国际标准

ISO 28000

第二版
2022-03

安全性和弹性——安全管理系统要求

Security and resilience — Security management systems Requirements

参考号 ISO 28000:2022(E)

受版权保护的文件

国际标准化组织版权办公室
CP 401？栗色de Blandonnet
8 CH-1214 Vernier，日内瓦
电话:+41 22 749 01 11
copyright@iso.org
网站:www.iso.org

在瑞士出版

内容页

序

ISO(国际标准化组织)是国家标准机构(ISO成员机构)的全球联盟。制定国际标准的工作通常是通过ISO技术委员会进行的。对已成立技术委员会的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有联系的政府和非政府国际组织也参与这项工作。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文件的程序以及旨在进一步维护本文件的程序。特别是，应注意不同类型的ISO文件需要不同的批准标准。本文件是根据ISO/IEC指令第2部分的编辑规则起草的(参见www.iso.org/directives).

请注意，本文件中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。在文档开发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专利声明列表中列出(参见www.iso.org/patents).

本文档中使用的任何商品名称都是为了方便用户而提供的信息，并不构成认可。

有关标准自愿性质的解释、与合格评定相关的ISO特定术语和表述的含义，以及有关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，请参见www.iso.org/iso/foreword.html.

本文件由ISO/TC 292技术委员会编制，*安全性和弹性*。

第二版取消并取代了第一版(ISO 28000:2007),第一版经过了技术修订，但保留了现有要求，以便为使用前一版的组织提供连续性。主要变化如下:

— 增加了关于原则的建议第4条更好地与ISO 31000协调；

— 在中添加了建议第8条为了更好地与ISO 22301保持一致，促进整合，包括:

  — 安全策略、程序、过程和处理；

  — 安全计划。

关于本文件的任何反馈或问题应提交给用户的国家标准机构。这些机构的完整清单可在以下网址找到www.iso.org/members.html.

介绍

大多数组织都面临着安全环境日益增加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，他们希望在其管理系统中系统地解决这些问题。安全管理的正式方法可以直接提高组织的业务能力和可信度。

本文件规定了安全管理系统的要求，包括对供应链安全保证至关重要的方面。它要求本组织:

— 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与安全相关的风险；

— 管理组织对法定、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。

安全管理与业务管理的许多方面都有联系。它们包括由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。应考虑对组织的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他们的提供商满足相关的安全标准，作为被包括在该供应链中的条件，以便满足安全管理的要求。

本文件将计划-执行-检查-行动(PDCA)模式应用于组织安全管理体系的计划、建立、实施、运行、监控、评审、维护和持续改进的有效性，参见表1和图1.

表PDCA模型的解释

计划(建立)	建立与提高安全性相关的安全策略、目标、指标、控制措施、流程和程序，以交付与组织的总体策略和目标相一致的结果。
做 (实施和操作)	实施和运行安全政策、控制措施、流程和 程序。
支票 (监控和审查)	对照安全策略和目标监控和审查绩效，将结果报告给管理层进行审查， 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，通过采取纠正措施和重新评估安全管理系统的 范围和安全政策及目标，维护和改进安全管理系统。

