ISO 28000:2022
安全与韧性 安全管理体系 要求

目　录

前　言

ISO(国际标准化组织）是一个由国家标准机构（ISO 成员机构）组成的全球联合会。制定国际标准的工作通常是用过 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.org/directives)。

请注意，本标准中的某些内容可能涉及专利。ISO 不负责识别任何或所有此类专利。在文件制定过程中发现的任何专利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.org/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 特定术语的表达方式的含义，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/foreword.html。

本标准由 ISO/TC 292 技术委员会（安全和韧性）编写。

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 ISO 31000 更好地协调。

——在第 8 章中增加了建议，以便与 ISO 22301 更好地保持一致，促进整合，包括:

——安全策略、程序、过程和处置方案;

——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系统地解决这些问题。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：

——评估其运作的安全环境，包括其供应链（包括依赖性和下相互依赖性）。

——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、监督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，必须考虑到供应链的本质上是动态的。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。

本标准将计划--执行--检查--行动（PDCA)模式应用于组织的安全管理体系的规划、建立、实施、运行、监控、审查、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

计划（建立）	建立与改善安全有关的安全方针、目标、指标、控制、流程和程序，以提供与组织的总体方针和目标相一致的结果。
执行（实施和操作）	实施和操作安全方针、控制、流程和程序。
检查（监视和评价）	根据安全方针和目标监视和评价绩效，将结果报告给管理层进行评审，并确定和授权采取补救和改进行动。
行动（保持和改进）	通过采取纠正措施，管理评审结果和重新评估安全管理体系的范围和安全方针及目标保持和改进安全管理体系，

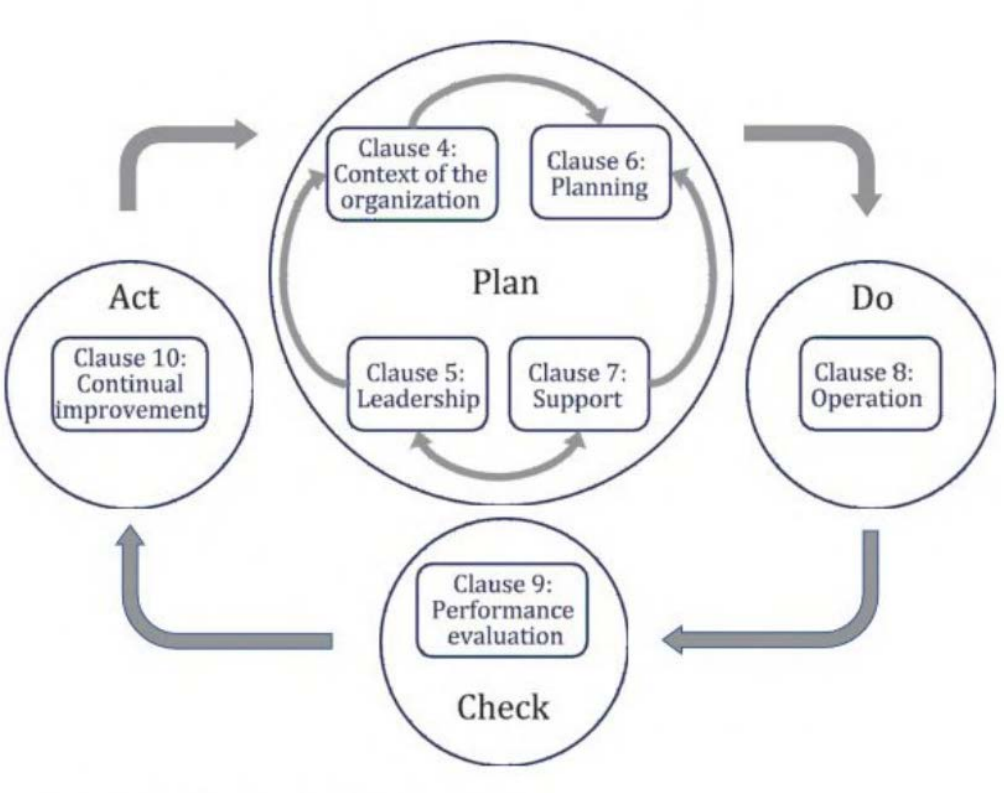

图 1　PDCA 模型应用于安全管理体系

这确保了与其他管理体系标准，如 ISO 9001、ISO 14001、ISO 22301、ISO/IEC 27001、ISO 45001 等一定程度的一致性，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，可通过外部和内部审核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的要求，包括与供应链相关的方面。

