.2 响应团队

组织应实施并保持一种团队，确明确指定一名或一组负责响应安全相关脆弱性和威胁的人员或团队。指定人员或每个团队的角色和职责，以及人员或团队之间的关系，应予以明确标识、沟通和文件化。

总而言之，各小组具备以下能力：

a)评估安全威胁的性质、程度及其潜在影响；

b)根据预先确定的阙值评估影响，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事项，确定优先事项；

f)监视与安全相关脆弱性的任何变化，威胁者的意图和能力的变化或安全违规行为，以及组织的效果；

g)启动安全处理措施；

h)与有关相关方、主管部门和媒体沟通；

i)配合沟通管理，为沟通计划做出贡献。

对于每个指定的人或团队来说，应：

--确定工作人员，包括具有履行其指定职责所需的职责、权限和能力的候补人员。

—文件化的程序以指导其行动，包括应对响应的启动、运行、协调和沟通的程序。

8.6.3 预警和沟通

组织应文件化并保持以下方面的程序：

a) 在内部和外部与相关相关方进行沟通，包括沟通什么、何时沟通、与谁沟通以及如何沟通；

注：组织可以文件化并保持关于组织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。

b) 接收、文件化来自相关方（包括任何国家或区域风险预警系统或类似系统）的沟通并予以回应；

c) 确保在安全违规、脆弱性或威胁期间沟通手段的可获得性；

d) 促进与安全威胁和/或违规响应者之间的结构化沟通；

e) 提供安全违规后组织媒体响应的详细信息，包括沟通策略；

f) 记录安全违规的详细信息、所采取的行动和所做的决定。

适用时，还就考虑并实施以下事项：

-向可能受到实际或即将发生的安全违规事件影响的有关相关方发出警报。

—确保多个响应团队之间的适当的协调和沟通。

预警和沟通程序应作为组织测试和培训计划的一部分进行演练。

8.6.4 安全计划的内容

组织应文件化并保持安全计划。这些计划应提供指导和信息，以帮助团队应对安全脆弱性、威胁和/或违规行为，并协助组织进行响应和恢复其安全。

总的来说，安全计划应包含。

a)各小组将采取措施的详细信息，以。

1)继续或恢复可接受的安全状态。

2)监视实际或即将发生的安全威胁、脆弱性或违规行为的影响以及组织对其的响应。

b) 对预先确定的阈值和启动响应的过程的引用；

c)恢复组织安全的程序；

d)管理安全脆弱性和威胁或实际或即将发生的安全违规行为的直接后果的详细信息，并适当考虑：

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）丢失或无法使用。

每项计划应包括：

－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（包括启动准则）、操作、协调和沟通团队措施所需的信息；

－内部和外部的相互依存关系；

－其资源的需求；

－其报告的需求；

一个解除过程。

每项计划应在需要的时间和地点可用和可使用。

8.6.5 恢复

组织应有文件化的关过程，以从安全违规之前、期间和之后所采取的任何临时措施中恢复组织的安全。

9.绩效评价

9.1 监视、测量、分析和评价

组织应确定：

a)需要监视和测量什么；

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；

c)何时实施监视和测量；

d)何时对监视和测量的结果进行分析和评估。

组织应保留适当的成文信息，以作为结果的证据。

组织应评估安全管理体系的绩效和有效性。

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。

9.2.2内部审核方案

组织应依据有关过程的重要性和以往的审核结果，策划、建立、实施和保持一个或多个审核方案，审核方案包括频率、方法、职责、策划要求和报告。

组织应：

a)确定每次审核的审核目标、准则和范围;

b)选择审核员并进行审核，以确保审核过程的客观公正;

c)确保将审核结果报告给相关管理员;

d)核实安全设备和人员是否得到适当的部署;

e)确保及时采取任何适当的纠正和纠正措施，以消除所发现的不合格及其原因;

f)确保后续审核措施包括对所采取的措施进行验证查并报告验证结果;

g)保留成文信息，作为实施审核方案和审核结果的证据;

应基于对组织活动的风险评估结果和以往的审核结果编制审核方案，审核方案应包括任何时间表、范围、频率、方法和能力，以及进行审核和报告结果的责任和要求。

9.3 管理评审

9.3.1总则

最高管理者应按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遇，并作为持续改进的一部分加以解决。

注：组织可以利用安全管理体系的过程，如领导、计划和绩效评估，来实现改进。

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情况；

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有关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)不合格与纠正措施；

2)监视和测量结果；

3)审核结果；

e)持续改进的机会；

f)对组织应遵守法律法规和其他要求的合规性评价结果；

g)来自外部相关方的沟通信息，包括投诉；

h)组织的安全绩效。

i)目标和指标的实现程度。

j)纠正措施的情况。

k)以往管理评审的后续措施。

l)不断变化的情况，包括与安全方面有关的法律法规和其他要求的发展（见4.2.2)。

m)改进建议。

9.3.3管理评审输出

管理评审的输出应包括：

a) 与持续改进机会有关的决定、

b) 对安全管理体系的进行变更的任何需求。

组织应保留成文信息，作为管理评审结果的证据。

10.改进

10.1 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。即使未受到与安全相关的脆弱性、迫在眉睫的安全威胁或正在发生的、对相关方造成影响的安全违规行为的提示，组织也应主动寻求改进机会。

10.2 不合格和纠正措施

10.2.1 当出现不合格时，组织应：

a)对不合格做出应对，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，消除不合格的原因，避免其再次发生或在其他场合发生：

1)评审并分析不合格；

2)确定不合格的原因；

3)确定是否存在或可能发生类似的不合格。

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。

纠正措施应与不合格所产生的影响相适应。

10.2.2 组织应保留成文的信息，作为下列事项的证据。

a)不合格的性质和随后采取的措施；

b)任何纠正措施的结果；

c)对安全相关事项的调查,包括：

-故障，含未遂事件和假警报；

-事件和紧急情况；

-不合格；

d)采取措施，减轻此类故障、事故或不合格所产生的任何后果。

程序应要求：所有提议的纠正措施在实施前，应通过安全相关风险的评估过程进行评审，除非立即实施可避免对生命或公共安全的紧迫风险。

为消除实际和潜在的不合格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称。

参考文件

[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，安全和韧性--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--实施供应链安全的最佳实践，评估和计划--要求和指导

[7] ISO 28002，供应链的安全管理体系--供应链中弹性的发展--要求与使用指南

[8] ISO 28003，供应链安全管理体系--对提供供应链安全管理体系审计和认证的机构的要求

[9] ISO 28004-1，供应链安全管理体系--ISO 28000的实施指南--第1部分：一般原则

[10] ISO 28004-3，供应链安全管理体系--ISO 28000实施指南--第3部分：中小型企业（非海港）采用ISO 28000的补充具体指导。

[11] ISO 28004-4，供应链安全管理体系--ISO 28000的实施指南--第4部分：如果遵守ISO 28001是一个管理目标，那么实施ISO 28000的补充具体指导。

[12] ISO 31000，风险管理--指南

[13] ISO 45001，职业健康与安全管理体系--要求与使用指南

[14] ISO Guide 73，风险管理- 词汇