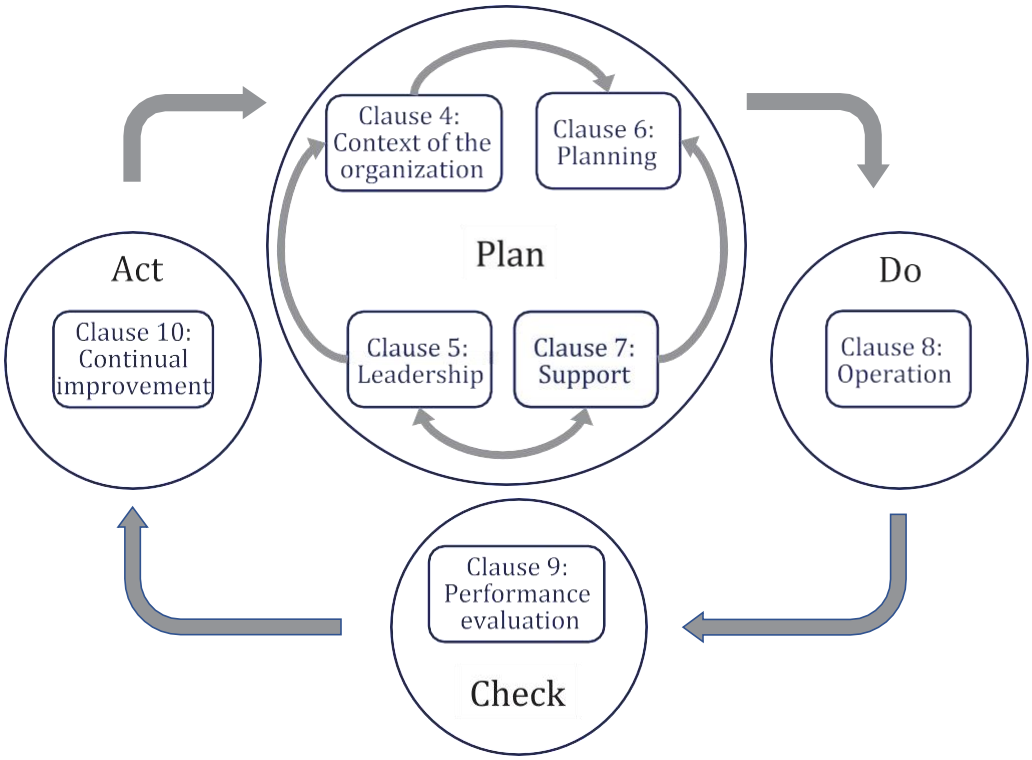

图1 —应用于安全管理体系的PDCA模型

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。，从而支持相关管理系统的一致和集成的实施和操作。

对于有此愿望的组织，安全管理体系与本文件的符合性可通过外部或内部审核过程进行验证。

安全性和弹性—安全管理系统—要求

1 范围

本文件规定了安全管理系统的要求，包括与供应链相关的方面。

本文件适用于打算建立、实施、维护和改进安全管理体系的所有类型和规模的组织(如商业企业、政府或其他公共机构和非营利组织)。它提供了一个整体和通用的方法，而不是特定的行业或部门。

本文件可在组织的整个生命周期中使用，并适用于所有层次的任何内部或外部活动。

2 引用标准

以下文件在文本中被引用，其部分或全部内容构成本文件的要求。对于注明日期的参考文献，仅引用的版本适用。对于未注明日期的引用文件，引用文件的最新版本(包括任何修订)适用。

ISO 22300，*安全性和弹性—词汇*

3 术语和定义

在本文件中，ISO 22300和以下给出的术语和定义适用。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:可从以下网址获得https://www.iso.org/obp

— IEC电子百科:可从以下网址获得https://www.electropedia.org/

3.1
组织
一个人或一群人，他们有自己的职责、权力和关系来实现自己的目标*目标*(3.7)

条目注释1:组织的概念包括但不限于独资经营者、公司、法人、商行、企业、当局、合伙企业、慈善机构或机构，或其一部分或组合，无论是注册或非注册、公有或私有。

注2:如果该组织是一个较大实体的一部分，术语“组织”仅指该较大实体中属于*安全管理系统*(3.5).

3.2
有关的当事人(首选术语)
利益相关者(公认术语)
人或*组织*(3.1)能够影响决策或活动、被决策或活动影响或认为自己被决策或活动影响

3.3
高管理层
指挥和控制一个或一群人*组织*(3.1)在最高层

条目注释1:最高管理者有权在组织内授权和提供资源。

条目的注释2:如果*管理系统*(3.4)只涵盖组织的一部分，那么高层管理人员是指那些指导和控制组织那部分的人。

3.4
管理系统
的一组相互关联或相互作用的元素*组织*(3.1)来建立*政策*(3.6)和
目标(3.7)，以及*处理*(3.9)来实现这些目标

条目注释1:一个管理体系可以针对一个或几个学科。

条目注2:管理体系要素包括组织的结构、角色和职责、策划和运作。

3.5
安全管理系统
协调系统*政策*(3.6),*处理*(3.9)和组织管理其安全性的实践*目标*(3.7)

