ICS 03.100.01
A 90

中华人民共和国国家标准

GB/T 38702—2020/ISO 28001:2007

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

Security management systems for the supply chain—Best practices for implementing supply chain security, assessments and plans—Requirements and guidance

(ISO 28001:2007,IDT)

2020-03-31 发布　　2020-09-01 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

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准使用翻译法等同采用 ISO 28001:2007《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》。

本标准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。

本标准起草单位:中国标准化研究院、北京城市系统工程研究中心、耀泰物流股份有限公司、福建你他共创网络科技有限公司、中国质量认证中心、江苏辉源供应链管理有限公司、国网山东省电力公司、方圆标志认证集团有限公司、中国网络安全审查技术与认证中心。

本标准主要起草人:秦挺鑫、王晶晶、叶耀华、潘英、白元龙、孙世军、宋跃炜、孙宏志、张超、曾耀、魏军、陈伟、张剑、汪勇、吴琬光。

引　言

国际供应链中的安全事故已威胁到各贸易国的国际贸易和经济的发展，人员、货物、基础设施和设备——包括运输工具——都要防止发生安全事件及其潜在的破坏性效应。总体而言，这种保护对经济和社会等各个方面都是有利的。

国际供应链是高度动态的，由许多实体和业务伙伴组成。本标准识别了这种复杂性，组织可依据其特定的商业模式和在国际供应链中的角色和作用应用本标准的要求。

本标准为组织在国际供应链及其组成部分中确定和记录合理的安全水平提供了选择，使得组织能够基于国际供应链中的安全风险做出更好的决策。

本标准是多元化的，并意在协调和补充《世界海关组织(WCO)全球贸易安全和便利标准框架》。本标准无意覆盖、替代或取代各海关机构的供应链安全方案、认证和验认要求。

本标准旨在帮助组织就其在国际供应链中控制的部分确定适当的安全水平。同时，也为内部或外部审核员或使用国际标准作为供应链安全方案接收准则的政府机构提供了确认或验证组织当前供应链安全水平的依据。客户、业务伙伴、政府部门和其他方可要求声称符合本标准的组织通过接受审核或确认来证明这种符合性。政府部门可就由其他政府的部门实施的确认予以相互认可。如需由第三方组织实施审核，组织宜考虑聘请一个由主管机构[国际认可论坛(IAF)成员]认可的第三方认证机构(参见附录 C)。

本标准无意重复政府要求和遵循《世界海关组织(WCO)全球贸易安全和便利标准框架》的相关供应链安全标准。已经由互认的政府认证或确认的组织是符合本标准的。

本标准可以输出如下结果：

——覆盖范围的表述：界定由安全计划所包含的供应链边界；

——安全性评估：记录供应链脆弱点以定义安全威胁场景，并描述来自每个潜在安全威胁情境的合理预期影响；

——安全计划：描述安全措施，其目的是管理由安全性评估识别的安全威胁场景；

——培训方案：陈述如何培训安全人员以符合与其任务相关的安全要求。

为了实施制定安全计划所需的安全评估，使用本标准的组织将：

——识别产生的威胁(安全威胁场景)；

——确定人员将通过安全性评估识别的安全威胁场景推进为安全事件的方法。

通过评审供应链当前的安全状态做出决策。基于该评审的发现，采用专业判断来识别供应链遭受每个安全威胁场景的程度。

如果认为供应链对于遭受的每个安全威胁场景的程度不可接受，则组织将制定附加程序或采取运行调整以降低发生的可能性或产生的影响，或同时降低两者。这些都称为应对措施。基于优先原则，应对措施需列入安全计划中，以将威胁降低到一个可接受的水平。

基于保护人员、财产和国际供应链任务的安全过程，附录 A 和附录 B 给出了风险管理说明性示例，有助于组织针对复杂供应链采用宏观方法和/或针对供应链的局部采用更为离散的方法。

这些附录也旨在：

——促进对此类方法的理解、采纳和实施，并可由组织按需调整；

——为持续改进基础性安全管理提供指南；

——帮助组织管理资源以解决既有和新显现的安全风险；

——表述对供应链(从原料配送到成品的存贮、制造和运输到市场)实施风险评估和减轻安全威胁的可能的方法。

如果组织采用并实施了本标准,附录C为其获得咨询建议和认证提供了指南。

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

1　范围

本标准为处于国际供应链中的组织提供了要求和指南，以：

——制定和实施供应链安全过程；

——建立并记录供应链整体或部分的最低安全级别；

——协助组织满足《世界海关组织标准框架》内适用的授权运营者（AEO）准则和符合国家供应链安全方案。

注：只有参与该框架的各国海关机构才可以按照其供应链安全方案及相关的认证和验证要求指定组织作为授权经营者（AEOs）。

此外，本标准确定了一些可作为验证的文件要求。

本标准的使用者将：

——确定已建立安全的国际供应链的环节（见 4.1）；

——对供应链的该环节实施安全评估并制定适当的应对措施；

——制定并实施供应链安全计划；

——对安全人员进行安全职责的培训。

2　规范性引用文件

下列文件对于本文件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）适用于本文件。

ISO /PAS 20858　船舶与航海技术　海运港口设施安全评估和安全计划编制（Ship and marine technology—Maritime port facility security assessments and security plan development）

国际海事组织　国际海上生命安全公约（SOLAS），1974 年，修正案[International Convention for the Safety of Life at Sea (SOLAS), 1974, as amended]

3　术语和定义

下列术语和定义适用于本文件。

3.1

有关执法部门及其他政府官员　appropriate law enforcement and other government officials

对国际供应链或其环节拥有特定法定管辖权的政府和执法部门的人员。

3.2

资产　asset(s)

