ICS 03.100.01
CCS A 90

中华人民共和国国家标准

GB/T 45953—2025

供应链安全管理体系规范

Specification for security management systems of supply chain

2025-08-01 发布　　2025-11-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由全国公共安全基础标准化技术委员会(SAC/TC 351)提出并归口。

本文件起草单位：南京医药股份有限公司、中国标准化研究院、江苏省质量和标准化研究院、国网福建省电力有限公司、招商新疆质量和标准化研究院有限公司、北京工商大学、对外经济贸易大学、华为技术有限公司、中国国际贸易促进委员会商业行业委员会、南京卫岗乳业有限公司、苏州市东吴保安服务有限公司、天津大学、江苏省润天生化医药有限公司、美的集团股份有限公司、中信戴卡股份有限公司、贵州省交通规划勘察设计研究院股份有限公司、贵州习酒投资控股集团有限责任公司、舍得酒业股份有限公司、泸州老窖股份有限公司、中远海运工程物流有限公司、青岛新前湾集装箱码头有限责任公司、中铁十四局集团有限公司、四川省旺达生物饲料股份有限公司、东阿阿胶股份有限公司、漳州片仔癀药业股份有限公司、中安环(深圳)科技发展有限公司、北京华远润泽国际认证有限公司、苏州昆环检测技术有限公司、中国物资储运协会、中国计量大学、中国科学技术大学、北京市科学技术研究院、中国科技产业化促进会、徐州捷科思网络科技有限公司、江苏云意电气股份有限公司、广西桂冠电力股份有限公司。

本文件主要起草人：马云涛、张超、孟祥程、管旭琳、李光磊、郑宇、何明珂、李丽、杨春阳、姚歆、李军、刘珏、王皖、阮舒曼、秦挺鑫、白元龙、赵玉菲、周倩、孔肖菡、王建峰、郑重、张华、陈鸿毅、张金花、杨志刚、刘海峰、石碧峰、杜镔、周莉、陈强、蒲吉洲、余东、何灿、廖源、陈健、张连钢、李庆民、唐志伟、程杰、于娟、王成、朱敬云、胡永明、张启民、张苏、张杰、卢成绪、张冬芹、朱伟、白鑫、张夏阳、胡天勇、李永翠、张奉春、余大军、李羿宏、巫琳。

供应链安全管理体系规范

1 范围

本文件规定了供应链安全管理体系的组织环境、领导力、规划、支持、运作、绩效评估和改进等要求。

本文件适用于各种类型和规模的组织(如政府、企业或其他公共机构和非营利组织)建立、实施、维护和改进的供应链安全管理体系。本文件适用于在组织的整个生命周期以及各个层级的活动。

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,仅该日期对应的版本适用于本文件;不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

GB/T 44483 安全与韧性 术语

3 术语和定义

GB/T 44483 界定的以及下列术语和定义适用于本文件。

3.1

供应链 supply chain

从原材料来源到通过运输途径将产品或服务交付至终端用户的一系列资源和流程。

注:生产和流通过程中,围绕核心企业,将所涉及的原材料供应商、制造商、下游伙伴链接所形成的网链结构。

[来源:GB/T 18354—2021,3.8,有修改]