3.6
政策
安的意图和方向*组织*(3.1)正如其正式表达的那样*高管理层*(3.3)

3.7
目标
要取得的结果

条目注释1:目标可以是战略的、战术的或操作的。

条目注释2:目标可以与不同的学科相关(如财务、健康和安全以及环境)。例如，它们可以是整个组织的，也可以是特定于某个项目、产品和*过程*(3.9).

注3:目标可以用其他方式表达，如预期结果、目的、操作标准、安全目标，或使用具有类似含义的其他词语(如目的、目标或目标)。

条目注释4:在上下文中*安全管理系统*(3.5)，安全目标由*组织*
(3.1)，与安全一致*政策*(3.6)，以达到特定的效果。

3.8
危险
不确定性对的影响*目标*(3.7)

条目注释1:影响是与预期的偏差。它可以是积极的，也可以是消极的，或者两者兼而有之，并且可以处理、创造或导致机会和威胁。

条目注释2:目标可以有不同的方面和类别，并且可以应用于不同的级别。

条目注释3:风险通常以风险源、潜在事件、其后果和可能性来表示。

3.9
过程
使用或转换输入以交付结果的一组相关或交互活动

条目注释1:一个过程的结果是称为产出、产品还是服务取决于上下文
引用的。

3.10
能力
运用知识和技能实现预期结果的能力

3.11
记录的信息
需要由控制和维护的信息*组织*(3.1)和包含它的介质

条目注释1:记录的信息可以是任何格式和媒体，也可以来自任何来源。条目注释2:记录的信息可

参考:

— 这*管理系统*(3.4)，包括相关的*处理*(3.9);

— 为组织运作而创建的信息(文档)；

— 取得成果的证据(记录)。

3.12
表演
可测量的结果

条目注释1:绩效可以与定量或定性结果相关。

条目注2:绩效可能与管理活动有关，*处理*(3.9)、产品、服务、系统或
组织(3.1).

3.13
持续改进
要增强的重复性活动*表演*(3.12)

3.14
有效性
计划的活动得以实现和计划的结果得以实现的程度

3.15
要求
明确的、通常隐含的或必须的需求或期望

条目注1:“一般暗示”指的是习惯或惯例*组织*(3.1)和
当事人(3.2)所考虑的需求或期望是隐含的。

条目注2:规定的要求是一种陈述的要求，例如*记录的信息*(3.11).

3.16
一致
履行*要求*(3.15)

3.17
不一致
不履行*要求*(3.15)

3.18
校正动作
消除故障原因的措施*不一致*(3.17)并防止复发

3.19
审计
系统和独立*过程*(3.9)获取证据并对其进行客观评估，以确定符合审计准则的程度

条目注释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)，也可以是组合审核(两个或两个以上学科的组合)。

条目注释2:内部审计由*组织*(3.1)本身，或者由外部方代表它。

条目注释3:“审计证据”和“审计标准”在ISO 19011定义。

3.20
尺寸
过程(3.9)来确定一个值

3.21
监视
确定系统的状态*过程*(3.9)或一项活动

条目注释1:为了确定状态，可能需要检查、监督或严格观察。

4 本组织的背景

4.1 了解组织及其背景

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的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 一般

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；

— 这些要求中的哪些将通过安全管理系统来解决。

4.2.2 法律、法规和其他要求

本组织应:

a) 实施并保持一个流程，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更新；

d) 适当时将这些信息传达给相关的相关方。

4.2.3 原则

4.2.3.1 一般

组织内安全管理的目的是创造价值，尤其是保护价值。

组织应该应用中给出的原则图2并在中进行了描述4.2到4.2.