本标准适用于意图建立、实施、保持和改进安全管理体系的所有类型和规模的组织（如商业企业、政府或其他公共机构和非盈利组织），本标准提供了一个整体的、普遍的方法，并不针对具体行业或部门。

本标准可以在组织的整个生命周期中使用，并且可以适用于任何活动，无论是内部的还是外部的，各级的。

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 安全和韧性—词汇

3 术语和定义

ISO 22300 及以下给出的术语和定义适用于本标准。

ISO 和 IEC 维护用于标准化的术语数据库可通过以下地址查询：

——ISO 在线浏览平台：https://www.iso.org/obp

——IEC 电子媒介: https://www.electropedia.org/

3.1 组织

为实现目标（3.7），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 1：组织包括但不限于个体经营者、公司、集团、商行、企事业单位、行政管理机构、合伙制企业、慈善机构或社会机构，或者上述组织的某部分或其组合，无论是否为法人组织、公有或私有。

注 2：如果该组织是一个较大的实体的一部分，“组织”一词仅指该较大实体中术语安全管理体系（3.5）范围的部分。

3.2 利益相关方

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

3.3 最高管理者

最高层指挥和控制组织（3.1）的一个人或一组人。

注 1：最高管理者有权在组织内下放权利和提供资源。

注 2：若管理体系(3.4)的范围仅涵盖一个组织的一部分，则最高管理者是指那些指挥并控制组织该部分的人员。

3.4 管理体系

组织(3.1)建立方针(3.6)和目标(3.7)以及实现这些目标的过程(3.9)的相互关联或相互作用的一组要素。

注 1：一个管理体系可以针对单一的领域或几个领域，如安全管理、财务管理或环境管理。

注 2：管理体系要素确定了组织的结构、岗位和职责、策划、运行、方针、惯例、规则、理念、目标以及实现这些目标的过程。

3.5 安全管理体系

由协调的方针（3.6）、过程（3.9）和实践组成的体系，一个组织通过它来管理其安全目标（3.7）。

3.6 方针

一个组织（3.1）的意图和方向，由其最高管理者（3.3）正式表达。

3.7 目标

要实现的结果。

注 1：目标可能是战略性的、战术性的或运行层面的。

注 2：目标可能涉及不同的领域（例如：财务、健康与安全以及环境的目标），并可应用于不同层次（(如：战略、组织(3.1)整体、项目、产品和过程(3.9))。

注 3：可以采用其他的方式表述目标，例如：预期的结果、预期结果、目的、运行准则、安全目标，或使用其它意思相近的词语(如：目的、终点或指标)。

注 4：在安全管理体系(3.5)中，组织(3.2.1)制定的安全目标，与安全方针(3.6)保持一致，以实现特定的结果。

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，可以是正面的或负面的或两者兼有的，并且可以解决、创造或导致机会和威胁。

注 2：目标可以有不同的方面和类别，也可以在不同的层面上应用。

注 3：风险通常用风险源、潜在事件、其后果和其可能性来表示。

3.9 过程

利用输入产生预期结果的相互关联或相互作用的一组活动。

注 1：一个过程的结果是否被称为产出、产品或服务，取决于参考的背景。

3.10 能力

运用知识和技能来实现预期结果的能力。

3.11 形成文件的信息

组织(3.1)需要控制并保持的信息及其载体。

注 1：形成文件的信息可以任何格式和载体存在，并可来自任何来源。

注 2：形成文件的信息可涉及：

—— 管理体系(3.4)，包括相关过程(3.9)；

—— 为组织运行而创建的信息(一组文件)；

—— 实现结果的证据[记录]。

3.12 绩效

可测量的结果

注 1：绩效可能与定量的或定性的结果有关。

注 2：绩效可能与活动、过程(3.9)、产品、服务、体系或组织(3.1 的管理有关。

3.13 持续改进

提高绩效(3.12)的循环活动。

3.14 有效性

实现策划的活动并取得策划的结果的程度。

3.15 要求

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(3.1)和利益相关方(3.2)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：在形成文件的信息(3.11)中阐明。

