国际标准

ISO 28000

第二版2022-03-15

安全和韧性 安全管理体系 要求

参考号ISO 28000:2022（E）

版权 受保护的 文件

ISO版权局
布朗登8•CP 401
瑞士日内瓦游标卡尺CH-1214电话
+41 22 749 01 11
传真+41227490947
copyright@iso.org
www.iso。组织

目 录

前言

ISO（国际标准化组织）是国家标准机构（ISO成员机构）的全球联合会。国际标准的制定工作通常通过ISO技术委员会进行。对已成立技术委员会的某一主题感兴趣的每个成员机构都有权派代表参加该委员会。与ISO保持联系的政府和非政府国际组织也参与了这项工作。ISO与国际电工委员会（IEC）在所有电工标准化问题上密切合作。

ISO/IEC指令第1部分描述了用于编制本标准的程序及其进一步维护的程序。特别是，应注意不同类型的ISO标准所需的不同批准标准。本标准根据ISO/IEC指令第2部分的编辑规则起草（参见www.iso组织/指令）。

需要注意的是，本标准的某些内容可能是专利权的主题。ISO不负责识别任何或所有此类专利权。标准编制过程中确定的任何专利权的详细信息将在引言和/或收到的ISO专利声明清单中（参见www.iso组织/专利）。

本标准中使用的任何商品名称均为方便用户提供的信息，不构成背书。

有关标准的自愿性质、与合格评定有关的ISO特定术语和表达的含义，以及ISO遵守世界贸易组织（WTO）技术性贸易壁垒（TBT）原则的信息，请参见www.iso org/iso/foreword.html。

本标准由技术委员会ISO/TC 292 安全和韧性委员会负责编制。

第二版取消并取代第一版(ISO 28000:2007)，但保留了现有要求，以便为使用上一版本的组织提供连续性。主要变化如下：

— 第4章增加了有关原则，以便更好地与国际标准化组织 31000标准保持一致;

— 第8章，为了更好地与国际标准化组织 22301，促进融合，包括：

  — -安全策略、程序、流程和处置；

  — -安全计划。

关于本标准的任何反馈或问题都应提交给用户的国家标准机构。有关这些版本的完整清单，请访问www.iso组织/成员.html网站。

引言

大多数组织都在安全环境中经历着越来越大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，他们希望在管理体系内系统地解决这些问题。正确的安全管理方法可以直接提高组织的业务能力和可信度。

本标准规定了安全管理体系的要求，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（包括依赖性和相互依赖性）；

— 确定是否有足够的安全措施来有效管理安全相关风险；

— -管理遵守组织签署的法定、监管和自愿义务；

— -协调安全流程和控制，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有关。它们包括组织控制或影响的所有活动，包括但不限于影响供应链的活动。应考虑对组织安全管理有影响的所有活动、职能和操作，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满足相关的安全标准，以此作为加入该供应链的条件，以满足安全管理的要求。

本文件将PDCA模式应用于组织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，参见表 1 和图 1。

表1——PDCA模式

计划（建立）	建立与提高安全性相关的安全策略、目标、指标、控制、流程和程序，以交付与组织总体策略和目标一致的结果。
做（实施和运行）	执行和操作安全策略、控制、流程和程序。
检查（监测和审查）	根据安全策略和目标监控和审查绩效，将结果报告给管理层审查，并确定和授权补救和改进措施。
行动（维护和改进）	根据管理评审的结果，通过采取纠正措施，维护和改进安全管理体系，并重新评估安全管理体系的范围、安全策略和目标。