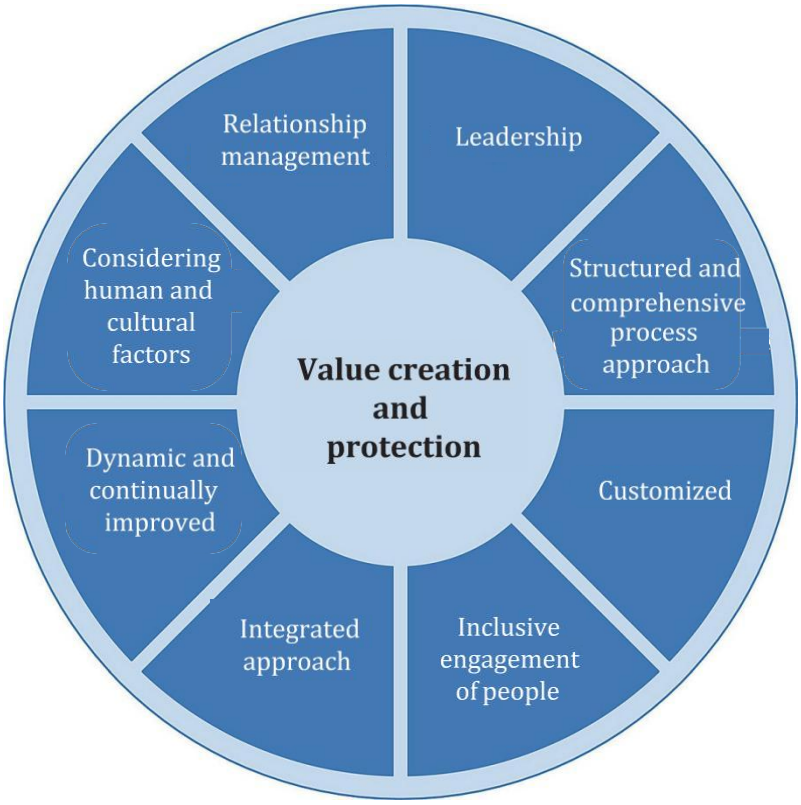

图2 —原则

4.2.3.2 领导力

各级领导应该确立统一的目标和方向。他们应该创造条件，协调组织的战略、政策、过程和资源，以实现其目标。第5条解释与此原则相关的要求。

4.2.3.3 基于最佳可用信息的结构化综合流程方法

包括供应链在内的结构化综合安保管理方法应有助于取得一致和可比的结果，如果将各项活动理解为作为一个连贯系统运作的相互关联的过程并加以管理，将更有成效和效率地实现这些结果。

4.2.3.4 定制

安全管理系统应该是定制的，并与组织的外部和内部环境和需求相称。它应该与其目标相关联。

4.2.3.5 人民的包容性参与

组织应当适当并及时地让相关方参与进来。It部门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安全管理。本组织应确保所有级别的每个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不可或缺的一部分。它应当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——都应该集成到安全管理系统中。

4.2.3.7 充满活力并持续改进

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，并随着组织内外环境的变化创造新的机会。

4.2.3.8 考虑到人文因素

人的行为和文化对安全管理的所有方面都有重大影响，应该在每个级别和阶段加以考虑。决策应基于对数据和信息的分析和评估，以确保决策更客观、更有信心，更有可能产生预期结果。应该考虑个人的看法。

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利益方的关系，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。

在确定这一范围时，组织应考虑

— 中提到的外部和内部问题 4.1;

— 4.2中提到的要求。4.2.