3.16 合格(符合)

满足要求(3.15)。

3.17 不合格(不符合)

未满足要求(3.15)。

3.18 纠正措施

为消除不合格(3.17)的原因并防止再发生所采取的措施。

3.19 审核

为获得客观证据并对其进行客观的评价，以确定满足审核准则的程度所进行的系统的、独立的并形成文件的过程(3.9)。

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，也可以是结合审核或联合审核。

注 2： 内部审核，有时称为第一方审核，由组织(3.1)自己或外部单位以组织的名义进行。

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)、产品、服务或活动的状态。

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问题，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：

——与安全管理体系有关的利益相关方；

——这些相关方的要求；

——这些要求中哪些将通过安全管理体系来解决。

4.2.2 法律法规要求和其他要求

组织应：

a）实施和保持一个程序，以识别、获取和评估与其安全相关的适用法律、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）记录这些信息并保持更新。

d）适当时与利益相关方沟通这些信息。

4.2.3 原则

4.2.3.1 总则

组织内部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 中给出的和 4.2.3.2 至 4.2.3.9 中描述的原则。

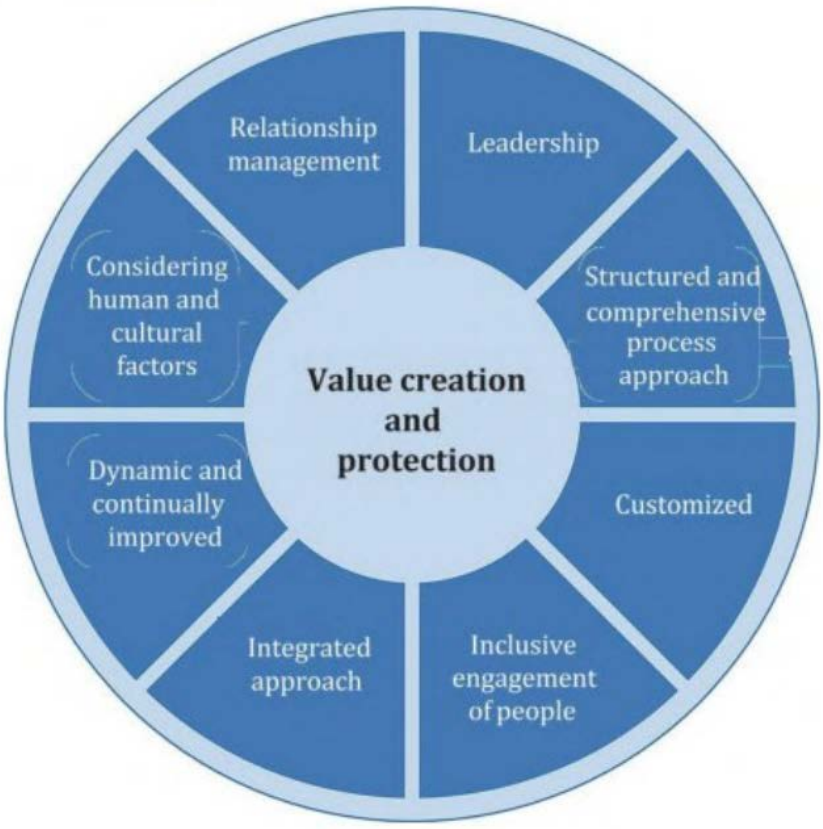

图2 - 原则

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。第 5 章解释了与此原则有关的要求。

4.2.3.3 基于最佳可用信息的结构化综合过程方法

包括供应链在内的结构化和全面的安全管理方法应有助于取得一致和可比较的结果，当各项活动被理解为相互关联的过程作为一个连贯的体系加以管理时，这些结果会更加有效。

4.2.3.4 定制化的

安全管理体系应是定制化的，与组织的外部和内部环境和需求相适宜。安全管理体系应与组织的目标相关。

4.2.3.5 人员参与

组织应适当的、及时的让利益相关方参与进来，应考虑他们的知识、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。组织应确保所有级别的人都得到尊重和参与。