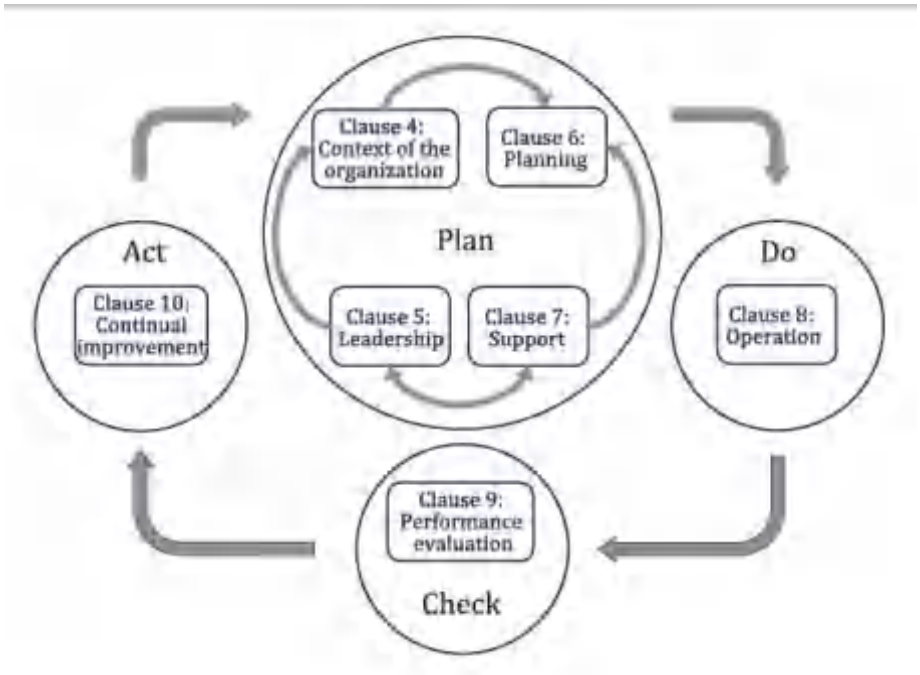

图1-PDCA模型在安全管理体系中的应用

这确保了与其他管理体系标准的一致性，例如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集成实施和运行。

对于有此意愿的组织，可通过外部或内部审核程序验证安全管理体系是否符合本标准。

安全和韧性 安全管理体系 要求

1 范围

本标准规定了与供应链相关的安全管理体系的要求。

本标准适用于准备建立、实施、维护和改进安全管理体系的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和非营利组织）。它提供了一种整体和通用的方法，而不是特定于行业或部门的方法。

本标准可在组织的整个生命周期内使用，并可应用于所有级别的任何内部或外部活动。

2 规范性引用文件

以下标准在文中引用时，其部分或全部内容构成了本标准的要求。凡是注日期的引用文件，仅引用的版本适用。对于不注日期的引用文件，其最新版本（包括任何修订）适用。

ISO 22300，安全和韧性-词汇

3 术语和定义

在本标准中，下列术语和定义ISO 22300 以下内容适用。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：可在https://www.iso.org/obp

— -IEC电子百科：可在https://www.electropedia.org/

3.1组织
具有管理职责、权限和组织结构以实现其目标的个人或群体（3.7）。

注1：组织的概念包括但不限于个体经营者、公司、法人团体、商号、企业、行政部门、合伙企业、慈善机构或机构，或其部分或组合，无论其是公共或私人的。

注2：如果组织是较大实体的一部分，术语“组织”仅指安全管理体系（3.5）范围内较大实体的一部分。

3.2利益相关方
个人或组织(3.1)能够被某一决定或活动影响，或认为自己被某一决定或活动影响的相关方。

3.3最高管理层

在最高管理层次上领导和控制一个组织的人或一群人(3.1)。

注1至:最高管理层在组织内部具有授权和提供资源的权力。

注2:如果管理体系(3.4)的范围只涵盖组织的一部分，那么最高管理者是指领导和控制该部分组织的人。

3.4管理体系

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

注1:管理体系可以是单个管理体系或多个管理体系的结合。

注2入:管理体系要素包括组织的结构、角色和责任、计划和实施。

3.5安全管理体系

组织用来管理其安全目标(3.7)并与安全方针(3.6)保持一致的一组要素、过程(3.9)和实施的管理体系。

3.6方针

由最高管理层正式批准和发布(3.3)的组织的意图和方向(3.1)。

3.7目标

客观的要达到的结果。

注1:目标可以是战略性的、战术的或可操作性的。

注2:目标可涉及不同学科(如金融、健康和安全以及环境)。例如，它们可以是组织范围的，也可以是特定于项目、产品和过程的(3.9)。

注3:目标可以以其他方式表达，例如预期结果、目的、操作标准、安全目标，或使用其他具有类似含义的词(例如:aim、goal或target)。

注4 :在安全管理体系(3.5)的背景下，安全目标是由组织(3.1)设定的，与安全方针(3.6)相一致，以实现特定的结果。

3.8风险

对目标的不确定性影响(3.7)。

注1:效果是与预期的偏差。它可以是积极的，也可以是消极的，或者两者兼而有之，它可以解决、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，可以应用在不同的级别。