3.2

供应链安全管理体系 security management system of supply chain

为达到组织的供应链安全目标的要素集合。

注:由协调的方针、流程和实践构成。

3.3

供应链安全管理方针 security management policy of supply chain

与组织的供应链安全及其相关流程和活动的控制框架有关的总体意图和方向。

3.4

供应链安全管理目标 security management objective of supply chain

为符合供应链安全管理方针(3.3)而需要达成的具体供应链安全成果。

注:这些成果与向客户或最终用户交付的产品、服务存在直接或间接的联系。

3.5

供应链安全管理指标 security management target of supply chain

实现供应链安全管理目标(3.4)所需的特定的性能水平。

3.6

供应链安全管理程序 security management programmes of supply chain

实现供应链安全管理目标(3.4)的方式。

3.7

上游　upstream

承担货物在进入组织直接运营控制前，在供应链(3.1)中所发生的一系列动作、过程和移动的主体。

注：这些活动包括但不限于原材料采购、零部件加工、集货、包装、仓储和转运及其所涉及的保险、财务、数据管理。

3.8

下游　downstream

承担货物在离开组织直接运营控制后，在供应链(3.1)中所发生的一系列动作、过程和移动的主体。

注：这些活动包括但不限于商品分销、零售、售后服务、包装、储存和配送及所涉及的保险、财务、数据管理。

4　组织环境

4.1　了解组织及其环境

组织应明确自身特点以及与其目的相关的、影响其实现供应链安全管理体系预期结果能力的外部和内部环境。

4.2　了解相关方的要求和期望

4.2.1　通则

组织应确定：

a)　供应链安全管理体系的相关方；

b)　相关方的要求和期望；

c)　需要通过供应链安全管理体系解决的要求和期望。

4.2.2　法律、法规和其他要求

组织应：

a)　实施并维持一个机制，以确定、访问和评估与其供应链安全有关的适用法律、法规和其他要求；

b)　确保在实施和维护其供应链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)　向供应链相关方传达需要的信息。

4.2.3　原则

4.2.3.1　通则

组织的供应链安全管理目的是确保供应链安全稳定，确保组织防控供应链风险、持续创造价值。

组织应采用图 1 中给出的、在 4.2.3.2～4.2.3.9 中描述的原则。

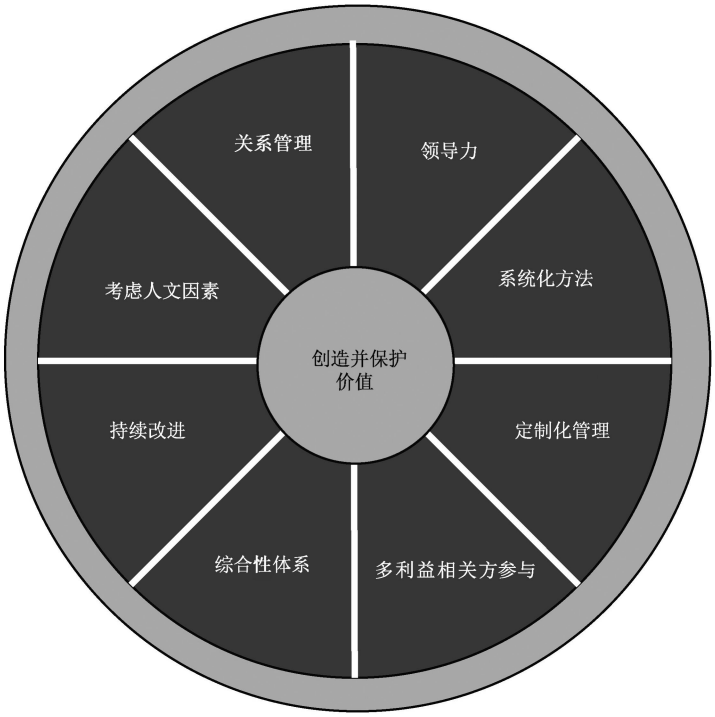

图 1　供应链安全管理工作的目的及其实现原则

4.2.3.2　领导力

组织的各级领导应建立统一的供应链安全管理目标和方向。应创造使组织的供应链战略、方针、程序和资源协调一致的条件，以实现其供应链安全管理目标。

4.2.3.3　系统化方法

供应链安全管理采取结构化和系统化的方法，基于现有信息，把各项安全要求转化为一个连贯的、相互关联的、融入业务的流程活动，并加以管理，则可更高效地达成目标。

4.2.3.4　定制化管理

供应链安全管理体系应与组织的目标相关、与组织的外部和内部环境和需求相匹配。

4.2.3.5　多利益相关方参与

组织宜考虑相关方的知识、观点和看法使其参与其中，以提高对供应链安全管理的认识并促进供应链安全管理。组织应确保所有级别都得到尊重并有机会参与供应链安全管理。

4.2.3.6　综合性体系

供应链安全管理应与本组织的其他管理体系相结合，是组织所有活动的组成部分。

组织的供应链风险管理，无论是正式的、非正式的还是直观的，都应纳入组织安全管理体系。

4.2.3.7　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，并随着组织的外部和内部环境变化创造新的机会。