4.2.3.6 综合方法

安全管理是所有组织活动的一个组成部分。它应该与组织的所有其他管理体系相结合。

组织的风险管理--无论是正式的、非正式的还是直观的--都应该被纳入安全管理体系。

4.2.3.7 动态且不断改进

组织应持续关注改进，通过学习和经验保持绩效水平，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的各个方面都有重大影响，应在每个层面和阶段加以考虑。决策应该建立在对数据和信息的分析和评估的基础上，以确保这些数据和信息具有更大的客观性和决策的信心，并更有可能产生预期的结果。应考虑个人感知的方式之一。

4.2.3.9 关系管理

为了持续的成功，组织应管理好与所有利益相关方的关系，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 中提到的内外部问题；

——4.2 中提到的要求。

范围应作为文件化信息可被获取。

如果组织选择从外部提供任何影响其安全管理体系合规性的过程，组织应确保这些过程得到控制。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确定。

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，包括所需的流程及其相互作用。

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对安全管理体系的领导作用和承诺。

——确保安全方针的安全目标得以建立，并于组织的战略方向相一致；

——确保识别和监视利益相关方的需求和期望，并及时采取适当的行动管理这些期望，

以确保将安全管理体系的要求融入组织的业务流程；

——确保将安全管理体系的要求融入组织的业务流程；

——确保安全管理体系所需的资源获取；

——就有效的安全管理和符合安全管理体系要求的重要性进行沟通；

——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做出贡献；

——促进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：本标准中提到的“业务”可被广义的解释为对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 建立安全方针

最高管理者应建立安全方针。安全方针应：

a) 与组织的宗旨相适应；

b) 为制定安全目标提供框架；

c) 包括满足使用要求的承诺；

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、方案等对组织的其他方面可能产生的不利影响。

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；

——与组织的整体安全风险评估相一致；

——规定在收购或合并其他组织，或对该组织的业务范围进行其他可能影响安全管理体系的连续性或相关性的变更时进行审查；

——描述和分配主要责任并对结果负责；

——作为文件化信息而可被获取；

——在组织内予以沟通；

——在适当时可为利益相关方所获取。

5.3 组织的角色、职责和权限

最高管理者应确保相关角色的责任和权限在组织内得到分配和沟通。

最高管理者应指定以下责任和权限：

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。

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 所提及的议题和 4.2 所提及的要求，并确定所

需应对的风险和机遇，以：

—— 确保安全管理体系实现预期结果；

—— 防止或减少不期望的影响；

——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。与组织及其相关方的安全相关的风险在 8.3 中进行了说明。

6.1.2 确定与安全相关的风险和机遇

确定与安全相关的风险和机遇，需要进行积极主动的风险评估，其中应考虑包括但不限于以下因素：

a) 物理或功能故障以及恶意或犯罪行为；

b) 环境因素、人的因素和文化因素以及其他内部或外部环境，包括组织控制之外影响组织安全的因素；

c) 安全设施的设计、安装、维护和更换；

d) 组织的信息、数据、知识和沟通管理；

e) 与安全威胁和漏洞有关的信息；

f) 供应商之间的相互依存关系。

6.1.3 应对与安全相关的风险并利用机遇

对已识别的安全相关风险的评估应为（但不限于）：

a) 组织的整体风险管理；

b) 风险应对措施；

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) 确定培训的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 制定安全目标