注3:风险通常用风险来源、潜在事件、其后果及其可能性来表示。

3.9过程

一组将输入转化为输出的相互关联或相互作用的活动。

注1:流程的结果称为输出、产品还是服务，取决于引用的上下文。

3.10能力

运用知识和技能实现预期结果的能力

3.11成文信息

组织需要控制和维护的信息(3.1)以及它所在的介质

注1：记录的信息可以是任何格式和介质，也可以来自任何来源。注2：记录信息可参考：

— -管理体系（3.4），包括相关流程（3.9）；

— -为组织运作而创建的信息（文件）；

— -取得成果的证据（记录）。

3.12绩效

可衡量的结果

注1：绩效可以与定量或定性结果相关。

注2：绩效可能与管理活动、过程（3.9）、产品、服务、系统或组织有关（3.1）。

3.13持续改进
提高绩效的经常性活动(3.12)

3.14有效性
计划活动的实现程度和计划结果的实现程度

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”是指该组织(3.1)和相关方(3.2)的习俗或惯例，隐含考虑了相关方的需求或期望。

注2：规定的要求是指文件化信息中规定的要求(3.11)。

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
消除不符合原因的措施(3.17)并防止重复发生。

3.19审核

获取证据并对其进行客观评价的系统和独立程序（3.9），以确定满足审核标准的程度。

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（组合两个或多个专业）。

注2：内部审核由组织进行(3.1)自身，或由代表其的外部方。

注3：“审核证据”和“审核标准”的定义见ISO 19011标准。

3.20测量

确定数值的过程（3.9）

3.21监控

确定系统、过程（3.9）或活动的状态。

注1：为确定状态，可能需要检查、监督或严格观察。

4 组织

4.1 理解组织及其环境

组织应确定与其目的相关的外部和内部事项，以及影响其实现安全管理体系预期结果（包括其供应链要求）的能力的事项。

4.2 理解相关方的需求和期望

4.2.1 总则

组织应确定：

— -与安全管理体系相关的相关方；

— -这些相关方的相关要求；

— -哪些要求将通过安全管理体系解决。

4.2.2 法律、法规和其他要求

组织应：

a) 实施和维护一个程序，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) 确保在实施和维护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最新；

d) 适时将此信息传达给相关利益方。

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，尤其是保护价值。

组织应适用本标准中给出的原则图2并在4.2.3.2 到4.2.3.9中贯彻。

图2：原则

4.2.3.2 领导作用

各级领导要确立统一的目标和方向。最高管理者为各级领导创造条件，协调组织的战略、策略、程序和资源，以实现其目标。第5章对此原则进行了有关的要求。

4.2.3.3 基于最佳可用信息的结构化的综合过程方法

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的结果，如果将活动理解为相互关联的过程，并将其作为一个连贯的（统一的）系统进行管理，则可以更有效地实现这些结果。

4.2.3.4 客户定制化

供应链安全管理体系应围绕组织的目标并应根据组织的外部和内部环境和需求进行设计和维护。

4.2.3.5 包容性的人员参与

组织应适当和及时地使有关各方参与进来。并应适当考虑他们的知识、观点和看法，提高认识和促进信息安全管理。组织应确保各级的每个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一个组成部分。并应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——都应纳入安全管理体系。

4.2.3.7 动态的持续改进

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，对变化作出反应，并随着组织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所有方面都有重大影响，应在每个级别和阶段加以考虑。应根据对数据和信息的分析和评价作出决定，以确保这些决定更客观、对决策更有信心，应该考虑个人的看法，则更有可能产生预期的结果。

4.2.3.9 关系管理

为了持续成功，组织应管理其与所有利益相关方的关系，组织应该管理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中提到的外部和内部事项;

— -4.2中提到的要求.