工厂、机器、财产、建筑物、车辆、船舶、飞机、运输工具和其他基础设施，或工厂以及具有特定且可量化的商业功能或服务的相关系统。

注：本定义包括安全交付必需的所有信息系统和安全管理应用程序。

3.3

授权经营者　authorized economic operator

以经批准的任何职能参与国际货物运输并被海关当局认定符合世界海关组织或相应供应链安全标准的一方。

注 1：授权经营者是在世界海关组织标准框架中定义的一个术语。

注 2：授权经营者包括其他的制造商、进口商、出口商、报关行、承运商、理货人、中间商、口岸、机场、货站经营者、综合经营者、仓储业经营者、分销商。

3.4

业务伙伴　business partner

与组织签订合同并协助其成为**供应链中的组织**(3.15)的承包人、供应商及服务提供方。

3.5

货物运输单元　cargo transport unit

公路货运车、铁路货运车、货物集装箱、公路罐车、铁路罐车或便携储罐。

3.6

后果　consequence

可合理被预期由组织在供应链中遭受的攻击或将供应链作为武器使用而造成的人员伤亡、财产损失或经济破坏，包括对运输系统的破坏。

3.7

运输工具　conveyance

国际贸易中将货物从一个地点运送到另一地点的工具。

示例：货箱、货盘、集装箱、货物装卸设备、卡车、船舶、飞机和轨道车。

3.8

对策　countermeasure

为降低安全威胁场景发生的可能性以实现目标或减小安全威胁场景造成的可能的**后果**(3.6)所采取的措施。

3.9

保管　custody

供应链中的组织在一段时间内直接控制供应链中货物的制造、加工、装卸和运输以及与之相关的航运信息。

3.10

下游　downstream

供应链中货物不再受组织保管的情况下的搬运、加工和移动。

3.11

货物　goods

供应链中在买方下单后为供买方使用或消费制造、加工、装卸或运输的零部件或原料。

3.12

国际供应链　international supply chain

在某些环节上跨越国际或经济体边界的供应链。

注 1：从订单执行到货物被目的地国家或经济体解除海关控制，供应链的所有环节都是国际性的。

注 2：如果公约或地区协议免除了来自特定国家或经济体的货物的报关，国际供应链的终点则是进口国或进口经济体的进口岸。如果协议或公约没有此项规定，则货物在进口港需进行报关。

3.13

可能性　likelihood

安全威胁场景可能发展成安全事件的难易程度。

注：可能性是基于现有安全过程针对发生安全事件的抵抗力进行评价的，包括对安全威胁场景的检查和以定性或定量方式的表述。

3.14

管理体系　management system

组织为管理其过程或活动，将输入的资源转化为产品或服务以实现组织的目标的结构。

注：本标准的目的并不是指定一个特殊的管理体系或要求创建一个独立的安全管理体系。ISO 9001(质量管理体系)、ISO 14001(环境管理体系)、ISO 28000(供应链安全管理体系)以及国际海事组织的《国际安全管理(ISM)规则》都是管理体系的例子。

3.15

供应链中的组织　organization in the supply chain

进行以下任一活动的实体：

——按采购订单制造、搬运、加工、装载、合并、卸载或收货，在某些环节跨越国际或经济体边界；

——在国际供应链中以任何方式进行货物运输，不管这个供应链中的任何环节是否跨越国界(或经济体边界)；或

——提供、管理或实施海关部门或商业管理中所用的航运信息的生成、发布或流动。

3.16

风险管理　risk management

基于对潜在的威胁、威胁产生的后果以及发生的概率或可能性的分析做出管理决策的过程。

注：启动风险管理过程的目的通常是对组织在特殊环境下运行所需的资源配置进行优化。

3.17

服务范围　scope of service

组织在供应链中执行的且无论何时执行的一项或多项职能。

3.18

安全申明　security declaration

业务伙伴以文件形式做出的承诺，该承诺表述由业务伙伴实施安全措施，至少包括如何保护国际贸易中的货物和器具和相关的信息及如何证实和确认安全措施。

注：供应链中的组织将使用该声明评价与货物安全相关的安全措施的充分性。

3.19

安全计划　security plan

为确保安全得到充分管理的策划安排。

注1：安全计划旨在确保保护组织避免安全事件的措施得以实施。

注2：安全计划可以包含在其他运行计划中。

3.20

安全　security

针对旨在对供应链造成损坏或破坏或由供应链造成损坏或破坏的故意行为的抵抗力。

3.21

安全事件　security incident

产生**后果**(3.6)的任何行为或状况。

3.22

安全人员　security personnel

供应链中的组织中承担相关安全职责的人员。

注：这些人可以是组织的雇员，也可以不是组织的雇员。

3.23

安全敏感信息　security sensitive information

安全敏感资料　security sensitive materials

由供应链安全过程产生的或纳入供应链安全过程的信息或资料，包含有关安全过程、装运或政府指令，不便向公众提供或被某些人利用制造安全事件的信息和资料。

3.24

供应链　supply chain

基于买方订单，从原材料采购到货物的制造、加工、装卸和交付及为买方提供相关服务的过程和资源的链接集链式集合。

注：供应链可包括经销商、制造商、物流服务商、内部配送中心、分销商、批发商和其他与货物的制造、加工、装卸和交付以及相关服务有关的实体。

3.25

目标　target

供应链中组织内的人员、运输方式、货物、有形资产、制造过程和装卸、控制或文件系统。

3.26

安全威胁场景　security threat scenario

可能发生潜在安全事件的情况。

3.27

上游　upstream

供应链中的组织对货物进行保管前所发生的货物搬运、加工和移动。

3.28

世界海关组织　World Customs Organization；WCO

独立于政府间的机构，其使命是提高海关当局的有效性和效率。

注：世界海关组织是处理海关事务的唯一的全球政府间组织。

4　申请范围

4.1　申请书

供应链中的组织应在《申请书》中对其声称符合本标准的处于国际供应链中的环节进行描述。《申请书》应至少包含以下信息：

a）　组织的详细资料；

b）　服务范围；

c）　在确定的服务范围内所有业务伙伴的名称和联系方式；

d）　完成安全评估的日期及安全评估的有效期；

e）　经授权代表组织签字的人员的签名。

供应链中的组织可将供应链的其他部分写入《申请书》，如包括最终目的地。

4.2　业务伙伴

若《申请书》中说明供应链中的组织与业务伙伴合作，组织应依据4.3和4.4的规定要求这些业务伙伴提供一份安全声明。组织对其进行安全评估时应考虑此安全声明，并可能要求制定特定的应对措施。

4.3　国际公认的证书或批文

持有依据强制性国际公约（治理各交通运输部门的安全性）所颁发的国际公认的证书或批文的运输

公司和设施，已具备符合本标准适用要求的安全规范、计划和过程，无须对其实施审核以确认符合性。对于船运公司、船舶和港口设施，适用时，证书或批文应依据《国际海上生命安全公约》(SOLAS)的XI-2/4或XI-2/10的规定予以颁发。

