ICS 01.040.31

中华人民共和国电子行业标准

CCS V02

|  |
| --- |
|  |

SJ/TXXXXX-202X

|  |
| --- |
|  |

电子信息行业 供应链安全管理规范

（征求意见稿）

|  |
| --- |
|  |
|  |

202X- XX-XX发布

202X- XX-XX实施

中华人民共和国工业和信息化部   发布

SJ

目 次

[前 言 II](#_Toc162362791)

[引 言 III](#_Toc162362792)

[1 范围 1](#_Toc162362793)

[2 规范性引用文件 1](#_Toc162362794)

[3 术语和定义 1](#_Toc162362795)

[4 总则 2](#_Toc162362796)

[4.1 电子信息行业供应链模型 2](#_Toc162362797)

[4.2 电子信息行业供应链安全影响因素 3](#_Toc162362798)

[4.3 电子信息行业供应链风险管理 3](#_Toc162362799)

[4.4 电子信息行业供应链策略管理 4](#_Toc162362800)

[4.5 运行中的安全 4](#_Toc162362801)

[4.6 电子信息行业供应商管理 9](#_Toc162362802)

[4.7 电子信息行业供应链安全预警与应急管理 10](#_Toc162362803)

[4.8 电子信息行业供应链安全监测 11](#_Toc162362804)

[4.9 电子信息行业供应链安全数据和信息化管理 12](#_Toc162362805)

[附录A.1（资料性附录） 13](#_Toc162362806)

[电子信息企业供应链管理关键指标 13](#_Toc162362807)

[附录A.2（资料性附录） 15](#_Toc162362808)

[电子信息企业供应链安全关键指标 15](#_Toc162362809)

[附录A.3（资料性附录） 16](#_Toc162362810)

[电子信息企业供应链安全风险计算方法 16](#_Toc162362811)

[附录A.4（资料性附录） 17](#_Toc162362812)

[电子信息企业供应链安全威胁清单 17](#_Toc162362813)

[附录A.5（资料性附录） 18](#_Toc162362814)

[电子信息企业供应链安全脆弱性清单 18](#_Toc162362815)

[附录A.6（资料性附录） 20](#_Toc162362816)

[电子信息企业供应链安全事件后果分类 20](#_Toc162362817)

[附录A.7（资料性附录） 21](#_Toc162362818)

[电子信息企业供应链安全事件发生可能性分类 21](#_Toc162362819)

[附录A.8（资料性附录） 22](#_Toc162362820)

[电子信息企业供应链安全风险处置模型 22](#_Toc162362821)

[附录A.9（资料性附录） 23](#_Toc162362822)

[电子信息企业供应链紧急情况清单 23](#_Toc162362823)

[附录B（资料性附录） 26](#_Toc162362824)

[电子信息企业供应链相关法律法规 26](#_Toc162362825)

[附录C（资料性附录） 27](#_Toc162362826)

[电子信息行业物料分类表 27](#_Toc162362827)

[参考文献 30](#_Toc162362828)

#

# 前 言

本标准按照GB/T1.1-2020《标准化组导则 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这些专利的责任。