4.2.3.8 考虑人文因素

人员行为和文化对安全管理的各个方面都有影响。决策应基于对数据和信息的分析和评估，以确保决策更加客观、可信，更有可能产生预期的结果，同时宜考虑个人的看法。

4.2.3.9 关系管理

为确保持续成功，组织应管理好利益相关方的关系，因为它们可能影响本组织供应链管理的绩效。

4.3 确定供应链安全管理体系的范围

组织应确定供应链安全管理体系的边界和适用性，以确定其范围。在确定适用范围时，组织宜考虑：

a） 4.1 中提到的外部和内部环境；

b） 4.2 中提到的要求。

该范围应作为文件化信息提供。

当供应链组织选择外包而影响到与要求的符合性时，组织应确保外包过程受到控制。外包行为的必要控制和责任应在供应链安全管理体系中明确规定。

4.4 供应链安全管理体系

组织应根据本文件的要求，建立、实施、维护并持续改进供应链安全管理体系，包括所需的流程及其相互作用。

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在供应链安全管理体系方面的领导力和承诺：

a） 保证制定供应链安全方针和安全目标，并与组织的战略方向相一致；

b） 考虑组织供应链相关方的要求和期望，并及时采取适当行动管理这些期望，以保证将供应链安全管理体系要求纳入组织的业务流程；

c） 保证将供应链安全管理体系要求纳入组织的业务流程；

d） 保证供应链安全管理体系所需的资源可用；

e） 传达有效供应链安全管理和符合供应链安全管理体系要求的重要性；

f） 保证供应链安全管理体系实现其预期结果；

g） 保证供应链安全管理目标、指标和方案的可行性；

h） 保证本组织其他部分产生的任何安全方案，都能补充供应链安全管理体系；

i） 指导和支持人员为供应链安全管理体系的有效性作出贡献；

j） 促使本组织的供应链安全管理体系不断改进；

k） 支持其他相关角色，以展示其在其责任领域中的领导力。

注：本文件中提及的“业务”是对组织存在的目的具有核心意义的活动。

5.2 供应链安全方针

5.2.1 确定供应链安全方针

最高管理层应制定供应链安全方针：

a） 与本组织的方针相适应；
b） 为制定供应链安全目标提供框架；
c） 承诺满足适用要求；
d） 承诺不断改进供应链安全管理体系；
e） 考虑供应链安全方针、目标、指标、方案等对组织其他方面可能产生的不利影响。

5.2.2 供应链安全方针要求

供应链安全方针应：
a） 与组织的其他方针一致；
b） 与组织的整体供应链安全风险评估保持一致；
c） 规定在收购其他组织或与其他组织合并时，或在组织的业务范围发生可能影响供应链安全管理体系的连续性或相关性的其他变化时，进行审查；
d） 描述并分配主要的问责机制和成果责任；
e） 能作为文件信息提供；
f） 在组织内部进行交流；
g） 酌情向相关方提供。

5.3 角色、职责和权限

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。最高管理层应分配针对以下事项的责任和权力：
a） 确保供应链安全管理体系符合本文件的要求；
b） 向最高管理层报告供应链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 通则

在规划供应链安全管理体系时，组织宜考虑 4.1 中提到的问题和 4.2 中提到的要求，并确定需要应对的供应链风险和机遇，包括但不限于：
a） 保证供应链安全管理体系能够实现其预期结果；
b） 防止或减少非预期的影响；
c） 实现持续改进。
组织应计划：
a） 应对风险和机遇的行动；
b） 如何将这些行动纳入其供应链安全管理体系流程并实施；
c） 如何评估这些行动的有效性。
管理风险的目的是创造和保护价值。供应链风险管理应被纳入安全管理体系。与本组织及其供应链相关方安全有关的风险评估见 8.3。

6.1.2 确定供应链安全相关的风险并识别机遇

确定供应链安全相关风险以及识别和利用机遇，需要主动进行供应链风险评估，其中应考虑但不限于：

a) 法律及适用标准的合规问题；
b) 物理或功能故障以及人为的恶意或犯罪行为；
c) 人员以及其他内部或外部环境，包括其他影响组织供应链安全的因素；
d) 供应链安全设备的设计、安装、维护和更换；
e) 供应链组织的信息、数据、知识和通信安全；
f) 供应链信息系统和网络安全；
g) 与供应商、客户之间的相互依存关系；
h) 供应链物理设施的安全。