组织应对相关职能、层次设定安全目标。

安全目标应：

a) 与组织的安全方针保持一致；

b) 可测量（可行时）；

c) 考虑适用的要求；

d) 予以监视；

e) 予以沟通；

f) 适时更新；

g) 应保持有关安全目标的文件化信息。

6.2.2 确定安全目标

策划如何实现安全目标时，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。

建立和评审安全目标时，组织应考虑：

a) 技术、人员、行政和其他选择；

b) 对适当的利益相关方的意见和影响。

安全目标应与组织的承诺和持续改进保持一致。

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，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后果；

b) 安全管理体系的完整性；

c) 资源的可获得性；

d) 责任和权限的分配或再分配。

7 支持

7.1 资源

组织应确定并提供建立、实施、保持和持续改进安全管理体系所需的资源。

7.2 能力

组织应：

——确定在其控制下能够影响组织安全绩效的工作人员所必需具备的能力；

——基于适当的教育、培训或经历，确保工作人员具备胜任工作的能力。

——适用时，采取措施以获得和保持所必需的能力，并评价所采取措施的有效性；

保留适当的文件化信息作为能力证据。

7.3 意识

工作人员应意识到：

a) 安全方针

b) 其对安全管理体系有效性的贡献作用，包括提升安全绩效的益处；

c) 不符合安全管理体系要求的影响和潜在后果；

d) 他们在实现安全管理方针和程序和满足安全管理体系要求方面的角色和责任，包括应急准备和响应要求。

7.4 沟通

组织应确定安全管理体系有关的内外部沟通，包括：

——沟通什么；

——什么时候沟通;
——与谁沟通;
——如何沟通;
—— 决策前,对信息的敏感性进行评估。

7.5 文件化信息

7.5.1 总则

组织的安全管理体系应包括:

a) 本标准所要求的文件化信息;

b) 组织确定的实现安全管理体系有效性所需的文件化信息。

文件化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式和时限。

注： 对于不同组织而已，其安全管理体系的文件化信息可能因以下方面存在差异而不同：

——组织的规模及其活动、过程、产品和服务的类型；

——过程的复杂性及其相互作用；

——工作人员的能力。

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。

7.5.2 创建和更新

创建和更新文件化信息时，组织应确保适当的:

——标识和说明（如：标题、日期、作者或文件编号);

——形式（如：语言文字、软件版本、图表）与载体（如：纸质载体、电子载体);

——评审和批准，以确保适宜性和充分性。

7.5.3 文件化信息的控制

安全管理体系和本标准所要求的文件化信息应予以控制，以确保:

a) 在需要的场所和时间均可获得并适用;

b) 得到充分的保护（如防止失密、不当使用或完整性受损);

c) 定期审查并在必要时进行修订，并由授权人员批准其适当性;

d) 过期的文件、数据和信息被及时从所有发放点和使用点删除，或以其他方式保证不被意外使用。

e) 为法律或知识保护目的或两者兼有而保留的档案文件、数据和信息经过适当识别。

适用时，组织应针对下列活动来控制文件化信息:

——分发、访问、检索和使用;

——存储和保护，包括保持易读性;

——变更控制（如版本控制);

——保留和处置。

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

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

8 运行

8.1 运行策划和控制

为了满足安全管理体系要求和实施第 6 章所确定的措施，组织应策划、实施、控制所需的过程，通过：

——建立过程准则；

——按照准则实施过程控制。

保持和保留必要的文件化信息，以确信过程已按策划得到实施。

8.2 确定过程和活动

组织应确定为实现以下目标所必需的过程和活动。

a) 遵守组织的安全方针；

b) 遵守法律、法规的安全要求；

c) 组织的安全管理目标；

d) 组织的安全管理体系的实现

e) 供应链所需的安全水平。

8.3 风险评估和处置

组织应实施和保持一个风险评估和处置的程序。

注：风险评估和处置的过程在 ISO 31000 中进行了说明。

组织应：

a) 确定与其安全有关的风险，将风险与安全管理所需的资源进行优先排序。

b) 分析和评估已确定的风险；

c) 确定哪些风险需要处置；

d) 选择并实施应对这些风险的方案；

e）准备和实施风险处置计划。

注：本子条款中的风险与组织及其利益相关方安全有关。与管理体系的有效性有关的风险和机遇在 6.1 中说明。

8.4 控制措施

8.2 中所列的过程应包括对人力资源管理的控制，以及适宜时对安全有关的设备、仪器和信息技术的设计、安装、运行、翻新和修改。

对现有的安排进行修改或引入了可能对安全管理产生影响的新安排，组织应在实施前考虑与其相关的安全风险，新的或修改的安排应考虑包括：

a）修改后的组织结构、角色和责任；

b）培训、意识和人力资源管理；

c）修改后的安全管理方针、目标、指标和方案；

d）修改后的过程和程序；

e）引进新的基础设施、安全设备或技术，可能包括硬件和软件；

f）适宜时，引进新的承包商、人员供应商；

g）对外部供方的安全保证的要求。

组织应控制策划的变更和评审非预期改变的后果，必要时采取行动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、过程和处置方案