范围应作为成文信息可用。

如果一个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，该组织应确保这些过程受到控制。此类外部提供的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、维护和持续改进安全管理体系，包括必需的过程及其相互作用。

5 领导力

5.1 领导力和承诺

最高管理层应通过以下方式展示对安全管理体系的领导和承诺：

— -确保制定安全策略和安全目标，并与组织的战略方向相一致；

— -确保识别和监控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；

— -确保将安全管理体系要求整合到组织的业务流程中；

— -确保安全管理体系所需的资源可用；

— -传达有效安全管理和符合安全管理体系要求的重要性；

— -确保安全管理体系达到预期效果；

— -确保安全管理目标、指标和方案的可行性；

— -确保组织其他部门产生的任何安保计划都能补充安保管理体系；

— -指导和支持人员对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；

— -支持其他相关角色，在其职责范围内展示其领导力。

注：本文件中提及的“业务”可以广义地解释为指那些对组织存在的目的至关重要的活动。

5.2 安全方针

5.2.1 制定安全方针

最高管理层应制定一项安全方针：

a) 符合组织的宗旨；

b) 提供设定安全目标的框架；

c) 包括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、计划等可能对组织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：

— -与组织的其他方针保持一致；

— -与组织的整体安全风险评估保持一致；

— -规定在收购或与其他组织合并，或该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其他变化时进行审查；

— —描述并分配主要责任人和管理责任；

— -形成成文信息信息并可用；

— -在组织内部进行沟通；

— -视情况提供给相关方。

注：各组织可以选择制定详细的安全管理策略供内部使用，该策略将提供足够的信息和指导，以推动安全管理体系（其中部分内容可能是保密的），并制定一份摘要（非保密）版本，其中包含广泛的目标，以分发给感兴趣的合作组织。

5.3 角色、责任和权限

最高管理者应确保相关角色的职责和权限在组织内得到分配和沟通。

最高管理者应分配以下职责和权限：

a) 确保安全管理体系符合本标准的要求；

b) 向最高管理层报告安全管理体系的绩效。

6 规划

6.1 应对风险和机遇的措施

6.1.1 总则

在规划安全管理体系时，组织应考虑4.1提到的事项以及4.2提到的要求并确定需要应对的风险和机遇：

— -确保安全管理体系能够达到预期结果；

— -防止或减少不良影响；

— -实现持续改进。

组织应规划：

a) 应对这些风险和机遇的措施；

b) 如何：

— -将措施整合并实施到其安全管理体系流程中；

— -评估这些措施的有效性。

管理风险的目的是创造和保护价值。风险管理应纳入安全管理体系。与组织及其相关方的安全相关的风险在8.3章节描述。

6.1.2 确定与安全相关的风险并识别机会

确定与安全相关的风险以及识别和利用机会进行主动风险评估，该评估应包括但不限于：

a) 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，包括影响组织安全的组织控制之外的因素；

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) 与安全威胁和漏洞有关的信息；

f) 供应商之间的相互依赖关系。

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提供以下信息（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) 安全管理流程；