本标准由\*\*\*\*\*\*\*\*提出。

本标准由\*\*\*\*\*\*\*\*归口。

本标准起草单位：等。

本标准主要起草人：

# 引 言

采用供应链安全管理体系是组织的一项战略决策，能够帮助其提高整体绩效，为推动可持续发展奠定良好基础。

组织根据本标准实施供应链安全管理体系的潜在益处是：

a）提升客户满意度；

b）降低企业成本；

c）优化供应链整体流程和品质；

d）证实符合规定的供应链安全管理体系要求的能力；

本标准可用于内部和外部各方。

实施本标准并非需要：

——统一不同供应链安全管理体系的架构；

——形成与本标准条款结构相一致的文件；

——在组织内使用本标准的特定术语。

**电子信息行业 供应链安全管理规范**

# 1 范围

本标准为下列组织规定了供应链安全管理体系要求：

a)以供应链安全为管理视角，实施、维护和改进供应链安全管理体系；

b)需要证实其具有可信的供应链安全保障能力；

c)增强顾客满意。

本标准适用于电子信息企业实施供应链安全管理，并适用于不同规模和提供不同产品和服务的组织。

# 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。

GB/T 19000—2016 质量管理体系 基础和术语

GB/T 24420-2009 供应链风险管理指南

GB/T 25103-2010 供应链管理业务参考模型

GB/T 40753-2021 供应链安全管理体系实施指南

ISO28000-2022 供应链安全管理体系规范

# 3 术语和定义

3.1 供应链

从原材料采购一直到通过运输将产品或服务提供给最终顾客的一组过程和资源构成的网络。

注：供应链可能包括卖主、生产商、物流商、外销中心、配送者、批发商和其他到最终用户的实体。

3.2 安全

阻止了有意、未经授权而对供应链造成损害和破坏行为的状态。

针对旨在对供应链造成损坏或破坏或由供应链损坏或破坏的故意行为的抵抗力。

3.3 安全管理

组织通过有效地管理风险与潜在的威胁和影响而开展的系统的、协调的活动和实践。

3.4.设施

工厂、机器、财产、建筑、汽车、轮船、港口设施和基础设施或与之相关的计量、服务的系统。

注：此定义包括用于判定安全交付和安全管理的任何软件。

5.相关方

关注组织的业绩、成就或活动效果的个人或团体。

注：例如包括顾客、股东、金融机构、保险公司、法人团体、监管机构、雇员、合同方、供应商、劳工组织和一些社会团体等。

6.下游

发生在货物脱离组织的直接作业控制之后，供应链中涉及的行为、过程和货物移动，包括但不仅限于保险、金融、数据管理、包装、存储和货物转移。

7.上游

发生在货物到达组织的直接作业控制之前，供应链中涉及的行为、过程和货物移动，包括但不仅限于保险、金融、数据管理、包装、存储和货物转移。

8. 供应链管理 supply chain management；SCM

利用信息技术全面规划供应链中的商流、物流、资金流及信息流等，并进行计划、组织、协调与控制的各种活动和过程。

9. 商流 business process

指供应链中交易的商务过程。

10. 物流 logistics

物品从供应地向接受地的实体流动过程。根据实际需要，将运输、储存、装卸、搬运、包装、流通加工、配送、信息处理等基本功能实施有机结合。［

11. 资金流 fund flow

伴随供应链中商务活动而发生的资金往来的流动过程。

12. 信息流 information flow

伴随供应链中的商流、物流，资金流而产生的信息的流动过程。

[以上术语来源：ISO28000:2007]

## 4 总则

## 4.1 电子信息行业供应链模型

电子信息行业供应链管理，应从三个维度进行考虑，即：与供应链相关的活动、供应链流动过程和供应链风险管理过程（见图一）。对这些过程进行系统的管理，特别是管理这些过程之间的相互关系，能够使供应链管理更加完整和有效。供应链安全管理基于以下模型开展，能充分识别供应链安全问题，更好规避供应链风险，使组织的安全更具韧性。



**图一 电子信息行业供应链模型**

## 4.2 电子信息行业供应链安全影响因素

4.2.1 组织应识别影响供应链安全的因素，这些因素存在于组织提供的产品或服务、内/外向管理活动和应遵守的合规要求中，当发生变更或者引入新的时，应对影响安全的因素进行重新识别。

电子信息行业，典型的影响因素如：芯片等高端电子零部件的供应、软件组件供应、操作系统及工业软件使用、高端生产/开发和检测设备/工具使用、高端生产辅助设施使用、生产性辅助材料及设施使用以及售后技术支持等。

4.2.2 组织应对识别的供应链安全因素进行评价，将结果进行排序，并按照自身建立的评价准则确定重要安全因素。这些重要安全因素应定期进行评价，并且均需进行风险评估。

4.2.3 组织应将供应链安全因素的识别进行必要的渗透分析，如可行，包括供应商、供应商的供应商等，直至处于可接受状态为止。

4.2.4 组织应保持以下内容的文件化信息：

1. 供应链安全因素及影响结果；
2. 确定供应链安全因素的评价准则；
3. 供应链安全重要因素；

## 4.3 电子信息行业供应链风险管理

组织应根据供应链安全因素识别的结果，将风险管理纳入组织的产品/服务、内/外向业务过程和相关的职能中，同时明确风险管理责任、职责和权限，并提供适宜资源。

组织应设置专责部门按照风险评估准则实施并保持风险评估和处置过程。

供应链安全风险评估过程主要包括风险识别、风险分析和风险评价三个过程，具体实施可以参照ISO31000的基本原则开展。

供应链安全风险处置过程主要包括评估已识别的风险，确定是否需要进一步采取措施。风险评估的结果应进行记录和沟通，根据风险管理要求在相关职能和层级进行确认；

1. 确定需要处置的风险，并明确部门内处置风险相关的职责分工；
2. 实施风险应对，选择和实施风险处理方案，包括规避风险、接受风险、消除风险源、风险转移等；
3. 编制和实施风险应对计划，明确如何实施所选定的风险应对方案，并使相关人员了解应对计划，根据策划的要求实施；