该范围应作为文件化的信息提供。

如果组织选择由外部提供影响其安全管理体系符合性的任何流程，组织应确保此类流程得到控制。应在安全管理体系中确定对这种外部提供的过程的必要控制和责任。

4.4 安全管理系统

组织应根据本文件的要求，建立、实施、维护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 领导能力

5.1 领导和承诺

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。

— 确保安全政策和安全目标已经确立，并与组织的战略方向相一致。

— 确保识别和监测组织相关方的要求和期望，并及时采取适当行动管理这些期望，以确保将安全管理系统的要求纳入组织的业务流程。

— 确保将安全管理系统的要求整合到组织的业务流程中。

— 确保安全管理系统所需的资源是可用的。

— 传达有效安全管理和符合安全管理系统要求的重要性。

— 确保安全管理系统实现其预期结果。

— 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对安全管理系统的补充。

— 指导和支持人员为安全管理系统的有效性作出贡献。

— 促进组织的安全管理系统的持续改进。

— 支持其他相关角色在其职责范围内展现其领导力。

注意 本文件中提到的 "业务 "可被广义地解释为对组织存在的目的具有核心意义的那些活动。

5.2 安全政策

5.2.1 确立安全政策

最高管理层应制定一项安全政策，该政策

a) 与组织的目的相适应。

b) 为设定安全目标提供一个框架。

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系统的承诺。

e) 考虑到安全政策、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 安全政策要求

安全政策应

— 与其他组织的政策一致。

— 与组织的整体安全风险评估相一致。

— 规定在收购或与其他组织合并的情况下，或在组织的业务范围发生可能影响安全管理系统的连续性或相关性的其他变化时，对其进行审查。

— 描述并分配主要责任和结果责任。

— 以文件化信息的形式提供。

— 在组织内部进行交流。

— 适当地提供给相关方。

注：组织可以选择制定详细的安全管理政策供内部使用，为推动安全管理系统提供足够的信息和方向（其中部分内容可以保密），并有一个包含广泛目标的摘要（非保密）版本，以便向有关方面传播。

5.3 角色、责任和权力

最高管理层应确保相关角色的责任和权限在组织内得到分配和沟通。

最高管理层应指定以下的责任和权力。

a) 确保安全管理体系符合本文件的要求。

b) 向最高管理层报告安全管理体系的绩效。

6 规划

6.1 应对风险和机遇的行动

6.1.1 一般情况

在对安全管理体系进行规划时，组织应考虑以下内容中提到的问题 4.1 中提到的问题，以及4.2中提到的要求。4.2 并确定需要应对的风险和机会，以便

— 保证安全管理体系能够实现其预期结果。

— 防止或减少不希望出现的效果。

— 实现持续的改进。组织应计

划。

a) 应对这些风险和机遇的行动。

b) 如何。

— 将这些行动纳入其安全管理系统流程并加以实施。

— 评估这些行动的有效性。

管理风险的目的是为了创造和保护价值。管理风险应被纳入安全管理系统。与组织及其相关方的安全有关的风险在以下内容中述及 8.3.