6.1.3 管理供应链安全相关风险和机遇

对已确定的供应链安全相关风险的评价应开展的工作包含但不限于：
a) 本组织的整体风险管理；
b) 供应链风险应对；
c) 供应链安全管理目标；
d) 供应链安全管理流程；
e) 供应链安全管理体系的设计、规范和实施；
f) 确定足够的资源，包括人员配备；
g) 确定培训需求和所需的能力水平。

6.2 供应链安全目标和实现这些目标的规划

6.2.1 设置供应链安全目标

组织应在相关职能和级别设置供应链安全目标。这些安全目标应：
a) 与供应链安全方针一致；
b) 可测量(如果可行)；
c) 考虑到适用的要求(技术层面及社会和环境层面)；
d) 能被监测；
e) 能被交流传递；
f) 能更新；
g) 能作为文件信息提供。

6.2.2 确定供应链安全目标

在规划如何实现其供应链安全目标时，组织应确定：
a) 将做什么；
b) 需要哪些资源；
c) 谁来负责；
d) 何时完成；
e) 如何评估结果。

在确定和评审其供应链安全目标时，组织宜考虑：
a) 技术、人力、行政和其他备选办法；
b) 相关方的看法和对其的影响。

供应链安全目标应符合本组织对持续发展的承诺。

6.3 变更规划

组织应有计划地进行供应链安全管理体系的变更及改进(见第 10 章)。

本组织应考虑:

a) 变化的目标及其潜在后果;

b) 供应链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、维护和持续改进供应链安全管理体系所需的资源。

7.2 能力

组织应:

a) 确定在其控制下,从事影响其供应链安全业绩的工作人员具备必要的能力;

b) 确保这些人在适当的教育、培训或经验的基础上有能力,并得到适当的安全审查;

c) 在适当的情况下,采取行动获得必要的权限,并评估所采取行动的有效性;

d) 提供适当的文件资料作为能力证据。

注:适当的行动包括:为目前雇佣的人员,提供培训、指导或进行重新分配,或雇佣、签约合格人员。

7.3 意识

本组织控制下从事供应链安全管理工作的人员应了解:

a) 供应链安全方针;

b) 其对供应链安全管理体系有效性的贡献,包括因改进供应链安全性能获得的好处;

c) 不符合供应链安全管理体系要求的影响;

d) 其在遵守供应链安全管理方针和程序以及供应链安全管理体系的要求方面的作用和责任,包括应急准备和反应要求。

7.4 沟通

组织应确定与供应链安全管理体系有关的内部和外部沟通,包括:

a) 传达的内容;

b) 何时沟通;

c) 与谁沟通;

d) 如何沟通;

e) 传播之前确定信息的敏感性。

7.5 文件化信息

7.5.1 通则

组织的供应链安全管理体系中应包括:

a) 本文件要求的文件化信息;

b） 由组织确定的供应链安全管理体系有效性所必需的文件化信息。

文件化信息应说明实现供应链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：因下列因素，使得供应链安全管理体系的文件化信息范围因不同的组织而不同：