符合第1段特征的前提下，运输公司和设施除拥有国际公认的安全证书或批文外，各国海关部门可能还要求其实施额外的安全措施和规范，作为指定授权经营者(AEO)的条件。

4.4 免除安全申报要求的业务伙伴

业务伙伴向组织证实其：

a) 经验证符合本标准或ISO 20858；

b) 符合4.3所覆盖的要求；或

c) 已依据国家海关部门的供应链安全方案被指定为授权经营者(AEOs)，该方案的确定符合《全球贸易安全与便利标准框架》(WCO SAFE)。

以上均应在《申请书》中列出。然而，组织无须对此类业务伙伴实施额外的安全评估或要求其提供安全申明。

4.5 业务伙伴的安全评审

除了业务伙伴符合4.3或4.4的要求外，供应链中的组织应对业务伙伴的过程和设施实施评审以确认其安全声明的有效性。评审的范围和频次应通过对相关风险的分析来确定。组织应保留此类评审的结果。

注：为方便阅读，对声称符合要求的组织，包括由业务伙伴运行的供应链环节，无论是否符合本标准，以下段落中均称为“组织”，除非另有明确要求。

5 供应链安全保障过程

5.1 总则

国际供应链中采用本标准的组织需要管理供应链中其所处环节的安全，并建立管理体系以支持这一目标，本标准要求建立和实施安全规范和/或过程以降低对可能导致安全事件发生的活动对国际供应链造成的风险。

申明符合本标准的供应链中的组织应制定一个安全计划。该安全计划应基于安全评估的输出，包括记录现行的安全措施和程序及纳入适用于已包括在其《申请书》中的国际供应链环节的应对措施。

5.2 安全评估范围的识别

安全评估范围应包括组织实施的所有活动，如其《申请书》(见4.1)所述。应定期实施评估，且应适时修订安全计划。评估结果应予以记录和保存。

安全评估应覆盖有关在组织监保管期间货物搬运和移动的信息系统、文件和网络。组织应对其全部场所内现有的安全安排(4.3和4.4所提及的)进行评估，并对存在潜在安全脆弱点的业务伙伴进行评估。

5.3 安全评估的实施

5.3.1 评估人员

实施安全评估的人员或团队应同时具备以下技能和知识，包括但不限于：

——适用于国际供应链各方面的评估技巧，从供应链中的组织监管货物到货物不再受组织保管或

离开国际供应链；

——采取适当的措施规避对安全性敏感材料进行未授权的泄露和侵入的风险；

——适当时，涉及货物的制造、搬运、加工、移动和/或记录的运行和程序；

——在供应链相应环节中的托管、运输、人员、经营场所和信息系统有关安全措施；

——了解安全威胁及其减缓方法；

——理解本标准。

实施评估的人员或团队成员的名字及其资质应予以记录。

5.3.2 评估过程

组织应建立、实施和保持程序以识别目前用于减缓安全威胁的应对措施。组织应针对适当的威胁情况建立清单，包括有关政府官员所重视的威胁情况。若政府官员未参与，应在安全性评估中予以记录。

针对每个安全威胁场景，组织应评估现有的应对措施，确定每个安全威胁场景发生的可能性及其后果，评价采取额外的应对措施以将安全风险降低至可接受的水平的必要性。

组织应评审业务伙伴依据 4.2 的规定所提供的安全声明，并运用专业判断、对实体的知识和/或监管机构的要求，或许还需获取并使用其他信息以确定安全声明是否可接受。

在实施安全评估和确定《申请书》中描述的供应链的整体脆弱性时，组织应考虑安全声明的具体内容及有效性。

业务伙伴如符合 4.3 或 4.4 的规定时，可不必进行进一步的评估。

以下信息应予以记录：

a) 考虑到的所有安全威胁场景；

b) 用于评估这些威胁情况的过程；

c) 经识别和优先排序的所有应对措施。

5.4 供应链安全计划的制定

组织应制定和保持针对其《申请书》中描述的整个供应链的安全计划。该计划可细分为多个附录，每个附录描述针对供应链特定环节制定的安全措施，包括 4.3 和 4.4 中所提及的业务伙伴保持的符合其安全声明的安全措施。该计划或附录还应说明组织将如何对此类安全声明进行监视和定期评审。

在制定安全计划时，组织应评审和考虑使用资料性附录 A 和附录 B 中的指南信息。

5.5 供应链安全计划的执行

组织应建立管理体系以保证供应链安全过程得以实施。

5.6 供应链安全过程的记录和监视

5.6.1 总则

组织应建立和保持程序以记录、监视和测量上述管理体系的绩效。组织应按策划的时间间隔对管理体系实施审核，以确保管理体系得以适当实施和保持。审核结果应予以记录并保留。

5.6.2 持续改进

组织应评估改进其安全安排的机会，作为提高供应链中其所处环节的安全性的手段。

5.7 安全事件发生后需采取的措施

组织控制的国际供应链环节发生安全事件后，组织应对其安全计划进行评审。这些评审应：

a) 确定事件发生的原因和纠正措施；

b) 确定安全恢复措施和程序的有效性；并

c) 考虑此类决定，按照 5.3.2 的要求重新评估供应链中的这些环节。

安全性遭到破坏时，组织应适时根据安全计划和合同关系确定的要求按照程序向海关和/或相关的执法机构报告。

组织应在法律法规规定的时间内保存委托方的货物和其他要求的供应链数据。

5.8 安全信息的保护

组织的安全计划、措施、过程、程序和记录应被视为敏感的安全信息，并防止未经授权的访问或披露。此类信息只能向“有知悉需求”的人员披露。除相关的执法机构或其授权的人员外，其他人员在以下情况中“有知悉需求”：

a) 需要访问特定的安全敏感信息以实施安全计划中规定的安全活动的人员；

b) 接受培训以实施安全计划中规定的安全活动的人员；

c) 监督其他实施安全计划中规定的安全活动的人员所需的信息；

d) 根据与组织的合同关系依照所约定的条款和条件经授权访问由组织控制的安全敏感信息的人员或其代表。

注：如果组织通过了经权威认可机构认可的第三方认证机构实施的 ISO 28001 认证，或双边互认的政府证明或证实其符合 ISO 28001 要求，此类经合同约定的对组织安全敏感信息的访问权并非必需，而是取决于组织的明确同意。保护组织的敏感安全信息免于未经授权的访问或披露这一事实并不妨碍组织向业务伙伴和其他人简要介绍其供应链安全布置和体系的情况。