6.1.2 确定与安全相关的风险和识别机会

确定与安全相关的风险并识别和利用机会，需要进行主动的风险评估，这应包括对以下方面的考虑，但不限于此。

a) 物理或功能故障以及恶意或犯罪行为。

b) 环境、人力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、知识和通信管理。

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 应对安全相关风险和利用机会

对已识别的安全相关风险的评估应提供给（但不限于）以下方面的投入。

a) 組織的整體風險管理。

b) 风险处理。

c) 安全管理目标。

d) 安全管理程序。

e) 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 安全目标和实现这些目标的计划

6.2.1 确立安全目标

组织应在相关的职能和级别上建立安全目标。这些安全目标应

a) 与安全政策一致。

b) 是可衡量的（如果可行）。

c) 考虑到适用的要求。

d) 受到监控。

e) 进行沟通。

f) 适当地更新。

g) 作为文件化的信息提供。

6.2.2 确定安全目标

在计划如何实现其安全目标时，组织应确定。

— 将要做什么？

— 需要什么资源？

— 谁将负责。

— 何时完成。

— 如何对结果进行评估。

在建立和审查其安全目标时，一个组织应考虑到。

a) 技术、人力、行政和其他选择。

b) 有关各方的意见和影响。

安全目标应与组织对持续改进的承诺相一致。
完善。

6.3 变革的规划

当组织确定需要对安全管理系统进行变更时，包括在第10条中确定的那些变更。第10条时，应以有计划的方式进行变更。

组织应考虑

a) 变更的目的及其潜在后果。

b) 安全管理系统的完整性。

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系统所需的资源。

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。

— 确保这些人在适当的教育、培训或经验的基础上具备能力，并通过适当的安全审查。

— 在适用的情况下，采取行动以获得必要的能力，并评估所采取行动的有效性。

应提供适当的文件化信息作为能力的证据。

注意 适用的行动可以包括，例如：为目前的雇员提供培训、指导或重新分配；或者雇用或签约有能力的人。

7.3 认识

在组织控制下从事工作的人员应了解

— 安全政策。

— 他们对安全管理系统的有效性的贡献，包括改善安全性能的好处。

— 不符合安全管理体系要求的影响。

— 他们在遵守安全管理政策和程序以及安全管理系统的要求方面的作用和责任，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

— 沟通的内容。

— 何时沟通？

— 与谁沟通？

— 沟通的方式。

— 信息在传播前的敏感性。

7.5 记录的信息

7.5.1 一般情况下

组织的安全管理系统应包括

a) 本文件所要求的文件化信息。

b) 组织认为对安全管理系统的有效性有必要的文件化信息。

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手段和时限。

注：安全管理系统的文件化信息的范围可能因不同的组织而不同，原因如下。

— 组织的规模及其活动、流程、产品和服务的类型。

— 流程的复杂性及其相互作用。

— 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 创建和更新文件化的信息

在创建和更新记录的信息时，组织应确保适当的。

— 识别和描述（例如，标题、日期、作者或参考编号）。

— 格式（例如，语言、软件版本、图形）和媒介（例如，纸张、电子）。

— 审查和批准是否合适和充分。

7.5.3 对文件化信息的控制

安全管理体系和本文件所要求的文件化信息应得到以下控制
控制，以确保

a) 在需要的地方和时间，它是可获得的并适合使用的。

b) 它得到充分的保护（例如，防止保密性的丧失、不当使用或完整性的丧失）。

c) 定期审查，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移除，或以其他方式保证不会被意外使用。

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。

对于文件化信息的控制，组织应酌情处理以下活动。

— 分发、访问、检索和使用。

— 存储和保存，包括保持可读性。

— 对变更的控制（例如，版本控制）。

— 保留和处置。

应酌情识别和控制由组织确定为安全管理系统的规划和运行所必需的外部来源的文件信息。

注：访问可以意味着关于只查看文档信息的许可，或查看和更改文档信息的许可和授权的决定。

8 操作

8.1 运行规划和控制

组织应计划、实施和控制满足要求所需的过程，并实施第6条确定的行动。第6条通过以下方式

— 建立过程的标准。

— 按照标准实施对过程的控制。

应在必要的范围内提供文件化的信息，以使人们相信这些过程已按计划实施。

8.2 过程和活动的识别

组织应确定那些实现以下目标所必需的过程和活动。

a) 遵守其安全政策。

b) 遵守法律、法规和监管机构的安全要求。

c) 其安全管理目标。

d) 提供其安全管理系统。

e) 供应链的必要安全水平。

8.3 风险评估和处理

组织应实施并维护风险评估和处理流程。

注意 风险评估和处理的过程在ISO 31000中涉及。

组织应

a) 识别其与安全相关的风险，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) 确定哪些风险需要处理。

d) 选择并实施应对这些风险的方案。

e) 准备和实施风险处理计划。

注意 本子条款中的风险与组织及其相关方的安全有关。与管理体系的有效性有关的风险和机会在以下内容中处理 6.1.