a） 组织的规模及其活动类型、流程、产品和服务；

b） 过程的复杂性及其相互作用；

c） 人的能力。

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，以防止未授权的访问。

7.5.2 创建和更新文件化信息。

在创建和更新文件信息时，组织应确保适当的：

a） 识别和描述（例如标题、日期、作者或参考编号）；

b） 格式（如语言、软件版本、图形）和媒体（如纸张、电子）；

c） 审查和批准是否合适和充分。

7.5.3 文件化信息的控制

供应链安全管理体系和本文件要求的供应链安全文件化信息应受到控制，以确保：

a） 在需要的地方和时间，它是可用的并适合使用的；

b） 它得到了充分的保护（例如防止失去保密性、完整性、可用性）；

c） 定期审查并在必要时进行修订，并由授权人员批准其合适性；

d） 过时的文件、数据和信息应及时从所有发放点和使用点删除，或以其他方式保证不被意外使用；

e） 为法律或知识保存目的保留的档案文件、数据和信息得到适当的识别。

对于文件化信息，组织应酌情处理以下活动：

a） 分发、访问、检索和使用；

b） 储存和保存，包括保存易读性；

c） 对于变化的控制（例如版本控制）；

d） 保留和处置。

应酌情识别和控制由组织确定的、对供应链安全管理体系的规划和运行来说是必要的外部来源的文件信息。

注：访问权指仅查看文件化信息的权限，或查看和修改文件信息的权限。

8 运作

8.1 业务规划和控制

组织应通过以下方式规划、实施和控制满足要求所需的流程，并实施第6章中确定的行动：

a） 为流程制定标准；

b） 根据标准对流程实施控制。

应在必要的范围内提供文件化信息，以使人们相信这些流程已按计划执行。

8.2 流程和活动的识别

组织应确定实现以下目标所必需的流程和活动：

a） 遵守其供应链安全方针；

b） 遵守法律、法规和监管的安全要求；
c） 其供应链安全管理目标；
d） 其供应链安全管理体系的交付；
e） 供应链所需的安全水平。

8.3 风险评估和应对

组织应实施并维护风险评估和应对流程。

注1：风险评估和处理流程在ISO 31000中涉及。

组织应：

a） 确定其与供应链安全有关的风险，并将它们与供应链安全管理所需的资源进行优先排序；
b） 分析和评估已识别的风险；
c） 确定哪些风险需要处理；
d） 选择和实施应对这些风险的方案；
e） 制定和实施风险应对计划。

注2：本条中的风险与组织及其相关方的供应链安全有关。与管理体系的有效性相关的风险和机遇的处理见6.1。

8.4 控制

8.2中列出的流程应包括对人力资源管理的控制，以及酌情对与供应链安全有关的设备、仪器和信息技术项的设计、安装、运行、翻新和修改。如果对现有的安排进行修订，或引入了可能对供应链安全管理产生影响的新安排，组织应在实施之前考虑供应链安全相关的风险。

需考虑的新安排或修订的安排应包括：

a） 修订后的组织结构、角色或责任；
b） 培训、宣传和人力资源管理；
c） 修订供应链安全管理方针、目标、指标或方案；
d） 修订流程和程序；
e） 引入新的基础设施、供应链安全设备或技术，其中可能包括硬件和/或软件；
f） 酌情引入新的承包商、供应商或人员；
g） 对外部供应商的供应链安全保证的要求。

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。

组织应确保外部提供的与供应链安全管理体系相关的流程、产品或服务受到控制。

8.5 供应链安全政策、程序、流程和处理

8.5.1 识别和选择策略、处理方法

组织应实施并保持系统的程序，以分析与供应链安全有关的脆弱性和威胁。在这种脆弱性和威胁分析及其后续的风险评估的基础上，组织应确定并选择一种安全战略，其中包括一个或多个程序、过程和处理方法。

识别应基于战略、程序、流程和处理的程度：

a） 维护本组织的供应链安全；
b） 降低供应链安全漏洞的可能性；
c） 降低威胁实现的可能性；
d） 缩短任何供应链安全处理缺陷的期限，并限制其影响；
e） 规定提供足够的资源。

选择应基于战略、流程和处理的程度：

a） 满足保护组织供应链安全的要求；

b） 考虑组织可能承担或不承担的风险的数量和类型；

c） 考虑相关的成本和效益。

8.5.2 所需资源

组织应确定实施所选择的供应链安全程序、过程和处置对策的资源需求。

8.5.3 处理的实施

组织应实施和维护所选择的供应链安全处理方法。

8.6 供应链安全方案

8.6.1 通则

组织应根据所选择的战略和处理方法，制定并记录供应链安全计划和程序。组织应实施和维护一个响应架构，以便及时且有效地警告和向相关方通报与供应链安全相关的漏洞、迫在眉睫的供应链安全威胁或正在发生的供应链安全违规行为。响应架构应提供计划和流程，以便在供应链安全受到威胁或正在发生的供应链安全违规行为期间管理组织。

8.6.2 响应框架

8.6.2.1 组织应实施和维持响应框架，确定一个对接人或者一个/多个团队负责响应与安全相关的漏洞和威胁。对接人或团队的职责以及这些人员或团队之间的关系应能够清晰地确定、交流以及记录。