附 录 A
（资料性附录）
供应链安全过程

A.1 总则

本附录提供了创建供应链安全过程的指南，该过程可在已建立管理体系的组织中实施。图 A.1 提供了有关此过程的图形描述。

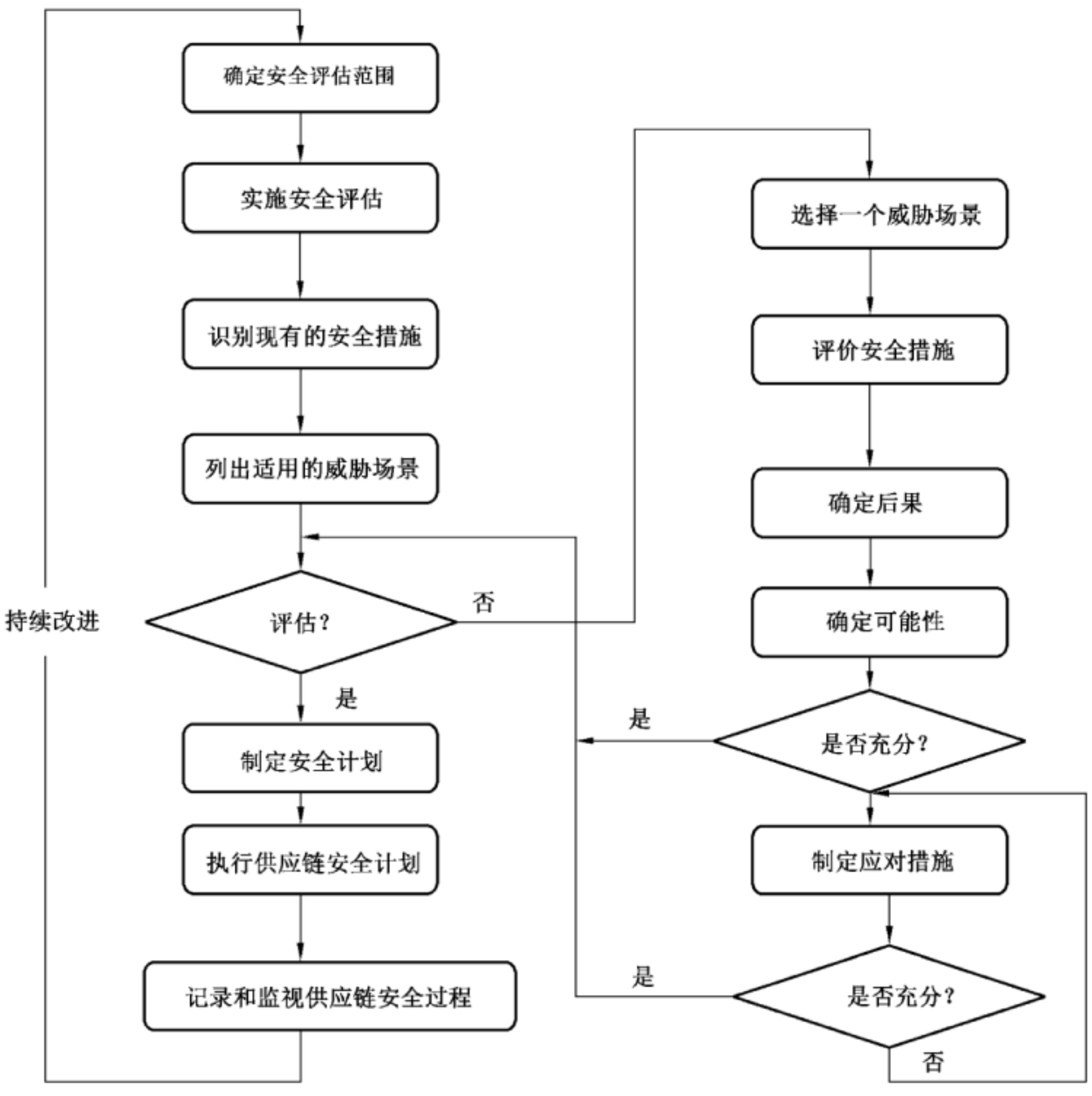

图 A.1 供应链安全过程的图形描述

A.2 识别安全评估范围

安全评估旨在识别组织在供应链中所处环节的安全风险。组织在其《申请书》中希望其所处环节符合本标准。为了完成这项评估，需确定评估范围的边界（包括实际的和虚拟的）。

A.3 实施安全评估

A.3.1 总则

具有资质的人员需要对存在潜在安全脆弱性的所有场所的现有安全布置进行评估，包括但不限于：

——在装箱、上托盘或准备装船前，货物的制造、加工或搬运；

——准备装运的货物在运输前的贮存或拼装；

——货物的运送；

——货物从运输工具上的装卸；

——货物保管权的交接；

——有关正在装运的货物的文件或信息的处理、产生或访问；

——采用不同交通工具进行运输的内陆运输路线和方式；

——其他。

A.3.2 绩效评审清单

下面的绩效评审清单提供了采用系统的方法评审现有安全布置的示例。

该部分绩效评审清单适用于已向组织证实过以下各项的合作伙伴：

a) 已经过验证符合本标准或 ISO 20858；

b) 符合 4.3 要求；或

c) 已按照国家海关根据世界海关组织《全球贸易安全与便利标准框架》确定的供应链安全方案被指定为授权经营者(AEOs)。

宜包含因素如何得到解决的注解，如符合本标准、ISO 20858，或者国际船舶和港口设施安全规则(ISPS 规则)。

A.3.3 绩效评审

对供应链中的组织实施安全评估时，可填写和参考表 A.1 所示的绩效评审清单。该清单并非详尽的，可根据风险评估和组织的商业模式进行调整。若所显示的因素已由供应链中的组织实施，宜选则“是”。若所显示的因素尚未实施或是部分符合，宜选择“否”。适当时，在备注栏中补充说明所采用的其他替代措施，或注明风险很低。如果因素不适用或不在组织的覆盖范围内，宜在“备注”栏中注明“不适用(NA)”。根据相关的法律法规要求在绩效评审清单中不能实施的项目，宜在备注栏中标识为禁止。