8.5.1 确定和选择策略和处置方案

组织应实施并保持系统化的过程，以分析与安全有关的漏洞和威胁。基于对这些漏洞和威胁的分析和后果风险评估，组织应确定和选择一个安全策略，其包含一个或多个程序、过程和处置方案。

确定应基于策略、程序、过程和处置方案的程度。

a）保持组织的安全；

b）降低安全漏洞的可能性；

c）降低威胁实现的可能性；

d）缩短任何安全处置方案不足的时间并限制其影响

e）提供充足可用的资源。

选择应基于策略、程序、过程和处置方案的程度。

——满足保护组织安全的要求；

——考虑组织可能承担或不承担的风险的数量和类型；

——考虑相关成本和效益。

8.5.2 资源需求

组织应确定实施所选择的安全程序、过程和处置方案的资源需求。

8.5.3 实施处置方案

组织应实施并保持所选择的安全处置方案。

8.6 安全计划

8.6.1 总则

组织应基于所选择的策略和处置方案，制定并记录安全计划和程序。组织应建立并保持一个响应结构以便能够及时和有效的警告与安全相关的漏洞和紧急安全威胁或正在进行的安全违规行为，并将其传达给利益相关方。响应结构应提供计划和程序，以便在遇到紧急安全威胁或正在进行的安全违规行为时管理组织。

8.6.2 响应结构

组织应实施并保持一个结构，确定并指定一个人或一个或多个团队负责应对安全相关漏洞和威胁。指定的人员或团队的角色和责任以及这些人员或团队的关系应得到明确、沟通并记录。

团队应具备以下能力：

a）评估安全威胁的性质和程度及其潜在影响；

b）根据预先定义的阈值评估影响，以证明激活正式的响应的合理性；

c）激活适当的安全响应；

d）计划需要采取的行动；

e）以生命安全为第一要务确定优先事项；

f）监控与安全相关的漏洞的任何变化、威胁因素或安全违规行为的意图和能力的变化以及组织的反应的影响。

g）激活安全处置方案

h）与相关利益相关方、当局和媒体进行沟通;

i）为沟通管理的沟通计划做出贡献。

对于指定的人员或团队来说，应有:

——确定的工作人员，包括具有履行其指定角色必要的责任、权限和能力;

——指导其行动的文件化程序，包括应对措施的激活、运行、协调和沟通。

8.6.3 警告和沟通

组织应记录并保持以下程序:

a）与有关的利益相关方进行内外部沟通，包括沟通的内容、时间、对象和方式。

注：组织可以记录并保持如何以及在何种情况下与员工及紧急联系人进行沟通的程序。

b）接收、记录和回应相关方的沟通，包括任何国家或地区风险咨询系统或同等机构。

c）在安全违规、漏洞或威胁期间确保沟通方式的可用性;

d）促进与安全威胁和/或违规行为的响应者的结构化沟通;

e）提供组织在违反安全规定后媒体反应的详细信息，包括沟通策略.

f）记录违反安全规定的细节、采取的行动和做出的决定。

适用时，以下内容应被考虑并实施:

——提醒可能受到实际或即将发生的安全违规影响的相关方;

——确保多个响应组织之间的适当协调和沟通。

警告和沟通程序应作为组织测试和培训计划的一部分。

8.6.4 安全计划的内容

组织应记录并保持安全计划。安全计划应提供指引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。

总体而言，安全计划应包含:

a）团队将要采取的行动的细节:

1） 继续或恢复商定的安全状态;

2）监控实际或即将发生的安全威胁、漏洞或违规行为的影响，以及组织对此的反应。

b）参考预先定义的阈值和激活响应的过程;

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违规的直接后果的详细信息，应适当考虑:

1） 个人福利;