8.4 控制措施

中所列的过程。8.2 应包括对人力资源管理的控制，以及酌情对与安全有关的设备、仪器和信息技术项目的设计、安装、操作、翻新和修改进行控制。在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与安全相关的风险。要考虑的新的或修订的安排应包括

a) 修订组织结构、角色或责任。

b) 培训、意识和人力资源管理。

c) 修订的安全管理政策、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，其中可能包括硬件和/或软件。

f) 酌情引进新的承包商、供应商或人员。

g) 对外部供应商的安全保证要求。

组织应控制计划中的变更，并审查非预期变更的后果，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 安全战略、程序、过程和处理方法

8.5.1 战略和处理方法的识别和选择

组织应实施并保持系统化的流程，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，组织应确定并选择由一个或多个程序、过程和处理方法组成的安全策略。

识别应基于战略、程序、过程和处理的程度。

a) 维护组织的安全。

b) 减少出现安全漏洞的可能性。

c) 减少威胁实现的可能性。

d) 缩短任何安全处理缺陷的时间并限制其影响。

e) 提供足够的资源。

选择应基于战略、流程和处理方法的程度。

— 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。

— 考虑相关的成本和收益。

8.5.2 资源要求

组织应确定实施所选安全程序、流程和处理方法的资源要求。

8.5.3 实施处理方法

组织应实施并维护选定的安全处理方法。

8.6 安全计划

8.6.1 一般情况下

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。组织应实施并维护一个响应结构，以便及时有效地警告并向有关方面通报与安全有关的漏洞和即将发生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组织。

8.6.2 应对结构

组织应实施并维护一个结构，确定一个指定人员或一个或多个团队，负责应对与安全有关的漏洞和威胁。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。

集体而言，这些小组应该有能力

a) 评估安全威胁的性质和程度及其潜在影响。

b) 根据预先确定的阈值评估影响，以证明启动正式响应的合理性。

c) 启动适当的安全响应。

d) 计划需要采取的行动。

e) 以生命安全为第一优先，确定优先事项。

f) 监测与安全有关的脆弱性的任何变化、威胁者的意图和能力的变化或安全违规行为的影响以及组织的反应。

g) 启动安全处理。

h) 与有关各方、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。每个指定的人或团队都应

该有。

— 确定的工作人员，包括具有履行其指定职责的必要责任、权力和能力的候补人员。

— 指导其行动的文件化程序，包括应对措施的启动、运行、协调和沟通程序。

8.6.3 警告和沟通

组织应记录并维护以下程序

a) 向有关各方进行内部和外部沟通，包括沟通的内容、时间、对象和方式。

注意 组织可以记录并保存有关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、记录和回应相关方的通信，包括任何国家或地区风险咨询系统或同等机构。

c) 确保在发生安全违规、漏洞或威胁期间，通信手段的可用性。

d) 促进与安全威胁和/或违规行为应对者的结构化沟通。

e) 提供本组织在发生安全违规事件后的媒体反应的细节，包括沟通策略。

f) 记录安全违规行为的细节、所采取的行动和所做的决定。在适用的情况下，还应该考

虑并实施以下措施。

— 提醒可能受到实际或即将发生的安全违规事件影响的有关各方。

— 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的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，并协助组织进行响应和恢复其安全。

总体而言，安全计划应包含

a) 团队将采取的行动的细节，以

1) 继续或恢复商定的安全状态。

2) 监测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响应。

b) 参考预先定义的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）损失或无法使用。每个计划应包括

— 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存关系。

— 其资源要求。

— 其报告要求。

— 撤出的过程。

每个计划都应该是可用的，并在需要的时间和地点提供。

8.6.5 恢复

组织应拥有记录在案的流程，以从安全违规行为发生之前、期间和之后采取的任何临时措施中恢复组织的安全。

9 性能评估

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。

— 何时应进行监测和测量。

— 何时对监测和测量的结果进行分析和评价。

应提供有记录的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 内部审计

9.2.1 总则

组织应按计划的时间间隔进行内部审计，以提供有关安全管理体系是否符合的信息。

a) 是否符合。

   1) 组织自身对其安全管理体系的要求。

   2) 本文件的要求。

b) 是否得到有效实施和维护。

9.2.2 内部审计计划

组织应计划、建立、实施和保持审计计划，包括频率、方法、责任、计划要求和报告。

在制定内部审计计划时，组织应考虑相关过程的重要性和以往的审计结果。

该组织应

a) 确定每次审计的目标、标准和范围。

b) 选择审计人员并进行审计，以确保审计过程的客观性和公正性。

c) 确保将审计结果报告给相关管理人员。

d) 核实安全设备和人员的适当部署。

e) 确保采取任何必要的纠正措施，不作无谓的拖延，以消除发现的不符合要求的情况及其原因。

f) 确保后续审计行动包括核查所采取的行动和报告核查结果。

应提供文件化的信息，作为实施审核方案和审核结果的证据。

审计方案，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计的结果。审计程序应涵盖范围、频率、方法和能力，以及进行审计和报告结果的责任和要求。