表 A.1 绩效评审清单

因素	是	否	备注
供应链安全管理			
● 组织是否建立了用于解决供应链安全问题的管理体系？			
● 组织是否指定专人负责供应链的安全？			
安全计划			
● 组织是否有现成的安全计划？			
● 策划是否包括了组织对上游和下游合作伙伴的安全期望？			

表 A.1（续）

因素	是	否	备注
• 组织是否制定了危机管理、业务连续性和安全恢复计划？			
资产安全			
• 组织是否制定措施解决： ——建筑物的物理安全性； ——对场所内外部环境的监视和控制； ——利用访问控制，禁止未经授权访问设施、运输工具，装卸码头和货物区，以及对身份识别卡（员工、访客、供应商等）和其他准入装置的发放施加管理控制？ • 是否存在可显著加强资产保护的运行安全技术？例如，采用入侵检测或覆盖供应链活动重要区域的 CCTV/DVS 影像记录，记录保留期应足够长以便用于事件的调查。			
• 是否制定了联络内部安全员或外部执法部门的协议，以防发生安全故障？			
• 是否制定了程序，限定、检测和报告未授权进入所有货物和运输储存区？			
• 在货物发放和接收前，是否有人员对货物的发放和接收进行确认？			
人员安全			
• 组织是否建立了程序，在雇用前对人员的诚信进行评价，并定期对其安全职责进行评价？			
• 组织是否开展岗位培训，帮助员工履行其安全职责，例如：维护货物完整性、识别潜在的内部安全威胁，保障访问控制措施？			
• 组织是否使员工了解公司所制定的报告可疑事件的程序？			
• 访问控制系统是否包含了立即清除合约到期的员工的身份识别卡和进入敏感区和信息系统的访问权的功能？			
信息安全			
• 是否执行程序确保用于货物加工的所有信息（电子的和人工的）均是易读的、及时的、准确的且防止被更改、丢失或导入错误数据？			
• 在组织运送或接收货物时是否核对货物与相应的运送文件的一致性？			
• 组织是否确保从业务伙伴那里收到的信息得到准确、及时的报告？			

表 A.1（续）

因素	是	否	备注
• 是否通过使用存储系统保护了相关的数据，不论主要数据处理系统是否运行（是否建立了数据备份过程）？			
• 是否所有用户都有唯一的标识码（用户 ID）且仅供个人使用，以保证其活动可以得到追溯？			
• 是否建立了一套有效的密码管理系统用于鉴定用户的真伪，是否要求这些用户至少每年更改一次密码？			
• 是否制定了保护措施以防止未经授权访问和不当使用信息？			
货物和运输安全			
• 是否建立了程序以限制、检测和报告对所有运输、码头装卸区及封闭式货物运输单元贮存区的未经授权的访问？			
• 是否指定合格人员负责监督货运业务？			
• 当检测出或怀疑有异常或违法活动发生时，组织是否建立了对相关的执法部门进行报告的程序？			
• 是否建立了程序确保被运送到供应链中其他组织（运输提供商、调度中心、联运公司等）的货物的完整性？			
• 是否建立了追踪运输路线威胁等级变化的程序？			
• 是否向运输经营者提供安全规则、程序或指南（例如，如何避开危险路线）？			
封闭式货物运输单元			
（世界海关组织《全球贸易安全与便利标准框架》附录的附件 1 包括了“密封完整性方案”，规定了对高安全性封印的和/或其他篡改检测装置的进行加盖和验证的程序。填写本表的人员宜评审该框架的相关部分。）			
• 若使用封闭式货物运输单元，是否建立了对符合 ISO /PAS 17712 的高安全性机械封印和/或其他篡改检测装置进行加盖和验证的书面程序？			
• 若使用封闭式货物运输单元，是否建立书面程序，检查在船运过程中运输保管权交接时封印是否有被窜改的迹象以及解决已被检测到差异？			
• 若使用封闭式货物运输单元，是否及时检查装填方在装填前是否对货物造成了损坏？			

表 A.1（续）

因素	是	否	备注
● 若使用封闭式货物运输单元，是否建立在装填方装填前对封闭式货物运输单元进行及时检查的书面程序，验证货物的物理完整性，包括单元锁定机制的可靠性？建议采取以下 7 点检查步骤： ——前壁 ——左侧 ——右侧 ——地面 ——天花板/屋顶 ——内/外卡箍 ——外部/底盘			

A.3.4 安全威胁场景

安全评估时考虑安全威胁场景，包括但不限于表 A.2 所列的内容。安全评估也宜考虑可能由政府部门、组织的管理层或实施评审的安全专家确定的其他场景。

表 A.2 供应链的安全威胁场景

安全威胁场景	应用
1. 侵入和/或控制供应链内的资产（包括运输工具）	损坏/破坏资产（包括交通工具）； 损坏/破坏使用资产或货物的外靶； 引起社会或经济动荡； 扣留人质/谋杀
2. 利用供应链走私	将武器非法运入或运出国家/经济体； 恐怖分子进入或离开国家/经济体
3. 篡改信息	从当地或远程侵入供应链信息系统/文件系统，目的是干扰运行或从事非法活动
4. 货物完整性	以散播恐怖主义为目的干扰、破坏和/或盗窃
5. 未经授权的使用	操纵国际供应链的运行以制造恐怖事件，包括使用运输工具作为武器
6. 其他	

A.4 制定安全计划

A.4.1 总则

安全计划和/或附录可纳入运行计划或程序中，无须成为单独的文件。如果安全计划纳入了其他计划中，组织宜保持一份对照表以验证安全计划的所有要求得到满足。

该计划可分为多个附录，各附录分别对供应链中某个特定环节的安全状况进行描述，包括组织的业务伙伴按照其安全声明（如适用）所维持的安全措施。该计划/附录还宜说明组织将如何监视或定期评