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（进一步）丢失或不可用。

每项计划应包括:

——其目的，范围和目标;

——实施该计划的团队的角色和责任;

——实施解决方案的行动;

——激活（包括激活准则）、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;

——退出的过程。

每项计划应在所需要的时间和地点是可用的。

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。

9 绩效评价

9.1 监视、测量、分析和评价

组织应确定：

——需要监视和策略什么；

——需要用什么方法进行监视、测量、分析和评价（如适用），以确保有效的结果；

——何时进行监视和测量；

——何时对监测和测量结果进行分析和评价。

组织应保留适当的文件化信息应作为结果的证据。

组织应评价安全管理体系的绩效和有效性。

9.2 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信息是否：

a）符合：

1）组织自身对其安全管理体系的要求；

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

组织应计划、建立、实施和保持（一个或多个）审核方案，包括频次、方法、职责、策划要求和报告。

在制定内部审核方案时，组织应考虑有关过程的重要性和以往审核的结果。

组织应：

a）确定每次审核的目标、准则和范围；

b）选择审核员并实施审核，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已适当部署；

e）确保在不无故拖延的情况下采取任何必要的纠正措施，以消除发现的不符合项及其原因；

f）确保后续审核行动包括对所采取行动的验证和验证结果的报告；

组织应保留文件化信息，作为审核方案实施和审核结果的证据。

审核计划，包括任何时间表，应以组织活动的风险评估结果和以往审核的结果为基础。审核程序应涵盖范围、频次、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估的结果以及管理评审的输出，以确定是否存在与业务或安全管理体系相关的需求或机会，这些需求或机会应作为持续改进的一部分加以解决。

9.3.2 管理评审输入

管理评审输入应包括：

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）与安全管理体系相关的利益相关方的需求和期望的变化；

d）安全绩效方面的信息，包括以下方面的趋势：

1）不符合项和纠正措施；

2）监视和测量的结果；

3）审核结果；

e）持续改进的机会；

f）对法律法规要求和其他要求的合规性评价的结果；

g）与外部利益相关方的沟通，包括投诉。

h）组织的安全绩效；

i）安全目标和指标实现程度。

j）纠正措施的状况；

k）以往管理评审的后续行动；

l）环境变化，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 管理评审结果

管理评审结果应包括持续改进机会的有关决定和任何对安全管理体系变更的需求。

组织应保留文件化信息，以作为管理评审结果的证据。

10 改进

10.1 持续改进

组织应不断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，即使不是因与安全相关的漏洞、紧急的安全威胁或利益相关方正在进行的安全违规行为引起的。

10.2 不符合和纠正措施

当不符合发生时，组织应：

a）及时对不符合做出响应，并在适用时：

1）采取措施予以控制和纠正；

2）处置后果；

b） 评价是否采取纠正措施，消除不符合的原因，防止不符合再次发生或在其他场合发生：

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）实施任何所需的行动；

d）评审所采取的任何纠正措施的有效性；

e）在必要时，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。

组织应保留文件化信息作为以下方面的证据：

——不符合的性质以及所采取的任何后续措施；

——纠正措施的结果；

——对安全方面的调查：

——事故，包括近乎失误和错误报警；

——事件和紧急情况；

——不符合；

——采取行动，减轻此类事件、事故或不符合。

程序应要求在实施前，通过安全相关风险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。

参考文献

[1] ISO 9001 质量管理体系-要求
[2] ISO 14001 环境管理体系-要求和使用指南
[3] ISO 19011 管理体系审核指南
[4] ISO 22301 安全与弹性 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-供应链弹性的发展-要求和使用指南
[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-第一部分：一般原则
[10] ISO 28004-3 供应链安全管理体系- ISO 28000 实施指南-第三部分：中小型企业（海港除外）采用 ISO 28000 的附加指南
[11] ISO 28004-4 供应链安全管理体系- ISO 28000 实施指南-第三部分：当以满足 ISO 28001 作为管理目标时实施 ISO 28000 的附加指南
[12] ISO 31000 风险管理-指南
[13] ISO 45001 职业健康安全管理体系-要求与使用指南
[14] ISO 指南 73 风险管理-词汇

（完）