e) 安全管理体系的设计、规范和实施；

f) 确定充足的资源，包括人员配备；

g) 确定培训需求和所需的能力水平。

6.2 安全目标和实现目标的规划

6.2.1 建立安全目标

组织应在相关职能和层次上制定安全目标。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) 被监监视；

e) 被沟通；

f) 适当时进行更新；

g) 保留安全目标信息并可用。

6.2.2 确定安全目标

在规划如何实现其安全目标时，组织应确定：

-要做什么；

— -需要哪些资源；

— -谁将负责；

— -何时完成；

— 如何评估结果。

在制定和审查其安全目标时，组织应考虑：

a) 技术、人力、行政和其他选择；

b) 对相关利益方的影响。

安全目标应与组织持续改进的承诺一致。

6.3 供应链安全管理体系的变更规划

当组织确定需要变更安全管理体系时，包括第10章识别的变更，变更应按计划的方式进行。

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) 资源的可用性；

d) 职责和权限的分配或重新分配。

7 支持

7.1 资源

组织应确定并提供建立、实施、维护和持续改进安全管理体系所需的资源。

7.2 能力

组织应：

— -确定在其控制下从事影响其安全绩效的工作的人员的必要能力；

— -确保这些人员在适当的教育、培训或经验基础上胜任工作，并获得适当的安全许可；

— -在适用的情况下，采取措施获得必要的能力，并评估所采取措施的有效性；

保存适当的成文信息作为能力证据。

注：适用的措施可包括，例如：针对现有人员提供培训、指导或重新分配；或聘任或签约有能力的人员。

7.3 意识

在组织控制下工作的人员应了解：

— -安全方针；

— 他们对安全管理体系有效性的贡献，包括改进安全性能的好处；

— 不符合安全管理体系要求所带来的影响；

— 他们在遵守安全管理方针和程序以及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；

— -关注信息在传播之前的敏感性。

7.5 成文的信息

7.5.1 总则

组织的安全管理体系应包括：

a) 本标准要求的成文信息；

b) 组织确定的、为安全管理体系有效性所必需的成文信息。

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间表。

注：安全管理体系的成文信息范围因组织而异，原因如下：

— -组织的规模及其活动、过程、产品和服务的类型；

— -过程及其相互作用的复杂性；

— -人的能力。

组织应确定信息的价值，并建立所需的完整性层级和安全控制，以防止未经授权的访问。

7.5.2 创建和更新

在创建和更新成文信息时，组织应确保：

— -标识和描述（如标题、日期、作者或编号）；

— -格式（如语言、软件版本、图形）和介质（如纸质、电子版）；

— -审查和批准适用性和充分性。

7.5.3 成文信息的控制

应控制安全管理体系和本标准要求的成文信息，以确保：

a) 在需要使用的地点和时间，文件是可用的和适宜的；

b) 其得到充分保护（例如，不受保密性损失、不当使用或完整性损失的影响）；

c) 必要时定期审查和修订，并由授权人员批准其充分性；

d) 及时从所有发布点和使用点删除过时的文件、数据和信息，或以其他方式确保不会意外使用；

e) 出于法律或知识保存目的保留的档案文件、数据和信息，或两者都经过适当标识。

为控制成文信息，组织应在适用的情况下处理以下活动：

— -分发、获取、检索和使用；

— -储存和保存，包括保存易读性；

— -变更控制（如版本控制）；

— -保留和处置。

组织确定的安全管理体系规划和运行所需的外来文件化信息，应适当予以识别和控制。

注：访问可能意味着决定是否仅允许查看记录的信息，或是否允许和授权查看和更改记录的信息。

8 运行

8.1 运行的规划和控制

组织应规划、实施和控制为满足要求所需的过程，并通过以下方式实施第6.1章中确定确定的控制来：

— -建立过程的准则；

— -按准则实施过程的控制。

文件化信息应在必要的程度上可用，以确保过程已按计划执行。

8.2 过程和活动的识别

组织应确定实现以下目标所需的过程和活动：

a) 遵守其安全策略；

b) 遵守法律、法规和监管安全要求；

c) 其安全管理目标；

d) 安全管理系统的交付；

e) 供应链所需的安全级别。

8.3 风险评估和处置

组织应实施并保持风险评估和处置流程。

注：风险评估和处置流程见 ISO31000。

本组织应：

a) 识别其安全相关风险，根据其安全管理所需的资源对其进行优先排序；

b) 分析和评估已识别的风险；

c) 确定哪些风险需要处置；

d) 选择并实施解决这些风险的方案；

e) 制定并实施风险处理计划。

注：本款中的风险与组织及其相关方的安全有关。与管理体系有效性相关的风险和机遇见6.1章节

8.4 控制

8.2中所列的过程应包括对人力资源管理的控制，以及设备、仪器仪表和信息技术的安全相关项目的设计、安装、操作、更新和修改。对现有安排进行修订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与安全相关的相关风险。拟考虑的新安排或订正安排应包括:

a) 修订组织结构、角色或职责；

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) 修订流程和程序；

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) 适用时引进新的承包商、供应商或人员；

g) 外部供应商的安全保证要求。

组织应控制计划的变更，并审查非预期变更的后果，必要时采取措施减轻任何不利影响。

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 安全方针、程序、流程和处理

8.5.1 策略和处置的识别和选择

组织应实施和维护体系化流程，以分析与安全相关的漏洞和威胁。基于这种脆弱性和威胁分析以及随后的风险评估，组织应确定并选择一种安全策略，该策略包括一个或多个程序、过程和处理方法。