审其安全声明。该安全计划/附录宜包括但不限于下列描述：

——该计划或附录所覆盖的供应链中的环节；

——所有安全人员的安全相关职责；

——安全管理层的结构，包括被指定为安全经理人员的姓名；

——人员在报告安全事件时使用的内部和外部紧急情况安全联系方式；

——承担安全责任的人员需具备的技能和知识；

——安全培训方案；

——为确保被分配安全职责的人员具备履行其安全职责所需的技能和知识的资质确认过程；

——安全计划的各项要素如何实施；组织的人员参加政府组织的安全演习或演练可当做符合该要求；

——满足政府强加的应急措施或提高安全水平的最低安全要求的过程。

该安全计划宜包含程序，包括但不限于以下安排：

——确保承担后续运输的组织在货物运送前收到货物运送的信息；

——确保需要进行合并/拆箱的商品/收到的货物与货物资料/货物舱单/清单保持准确一致；发出商品/货物单元时应核对购买或交付订单；

——在收到或发送货物前，确保交付或接收货物的司机的身份已得到确认；

——除了确认司机身份外，确保车主身份得到确认；

——确保所有短缺、超载及其他重大差异或异常现象得到解决和/或适当的调查，且若检测发现非法或可疑的活动，适时通知相关执法机构；

——描述在供应链该环节已经实施的应对措施；

——描述在安全事件发生时供应链安全环节已实施的安全恢复措施和程序；

——描述当商品/货物的保管权交接给另一组织时所实施的措施和程序；

——描述向经授权的人员披露有关被运送的货物的额外信息的程序；这宜包括用户如何确定要求提供额外信息的请求是否合法，及如何披露信息或披露什么信息；

——描述依据 A.4.3 要求建立的程序。

A.4.2 形成文件

组织宜在可获取的安全且可检索的位置保持下列最新文件：

——覆盖范围说明；

——已完成的安全评估；

——实施安全评估人员的姓名和资质；

——考虑过的所有应对措施的清单；

——安全声明；

——安全计划和附录(如适用)；

——有关培训课程和演练、参与人员、培训项目和日期的记录；

——法规或管理部门规定的其他文件。

A.4.3 沟通

可行时，组织宜与相关执法部门和其他政府官员建立联系，旨在：

——建立程序，防止商品/货物被篡改或涉嫌被篡改、发生于国际供应链相关的紧急情况或收到有关国际供应链的威胁。此类程序宜包括相关政府部门的专用电话号码。此类程序宜纳入组织的供应链安全计划。

——参加相关国家或地方级的政府官员主导的协商，讨论双方共同关心的事宜，包括海关规则和程

序及经营场所和货物运输安全要求。

——响应政府做出的努力并就对话框架提出有意义的见解，以确保组织的安全计划保持相关性和有效性。

如果相关执法部门和其他政府官员不希望参加此类对话，组织宜记录其意图，并对相关执法部门和其他政府官员的缺席进行描述。

A.5 安全计划的执行

实施新的或修订的安全计划表明运行规范发生了变更，需要依据组织的管理体系来进行，以确保可获得充分的资源、对其他运行产生的影响得到了管理及计划的有效性得到了监视和评估。

A.6 记录和监视安全过程

组织宜建立和保持监视和测量其安全管理体系绩效的程序，以确保其持续的适宜性、充分性和有效性。在确定监视和测量关键绩效参数的频次时，组织宜考虑相关的安全威胁和风险，包括潜在的恶化机制及其后果。