组织应指定部门及人员负责监督和检查风险管理的实施，收集和分析相关信息，记录风险管理的实施情况，并提供必要的反馈。

## 4.4 电子信息行业供应链策略管理

组织应针对供应链外部威胁、内部脆弱性和评价的风险结果，制定供应链安全管理策略,形成文件化信息并经批准。常见的供应链策略如：产品设计策略、定价策略、生产策略、库存策略、供应商策略、运输策略等。供应链安全策略应在内部进行传达，并在需要时传达给外部相关方；

组织应根据职责分工，实施和保持选定的安全策略。根据建立的控制程序、实施规范、响应计划等，保持安全策略实施的相关记录，包括实施安全策略所采取的进一步改进措施。

组织应对供应链安全策略的执行进行日常检查，确保策略被有效执行。应定期或在发生重大变更时进行评审，确保持续的适宜性、充分性和有效性。评审应包括供应链安全策略和供应链管理措施的改进机会，已适应组织的环境、业务状况、法律法规或技术环境发生的变化。

组织在策划供应链安全策略时，应根据对风险的接受程度，适当考虑供应商的或者供应商的供应商的风险状况。

## 4.5 运行中的安全

4.5.1 需求管理

组织应以用户需求为关注点，对用户需求进行确定和管理，为后续生产决策提供准确信息。

用户需求应明确（但不限于），形成文件化信息并经评审和批准：

1. 产品信息；
2. 物流信息；
3. 商业信息；
4. 资金信息；

组织应对需求实现的风险进行充分考虑，对需求实现过程进行监控，对需求实现的关键指标进行统

计和分析。

组织应对需求管理制定必要的控制计划，当需求发生变更时，应评审非预期变更的后果，必要时采

取措施减轻任何不利影响，并适时更新需求控制计划。

 组织应通过需求管理提升供应链效益，并开展供应链效益分析，分析信息及产生的后续改进活动

，应形成文件化信息。

4.5.2内向管理

4.5.2.1采购

 组织应制定采购战略，确定组织和外包方履行的职责。采购战略应符合组织的整体战略并充分考虑供应链风险。

组织应建立采购业务流程，确保采购过程规范，选定的供应方符合采购要求。组织应：

1. 基于自身业务特点、采购产品的重要性和可获得性，并考虑持续供应、地域分布等因素，识别其采购潜在风险，可采取联盟采购、一品多点等方式予以化解或降低风险；
2. 根据时事动态、自然环境事件等突发情况，分析影响程度，采取应对措施；
3. 根据供应方的经营和生产状况，及时应对意外事件的发生；
4. 要求供应方依据有关法律法规和标准要求，提供相符合的质量安全合格证明、溯源证明等。
5. 采购软件产品，应溯源其开发方，必要时进行安全测评；
6. 采购技术服务时，供应方应按照有关规定，实施人员身份安全认证程序，并提供技术能力评定、服务人员联系方式等信息；
7. 将需求预测等信息通知到供应方，沟通供应方及时将产品即将停产、改进等信息反馈给组织，避免产生不必要的风险。

组织应建立采购产品信息库、供应商信息库，在新品导入、产品定价、招投标、产品订货、供应商

下单等过程建立明确流程，并对实施过程进行监督。

 组织应与供应商建立良好的沟通过程，确保将采购风险降至组织可接受的程度。

组织应对采购全程建立并保留文件化信息。

4.5.2.2制造执行管理

 组织应根据需求信息开展生产决策，决策应充分考虑产品提供的风险。组织应对内外部资源进行充分整合，将物资流、信息流和资金流打造成一体化资源进行管理。

组织应对产品制造流程进行监控、跟踪和控制，确保产品及时交付的同时保证产品质量持续稳定满足要求。主要包括：

1. 设计开发：
2. 对设计开发进行策划，确定与市场、顾客需求相适宜的技术体制，尽量选择成熟度高的体制，策划书须得到评审；测试、试验、验证所需要的设施、设备、工具的可获得性和保障性应予以考虑；必要时，应确定设计开发工具（包括软硬件），并确保其可获得性及保障性；
3. 必要时，应根据设计开发的不同阶段，制定原材料（元器件）大纲，以指导各级产品开展设计；
4. 方案设计过程应识别核心和关键技术，制定妥善的解决措施。各级产品方案均须得到评审，必要时应邀请顾客参加；
5. 各级产品的原材料应综合技术、计划、质量、成本、国产化等方面要求开展选型，新选用物料应予以认证，物料清单应得到审核。从安全角度，选型、审核一般遵循以下原则：核心技术和产品有设计能力的避免外包外购，优先选择货架或成熟产品、材料，尽量选择优选供方，外协和代工宜选择质量可靠的合作方，核心物料和协作尽量选择国产供方。
6. 生产制造：