识别应基于策略、程序、过程和应对措施的程度：

a) 维护组织的安全；

b) 降低安全漏洞的可能性；

c) 降低实施威胁的可能性；

d) 缩短任何安全处理缺陷的周期，并限制其影响；

e) 提供充足的资源。

选择应基于策略、过程和处置的程度：

— -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；

— -考虑相关的成本和收益。

8.5.2 所需资源

组织应确定实施所选安全程序、过程和处理的资源要求。

8.5.3 处理的实施

组织应实施并维持选定的安全处理措施。

8.6 安全计划

8.6.1 总则

组织应根据选定的策略和处理方法，制定并记录安全计划和程序。组织应实施并维持一个响应机制，以便及时有效地向相关利益方发出与安全和迫在眉睫的安全威胁或持续的安全违规相关的漏洞警告和沟通。响应结构应提供在迫在眉睫的安全威胁或持续的安全违规期间管理组织的计划和程序。

8.6.2 响应机制

组织应实施和维护一个机制，确定负责应对安全漏洞和威胁的指定人员或一个或多个团队。指定人员或每个团队的角色和责任以及人员或团队之间的关系应明确确定、沟通和记录。

总体而言，团队应能够：

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，这些阈值证明启动正式响应是合理的；

c) 启动适当的安全响应；

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、威胁行为人的意图和能力的变化或安全违规行为的影响，以及组织的响应；

g) 启动安全处理；

h) 与相关利益方、当局和媒体进行沟通；

i) 与沟通管理部门一起制定沟通计划。对于每个指定人员或团队，应：

— -确定的员工，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；

— -指导其行动的文件化程序，包括响应的启动、操作、协调和沟通程序。

8.6.3 警告与沟通

组织应记录并维护以下程序：

a) 与相关利益方进行内部和外部沟通，包括什么、何时、与谁以及如何沟通；

注：组织可以记录和维护有关组织如何以及在何种情况下与员工及其紧急联系人沟通的程序。

b) 接收、记录和回复相关方的通信，包括任何国家或区域风险咨询体系或同等体系；

c) 确保在安全违规、漏洞或威胁期间通信手段的可用性；

d) 促进与安全威胁和/或违规响应者的结构化沟通；

e) 提供组织在违反安全规定后的媒体回应细节，包括沟通策略；

f) 记录安全违规的细节、采取的行动和做出的决定。在适用的情况下，还应考虑并实施以下

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；

— -确保多个响应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。

8.6.4 安全计划的内容

组织应记录并维护安全计划。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。

总体而言，安全计划应包括：

a) 团队将采取的行动细节：

1) 继续或恢复约定的安全状态；

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，以及组织的应对措施；

b) 参考预定义阈值和启动响应的过程；

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行为的直接后果的详细信息，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。每个计划应包括：

— -其宗旨、范围和目标；

— -实施计划的团队的角色和职责；

— -实施解决方案的行动；

— -启动（包括启动标准）、操作、协调和沟通团队行动所需的信息；

— -内部和外部的相互依赖；

— -所需资源；

— -报告要求；

— -退出的过程。

每个计划都应该在需要的时间和地点可用。

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 绩效评估

9.1 监测、测量、分析和评价

组织应确定需要监测和测量的内容;

— -监测、测量、分析和评价的方法(如适用)，以确保结果有效;

— 应在何时进行监视和测量;