8.6.2.2 总体上，各团队整体应能胜任：

a） 评估供应链安全威胁的性质、程度及其潜在影响；

b） 根据预先确定的阈值评估影响，以证明启动正式反应的合理性；

c） 启动适当的供应链安全响应；

d） 需要采取的计划行动；

e） 以生命安全为第一优先，确定优先事项；

f） 监测与供应链安全有关的漏洞的任何变化的影响、威胁者的意图和能力的变化或违反供应链安全规定的行为，以及组织的反应；

g） 激活供应链安全处理；

h） 与相关方、政府和媒体沟通；

i） 为沟通管理的沟通计划做出贡献。

8.6.2.3 对于每个对接人或团队，应有：

a） 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；

b） 指导其行动的文件化流程，包括应对措施的启动、运作、协调和沟通的程序。

8.6.3 警告和沟通

8.6.3.1 组织宜记录并保持程序如下：

a） 向相关方进行内部和外部沟通，包括沟通的内容、时间、对象和方式；

b） 接收、记录和答复相关方的来文，包括任何国家或区域风险咨询系统或类似机构；

c） 确保在违反供应链安全规定、出现漏洞或威胁时，通信手段的可用性；

d） 促进与供应链安全威胁和/或违规行为应对者的结构化沟通；

e） 提供本组织在发生违规事件后的媒体反应细节，包括沟通策略；

f） 记录供应链安全违规的细节、采取的行动和作出的决定。

8.6.3.2 在适用的情况下，宜考虑和执行以下各项：

a） 提醒可能受到实际或即将发生的供应链安全违规行为影响的相关方；

b） 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方案的一部分进行演练。

8.6.4 供应链安全方案的内容

8.6.4.1 组织应记录并维护供应链安全方案。这些方案应提供指导和信息，以协助团队应对供应链安全漏洞、威胁和/或违规行为，并协助组织进行应对和恢复其安全。

8.6.4.2 一般情况下，安全方案宜包含以下内容。

a） 各小组将采取的行动细节：

1） 继续或恢复商定的供应链安全状态；

2） 监测实际或即将发生的供应链安全威胁、漏洞或违规行为的影响，以及组织对它的反应。

b） 参考预设的阈值和激活响应的过程。

c） 恢复组织供应链安全的程序。

8.6.4.3 管理供应链安全漏洞和威胁或实际或即将发生的供应链安全违规行为的直接后果的细节，同时宜考虑：

a） 个人的福利；

b） 可能受损的资产、信息和人员的价值；

c） 防止核心活动的(进一步)损失或不可用。

8.6.4.4 每个方案应包括：

a） 其目的、范围和目标；

b） 实施计划的团队的作用和责任；

c） 实施解决方案的行动；

d） 激活(包括激活标准)、运作、协调和沟通团队行动所需的信息；

e） 内部和外部的相互依存关系；

f） 其资源需求；

g） 其报告要求；

h） 退出的流程。

每个方案都应是可用的，并能在需要的时间和地点提供。

8.6.5 恢复

本组织应制定有文件记录的程序，以便在安全违规之前、期间和之后所采取的任何临时措施中恢复组织的安全。

9 绩效评估

9.1 监测、测量、分析和评估

组织应确定：

a） 需要监测和测量的内容；

b） 监测、测量、分析和评估方法(如适用)，以确保结果有效；

c） 何时进行监测和测量；

d） 何时对监测和测量的结果进行分析和评估。

应提供文件化信息作为结果的证据。

组织应评估供应链安全管理体系的绩效和有效性。

9.2 内部审核

9.2.1 通则

组织应按计划定期对供应链安全管理体系进行内部审核，审核内容包括但不限于：

a） 供应链安全管理体系是否符合本组织本身对其供应链安全管理体系的要求和本文件的要求；

b） 得到有效的实施和维护。

9.2.2 内部审核方案

组织应规划、建立、实施和维护审核方案，包括频率、方法、责任、规划要求和报告。

在制定内部审核方案时，本组织宜考虑相关流程的重要性和以往审核的结果。

组织应：

a） 确定审核目标、标准和范围；

b） 选择审核员并进行审核，以确保审核过程的客观性和公正性；

c） 确保审核结果向相关管理人员汇报；

d） 核实供应链安全设备和人员是否得到合适的部署；

e） 确保毫不拖延地采取任何必要的纠正措施，以消除检测到的不符合项及其发生的原因；

f） 确保后续审核行动包括对所采取的行动进行核查并报告核查结果。

组织应提供文件化信息，作为审核方案执行情况和审核结果的证据。

审核方案，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核的结果。审核流程应涵盖范围、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 通则