A.7 持续改进

对供应链该环节的运行控制的管理宜评审组织的安全管理体系，以评估改进机会和变更安全管理体系的需求。

附 录 B
（资料性附录）
安全风险评估方法和对策的制定

B.1 总则

本附录给出的方法可供国际供应链中的组织用于评估其运行可能遭受的安全事件的风险，以确定适用于其供应链运行类型和规模的应对措施。该方法的使用顺序如下：

a） 列出范围内的所有活动；

b） 识别现有的安全控制措施；

c） 识别安全威胁场景；

d） 确定发生安全威胁场景的后果；

e） 考虑目前的安全状况，该情况发生的可能性；

f） 控制安全措施是否充分；

g） 如果没有，制定额外的安全措施。

图 B.1 为过程示意图。

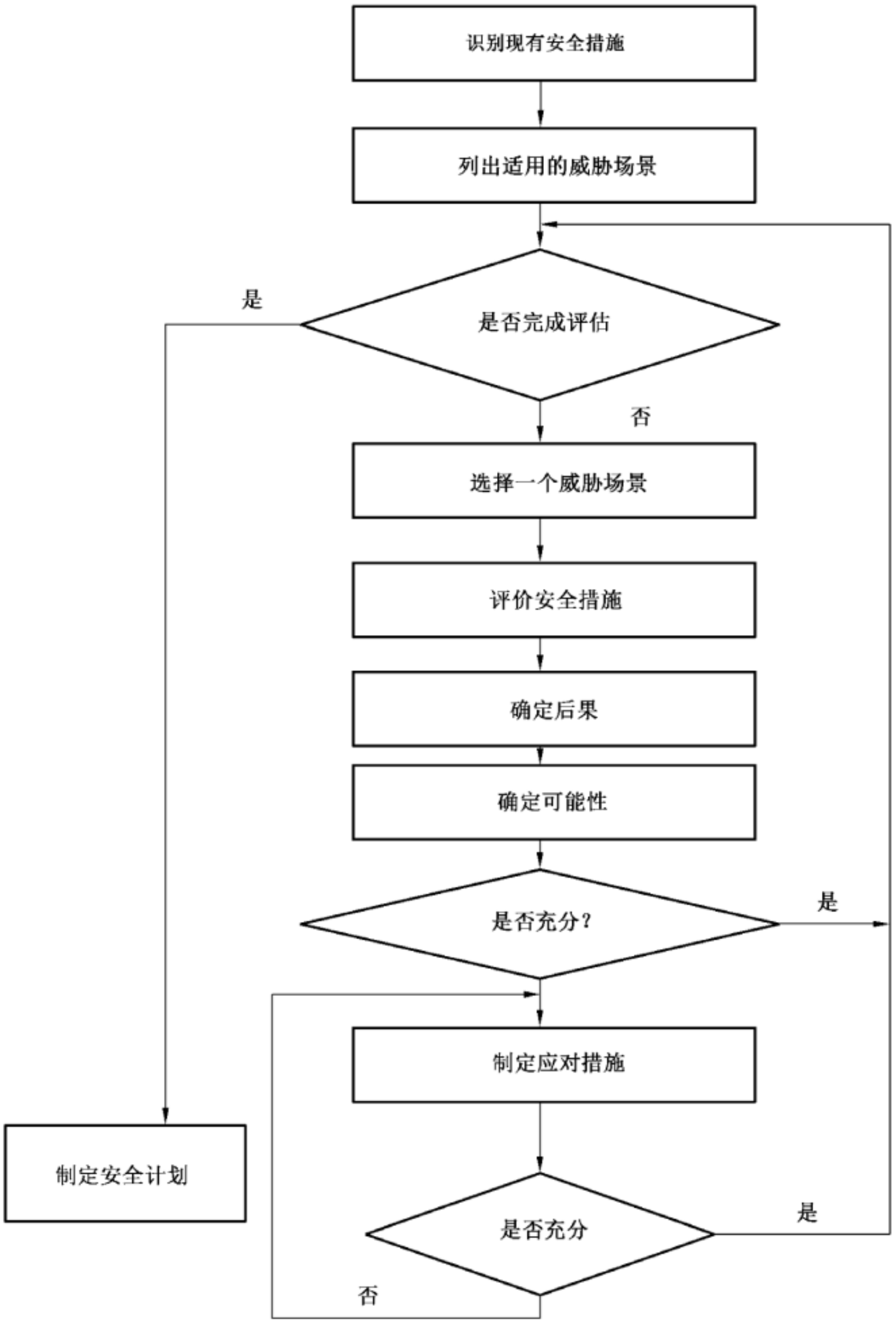

图 B.1　安全风险评估方法示意图

B.2　第一步——安全威胁场景的考虑

安全评估宜至少考虑表 B.1 所列出的安全威胁场景。安全评估也宜考虑由政府部门、供应链管理者或参与评估的安全专家识别的其他场景。

表 B.1　供应链的安全威胁场景

安全威胁场景示例	应用示例
1. 侵入和/或控制供应链内的资产(包括运输工具)	损坏/破坏资产； 损坏/破坏使用资产或货物的外靶； 引起社会或经济动荡； 扣留人质/谋杀
2. 利用供应链走私	将武器非法运入或运出国家/经济体； 恐怖分子进入或离开国家/经济体
3. 信息破坏	从当地或远程侵入供应链信息系统/文件系统，干扰运行或从事非法活动
4. 货物完整性	以散播恐怖主义为目的干扰、破坏和/或盗窃
5. 未经授权的使用	操纵国际供应链制的运行以制造恐怖主义事件，包括使用运输工具作为武器
6. 其他	

评估时考虑：

1)　对以下事项的访问控制：

——供应链中组织的营业场所，包括邻近地区；

——交通工具(卡车、铁路货车、航空器、驳船、船舶等)；

——信息系统；

——其他。

2)　交通方式（货运汽车、铁路、驳船、空运、海运等)，应考虑：

——正常运行；

——修理厂(如修车场)；

——由于故障等导致的变更；

——交通方式的变更；

——停用期间的运输工具；

——使用运输工具作为武器；

——其他。

3)　搬运：

——装载；

——制造；

——贮存(包括中间储存)；

——转运

——卸货；

——分装/合并；

——其他。

4)　货物的运输方式：

——空运；

——公路；

——铁路；

——内河水运；
——海洋船运；
——其他。

5） 适用于船运的入侵检测和预防。

6） 检查过程，例如车辆检查。

7） 雇员：
——能力、培训和意识；
——诚实；
——其他。

8） 业务伙伴的使用。

9） 内部/外部交流：
——信息交换；
——紧急情况；
——其他。

10） 有关货物的搬运或加工或运输路线的信息：
——数据保护；
——资料保证；
——其他。

11） 外部信息：
——法律的；
——当局的命令；
——行业规范；
——事故和事件；
——第一反应能力和反应时间；
——其他。

B.3 第二步——后果分类

对后果的评估宜考虑到可能的伤亡和经济损失。供应链中被评价的安全事件后果宜分为高、中、低三个等级（见表 B.2）。若数值结果可转化为定性的系统，则可在评估过程中采用数值系统。

针对所有安全事件的后果进行分类的依据宜予以记录。

确定高、中、低等级后果的数值时宜予以注意。采用过低的阈值可能导致针对安全威胁场景采取的应对措施高于实际需求。然而，采用过高的阈值则会忽略针对涉及组织或监管组织运行的政府不能容忍的安全威胁场景采取应对措施。

后果分类为“高”可被视为仅在发生的可能性较低的情况下才可接受的后果。

后果分类为“中”可被视为在发生的可能性较高的情况下不可接受的后果。

后果分类为“低”可被视为通常可接受的后果。

可接受性不宜与可取性或认同性相混淆。可接受性可理解为判断组织或监管组织运行的政府在某种与概率有关的情况下愿意接受的可能遭受的损害的数量。组织或政府可以决定，遭受一定程度的损害的可能性是不情愿的但却是可接受的。

表 B.2　后果分类

分配等级	后果
高	死亡和受伤:一定规模的死亡人数 和/或 经济影响:对资产和/或基础设施的严重破坏而阻止进一步运行 和/或 环境影响:生态系统受到大面积、多方面的毁灭性破坏
中	死亡和受伤:例如死亡 和/或 经济影响:对资产和/或基础设施的破坏而需要予以维修 和/或 环境影响:对生态系统的某一部分造成长期破坏
低	死亡和受伤:有受伤但无死亡 和/或 经济影响:对资产和/或基础设施和系统造成轻微损害 和/或 环境影响:局部环境破坏

B.4　第三步——安全事件发生可能性的分类

对潜在安全事件进行分类时,宜考虑安全绩效评审清单及提供的其他文件中所记录的供应链中物理安全措施和运行安全措施的状态。物理安全措施包括阻止或检测未经授权侵入目标的物体。运行安全措施包括阻止或检测未经授权侵入目标的人员和程序。针对特定资产发生的安全事件可能性宜分为高、中、低:

——高级宜适用于现有安全措施对安全事件的发生展现较弱抵抗能力的情况。若评估过程中使用了数值系统,数值结果宜转化为此定性的体系。

——中级宜适用于现有安全措施对安全事件的发生展现适中抵抗能力的情况。

——低级宜适用于现有安全措施对安全事件的发生展现强劲抵抗能力的情况。

对所有安全事件的发送概率进行分类的依据宜予以记录。

B.5　第四步——安全事件分级

表 B.3 中给出的安全事件等级表可用于确定何时宜考虑针对特定安全事件采取应对措施。

表 B.3　安全事件分级表

可能性分类				
高			中	低
后果分类	高	应对措施	应对措施	考虑
	中	应对措施	应对措施或适当时考虑	文件
	低	考虑	文件	文件

需对可能性和后果的评级均为高等级的安全事件确定应对措施，针对可能性评级为中等级且后果被评为高等级的安全事件也需如此。针对其他安全事件不需制定应对措施，除非被评估人认为是可取的。安全评估人员宜列出需采取应对措施的所有安全事件。

注：相关执法部门和其他政府官员可针对某些具有极高等级后果的场景（不论发生概率的大小）确定应对措施，作为国家方针。针对这一例外情况制定的应对措施宜由提出要求的政府来评审其有效性。

B.6 第五步——制定应对措施

若评价人员要求制定应对措施或认为制定应对措施是可取的，宜考虑减轻安全威胁场景的后果和/或可能性。最终目标是将安全威胁场景消除或将可能由安全威胁场景造成的伤害的可能性降至无须再采取额外应对措施的水平。

应对措施可归入以下几类措施：

——处置：可能为组织的措施，和/或物理性的措施；

——转移：风险的转移可以是分包、物理性转移到其他场所、变更时间等；

——终止：可能由于风险水平的原因，组织决定不再继续执行活动。

在某些特定情况下，因所需的应对措施无法实施、缺乏推行所需安全措施的权限或其他不可抗拒的因素，组织可能需容忍风险（见注解）。

注：容忍是指组织无法采取任何措施。此类活动和评估宜予以记录并定期评审。

B.7 第六步——实施应对措施

采取新的应对措施表明运作规范发生了变更，因此需要与组织的管理体系协调一致，以确保可获得充分的资源、对其他运行的影响得到管理及变更得到管理层的支持。

B.8 第七步——评价应对措施

宜采用本标准规定的方法评估每一项应对措施在降低可能性或后果（或两者同时）直至安全风险不再需要采取额外的应对措施方面的有效性。能实现这一目标的应对措施被认为是行之有效的，且宜被列入安全评估报告中。

B.9 第八步——过程的循环

在制定安全应对措施并评估有效后，继续下一个安全威胁场景，直至所列的安全威胁场景全部完成为止。

B.10 过程的持续

评估过程是持续的。如图 B.1 所示，安全性必须予以持续监视以确保安全措施按预期执行，且评估过程宜在需要时予以执行。

附 录 C
（资料性附录）
获取咨询建议和认证的指南

C.1 总则

有意实施 ISO 28001 的组织不一定要获得外部咨询服务。如果确定在实施安全评估、制定安全计划或实施所需的要求方面需要建议或帮助，组织可以寻求外部咨询服务。然而，寻求咨询服务的组织有责任核查并验证提供咨询服务的顾问的能力。例如，通过征求建议、听取参考意见或评审其已实施的工作进行核查和验证。向组织提供咨询的顾问不得参加对同一个组织的第三方审核。

C.2 通过审核证实与 ISO 28001 的符合性

ISO 28001 是一个要求规范，旨在帮助自愿实施该要求的组织确定和证实其在国际供应链中控制的那些环节具有适当水平的安全性。因此，它可作为通过第一方、第二方或第三方审核过程确定、确认或证实组织供应链现行安全性水平的依据，或选择将符合本标准作为进入其供应链安全方案的基本要求的政府机关。

审核类型：

——第一方审核是组织自我确定自身的符合性；

——第二方审核是由在供应链的运行中有既定利益的其他组织、机构或团体确定或验证组织是否符合约定的准则；

——第三方审核是由独立于所有各方的组织来确定或验证组织是否符合约定的准则。

由政府或政府代理机构实施验证和认证。

选择将符合本标准作为进入其供应链安全方案的基本要求的政府机关，或许希望亲自对符合性进行认证和验证，或为避免重复可选择信任其他机构的审核。世界海关组织（WCO）为各国海关当局制定了有关符合世界海关组织《全球贸易安全与便利标准框架》的国家海关供应链安全方案的验证和认证要求及对此类方案予以互认的指南。

C.3 由第三方认证机构实施 ISO 28001 认证

如果寻求通过第三方审核过程证实符合性，寻求认证的组织宜考虑选择由权威认可机构（如国际认可论坛（IAF）成员、签署《IAF 多边互认协议》（MLA）的机构）认可的第三方认证机构。此类获得认可的认证机构遵守国际互认规则、实施准则和审核协议，如 ISO 17021 和 ISO 19011。见注解部分。

参 考 文 献

[1] ISO 9001:2000 质量管理体系 要求(Quality management systems—Requirements)

[2] ISO 14001:2004 环境管理体系 要求与使用指南(Environmental management systems—Requirements with guidance for use)

[3] ISO 17021:2006 符合性评估 对提供管理体系的审核与认证的机构的要求(Conformity assessment—Requirements for bodies providing audit and certification of management systems)

[4] ISO/PAS 17712:2006 货运集装箱 机械密封(Freight containers—Mechanical seals)

[5] ISO 19011:2002 质量和/或环境管理体系审核指南(Guidelines for quality and/or environmental management systems auditing)

[6] ISO/PAS 20858:2004 船舶和航海技术 海运港口设施安全评估和安全计划研究制定(Ships and marine technology—Maritime port facility security assessments and security plan development)

[7] ISO 28000:2007 供应链安保管理体系规范(Specification for security management systems for the supply chain)

[8] ISO 28003:2007 供应链安全管理体系 对供应链安保管理体系提供审核和认证的机构要求(Security management systems for the supply chain—Requirements for bodies providing audit and certification of supply chain security management systems)

[9] 国际海事组织 国际安全管理(ISM)规则[International Safety Management(ISM) Code]

[10] 世界海关组织 SAFE 标准框架 附件 1 的附录(SAFE Framework of Standards—Appendix to Annex 1)