— -对监视和测量的结果进行分析和评价时；

— -在评估时，对监视和测量的结果进行分析。

应提供文件化信息作为结果的证据。

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

组织应按计划的时间间隔进行内部审核，以提供有关安全管理体系是否：

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) 有效实施和维护。

9.2.2 内部审核方案

组织应计划、建立、实施和维护审计计划，包括频率、方法、责任、计划要求和报告。

在制定内部审核计计划时，组织应考虑相关过程的重要性和以往审核的结果。

组织应：

a) 定义每次审核的目标、标准和范围；

b) 选择审核员并进行内审，以确保审核过程的客观性和公正性；

c) 确保审核结果报告给相关经理。

d) 核实安全设备和人员是否得到适当部署；

e) 确保及时采取任何必要的纠正措施，以消除发现的不合格及其原因；

f) 确保后续审核行动包括对所采取行动结果的验证和验证结果的报告。

保留成文信息作为实施审核计划和审核结果的证据。

内审计划，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结果为基础。审核程序应涵盖范围、频率、方法和能力，以及进审核和报告结果的责任和要求。

9.3 管理评审

9.3.1 总则

最高管理者应按计划的时间间隔审查组织的安全管理体系，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结果，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予以落实和解决。

注：组织可以使用安全管理体系的过程，如领导、规划和绩效评估，以实现改进。

9.3.2 管理评审 输入

管理评审应包括：

a) 以往管理评审的行动状态；

b) 与安全管理体系相关的外部和内部问题的变化；

c) 与安全管理体系相关的相关方需求和期望的变化；

d) 有关安全性能的信息，包括以下方面的趋势：

1) 不符合项和纠正措施；

2) 监测和测量结果；

3) 审核结果；

e) 持续改进的机会；

f) 审核和评估是否符合法律要求和组织认可的其他要求的结果；

g) 外部相关方的沟通，包括投诉；

h) 组织的安全绩效；

i) 达到目标和指标的程度；

j) 纠正措施的状态；

k) 以往管理评审的后续行动；

l) 不断变化的情况，包括与安全方面有关的法律、监管要求和其他要求的更新发展情况；

m) 改进建议。

9.3.3 管理评审结果

管理评审的结果应包括与持续改进机会有关的决定，以及安全管理体系变更的任何需要。

保留成文信息应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。本组织应积极寻求改进机会，即使不是因为与安全相关的漏洞和迫在眉睫的安全威胁或相关利益方正在发生的安全违规行为的改进机会。

10.2 不符合和纠正措施

当不符合发生时，组织应：

a) 对不符合作出反应，如适用：

1) 采取措施控制和纠正它；

2) 处理后果；

b) 通过以下方式评估消除不符合原因的行动需求，以使其不再发生或不在其他地方发生：

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) 实施任何必要的措施；

d) 审查所采取的任何纠正措施的有效性；

e) 如有必要，对安全管理体系进行变更。

纠正措施应与所遇到的不符合的影响相适应。保存文件化信息应作为以下证据：

— -不符合的性质以及随后采取的任何措施；

— -任何纠正措施的结果；

— -与安全相关的调查：

— 故障，包括未遂事故和误报警；

— 事件和紧急情况；

— 不符合；

— 采取措施减轻此类故障、事件或不符合产生的任何后果。

在纠正措施实施之前，通过安全相关风险评估程序对所有拟制的纠正措施进行审查，除非立即实施可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称。

参考文献

[1] 国际标准化组织 9001，质量管理体系-要求

[2] 国际标准化组织 14001，环境管理体系 要求

[3] 国际标准化组织 19011，管理体系审核指南

[4] 国际标准化组织 22301、安全性和韧性——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、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-供应链韧性的发展-要求和使用指南

[8] 国际标准化组织 28003，供应链安全管理体系-对提供供应链安全管理体系的审核和认证

[9] 国际标准化组织 28004-1，供应链安全管理体系.ISO 28000实施指南.第1部分：一般原则

[10] 国际标准化组织 28004-3，供应链安全管理体系-ISO 28000实施指南-第3部分：中小企业（海港除外）采用ISO 28000的附加具体指南

[11] 国际标准化组织 28004-4，供应链安全管理体系ISO 28000实施指南-第4部分：达到ISO 28001管理目标，所实施ISO 28000的附加具体指南

[12] 国际标准化组织 31000，风险管理-指南

[13] 国际标准化组织 45001职业健康和安全管理体系-要求和使用指南

[14] 国际标准化组织 指导 73，风险管理-术语和定义