最高管理层应按计划的时间间隔评审本组织的供应链安全管理体系，以确保其持续的适用性、充分性和有效性。

组织宜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供应链安全管理体系有关的需求或机会点，并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以下内容。

a） 以前管理评审的执行状况。

b） 与供应链安全管理体系有关的外部和内部问题的变化。

c） 供应链安全管理体系相关方的需求和期望的变化。

d） 有关供应链安全性的信息，包括以下方面：

1） 不符合项和纠正措施；

2） 监控和测量结果；

3） 审核结果。

e） 持续改进的机会。
f） 对遵守法律要求和本组织同意的其他要求的审核和评估结果。
g） 来自外部相关方的通信，包括投诉。
h） 组织的供应链安全业绩。
i） 目标和指标的实现程度。
j） 纠正措施的状况。
k） 以往管理评审的后续行动。
l） 不断变化的情况，包括与供应链安全相关的法律、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

管理评审的结果应包括与持续改进机会相关的决定，以及对供应链安全管理体系的任何修改需求。

应提供有文件化信息作为管理评审结果的证据。

10 改进

10.1 持续改进

组织应不断提高供应链安全管理体系的适用性、充分性和有效性。组织应积极寻求改进机会，即使不是由于与安全有关的漏洞、即将发生的安全威胁或正在发生的安全违规行为而促使利益相关方进行改进。

10.2 不符合和纠正措施

10.2.1 当出现不符合时，组织应采取以下措施。

a） 对不符合的应对包括：
   1） 采取行动控制和纠正不符合；
   2） 处理其后果。
b） 评估采取行动以消除不符合项原因的必要性，以便不在其他地方再次发生：
   1） 审查不符合；
   2） 确定不符合的原因；
   3） 确定是否存在或可能出现类似的不符合项。
c） 执行任何必要的行动。
d） 审查所采取的纠正措施的有效性。
e） 如有必要，对供应链安全管理体系进行更改。

纠正措施应适用于削减不符合项的影响。

10.2.2 文件化信息应包括以下内容。

a） 不符合的性质和随后采取的任何行动。
b） 任何纠正措施的结果。
c） 与供应链安全有关的调查包括：
   1） 故障，包括虚惊事件和错误警报；
   2） 事件和紧急情况；
   3） 不符合。

d） 采取行动，减轻此类故障、事件或不符合项所产生的任何后果。

流程应要求在实施前通过供应链安全相关的风险评估流程，对所有待评审的纠正措施进行评审，除非立即实施可以防止人员生命或公共安全面临的紧迫风险。

为消除实际和潜在的不符合项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，并与可能遇到的供应链安全管理相关风险相匹配。

参 考 文 献

[1] GB/T 18354—2021 物流术语

[2] ISO 9001 Quality management systems—Requirements

[3] ISO 14001 Environmental management systems—Requirements with guidance for use

[4] ISO 19011 Guidelines for auditing management systems

[5] ISO 22300 Security and resilience—Vocabulary

[6] ISO 22301 Security and resilience—Business continuity management systems—Requirements

[7] ISO 28001 Security management systems for the supply chain—Best practices for implementing supply chain security, assessments and plans—Requirements and guidance

[8] ISO 28003 Security management systems for the supply chain—Requirements for bodies providing audit and certification of supply chain security management systems

[9] ISO 28004-1 Security management systems for the supply chain—Guidelines for the implementation of ISO 28000—Part 1: General principles

[10] ISO 28004-3 Security management systems for the supply chain—Guidelines for the implementation of ISO 28000—Part 3: Additional specific guidance for adopting ISO 28000 for use by medium and small businesses (other than marine ports)

[11] ISO 28004-4 Security management systems for the supply chain—Guidelines for the implementation of ISO 28000—Part 4: Additional specific guidance on implementing ISO 28000 if compliance with ISO 28001 is a management objective

[12] ISO 31000 Risk management—Guidelines

[13] ISO 31073 Risk management—Vocabulary

[14] ISO 45001 Occupational health and safety management systems—Requirements with guidance for use

[15] ISO/IEC 27001 Information security, cybersecurity and privacy protection—Information security management systems—Requirements