9.3 管理审查

9.3.1 一般情况下

最高管理层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产出，以确定是否存在与业务或安全管理系统相关的需求或机会，并将其作为持续改进的一部分加以解决。

注：组织可利用安全管理体系的流程，如领导、计划和绩效评估，来实现改进。

9.3.2 管理审查的投入

管理审查应包括

a) 以前的管理审查的行动状况。

b) 与安全管理系统有关的外部和内部问题的变化。

c) 与安全管理系统相关的有关各方的需求和期望的变化。

d) 关于安全性能的信息，包括以下方面的趋势。

   1) 不符合要求的情况和纠正措施。

   2) 监测和测量结果。

   3) 审计结果。

e) 持续改进的机会。

f) 对法律要求和组织遵守的其他要求进行审计和评估的结果。

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) 纠正行动的状况。

k) 以往管理审查的后续行动。

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

m) 改进建议。

9.3.3 管理评审的结果

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系统的任何修改需要。

应提供记录的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系统的适宜性、充分性和有效性。组织应积极寻求改进的机会，即使不是由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引起的，也应向相关的利益方通报。

10.2 不符合项和纠正措施

当不符合项发生时，组织应。

a) 对不符合项作出反应，并视情况而定。

   1) 采取行动控制和纠正它。

   2) 处理后果。

b) 评估是否有必要采取行动消除不符合项的原因，以使其不再发生或在其他地方发生，方法是

   1) 审查不符合要求的情况。

   2) 确定造成不符合项的原因。

   3) 确定是否存在类似的不符合项，或可能发生。

c) 实施任何必要的行动。

d) 审查所采取的任何纠正措施的有效性。

e) 如有必要，对安全管理系统进行修改。

纠正措施应与遇到的不符合项的影响相适应。应提供文件化的信息作为以下方面的证据。

— 不符合项的性质和随后采取的任何行动。

— 任何纠正措施的结果。

— 与安全有关的调查。

   — 失败，包括差点发生的事件和错误警报。

   — 事件和紧急状况。

   — 不符合要求的情况。

— 采取行动以减轻由这些故障、事件或不符合要求的情况所引起的任何后果。

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行动进行审查，除非立即实施可以防止对生命或公共安全的紧迫暴露。

为消除实际和潜在的不符合要求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] ISO 9001。*质量管理系统 - 要求*

[2] ISO 14001。*环境管理系统--要求与使用指南*

[3] ISO 19011, *管理系统审计准则*

[4] ISO 22301, *安全和复原力--业务连续性管理系统--要求*

[5] ISO/IEC 27001, *信息技术 - 安全技术 - 信息安全管理系统 - 要求*

[6] ISO 28001, *供应链的安全管理系统--实施供应链安全、评估和计划的最佳实践--要求和指导*

[7] ISO 28002, *供应链安全管理系统 - 供应链中的复原力发展 - 要求及使用指南*

[8] ISO 28003, *供应链安全管理系统--对提供供应链安全管理系统审计和认证的机构的要求*

[9] ISO 28004-1, *供应链安全管理系统--ISO 28000的实施指南--第1部分。一般原则*

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

[11] ISO 28004-4, *供应链安全管理系统--ISO 28000实施指南--第4部分：如果遵守ISO 28001是一个管理目标，则关于实施ISO 28000的补充具体指南*

[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指南73, *风险管理--词汇表*

编码03.100.01; 03.100.70

价格根据20页计算