组织应：

1. 根据订单要求制定合理的生产计划，确保订单要求的产品按时交付；
2. 根据需求计划制定物料需求和采购、配发计划；如有物料停产、改型等情况，组织开展设计变更；
3. 按生产计划及相关文件资料开展生产制造，按要求做好异常情况处理并保存相关记录；
4. 与采购、供应商、仓库、设计、质量等做好沟通并开展协调，确保各项资源和信息畅通；
5. 确保生产制造过程的产品质量满足产品交付要求。
6. 产品质量管理

组织应对由产品质量造成供应链风险的情况进行管理，确保采购的产品、生产过程和

出厂前的产品质量满足要求。

 组织应建立完善的质量管理机制，对质量问题开展统计和分析，并不断开展质量改进。

 组织应保留完整的质量管控的文件化信息。

1. 仓储和搬运

 制造执行阶段的库存以原材料、在制品、半程品的形式存在。组织应对供应链的不确定性开展风险管理，同时确保库存数量与生产任务相匹配并能及时供应。组织应：

1. 建立生产制造过程仓储管理的相关制度；
2. 结合生产制造中元器件、原材料、辅料、半成品及成品的存储需求、生产计划、工艺布局等，配置必要的暂存库、中转库、半成品库及成品库等，设置专人进行管理；
3. 存储的物品、载具、设备、场地区域等均应做好标识，以便于识别和查询；
4. 确保库存储环境满足产品存放要求
5. 确定安全库存和零库存的适用范围及管理要求，综合采购周期、采购频次，确定采购产品安全库存和补库策略并得到评审。
6. 建立合理的安全库存存储方式并形成清单，例如自有库存、寄售库存和供应商管理库存（VMI）等，明确相关适用范围及管理要求；
7. 做好每次补库策略及评审结果记录；
8. 形成安全库存清单并保存；
9. 做好与需求、物料、生产、市场等沟通；

 组织应建立并优化仓储管理信息化系统，全方位对现有库存进行数据化管理并及时向所需部门提供库存信息，同时为安全库存提供预警数据支撑。

组织应确保在搬运过程中产品不受到损坏，避免由于产品问题造成供应链风险。

1. 创新管理

 组织应建立内部创新机制，确保供应链安全。

**4.5.3外向管理**

组织应确保将产成品及时安全地交付给客户，对包括：订单处理、运输、产成品的库存管理和仓储管理、包装、物料搬运等过程实施有效管理，同时保证相关的信息的安全。

4.5.3.1订单处理过程

组织应建立、实施并保持订单处理过程，必要时采用信息技术手段，确保按质、按量、按时满足顾客要求，应考虑：

* 1. 法律法规的要求、组织总体目标要求，进行客户资质和信用的检查；
	2. 客户需求信息被安全、准确、及时地得到满足，并有效传达；
	3. 明确以上过程中的信息安全管理手段以及监测方式，对检测结果进行分析，及时预警并采取及时有效地措施实施改善，以减少风险。

4.5.3.2运输、配送管理

组织应制定配送战略，建立、实施并保持运输和配送过程，预防、减少、回避或转移相关风险，满足客户对产品或服务的需求。

1. 采取适当的监视测量手段对运输、配送过程进行定期监控和检查评价，并在有追溯要求的情况

下实现过程追溯的要求；

1. 委托第三方物流的情况，按照4.6供应商管理的要求，确保交货的经济性、效率与安全性，建

立第三方准入、运作管理、考核、评价的制度；

1. 组织应做好内部和外部的沟通，确保信息准确，必要时保留沟通记录。

4.5.3.3仓储与库存管理

组织应制定仓储与库存管理战略，以更为经济的方式及时交付产品。

1. 建立合理的仓储规划和库存布局规划；
2. 使用适宜的工具对库存数据进行定期分析，确保库存产品的有效整合与合理利用；
3. 组织应保持必要程度的文件化信息，以确信过程能按策划的要求得到实施。

**4.5.5财务及金融管理**

组织应在供应链管理中建立财务管理过程，控制财务风险，确保各个环节的货款和资金流动得当。组织应开展以下控制活动：

1. 预算规划 - 制定供应链管理的预算计划以及如何支配和使用资金；
2. 成本控制 - 通过管理成本来提高整体利润，包括降低库存持有成本、运输成本等；
3. 资本调配 - 在不同的环节之间分配资金，确保每个环节都能正常运转，为公司带来利润；
4. 供应商合同管理 - 确定供应商价格和付款条件，以便更好地控制和规划开支；
5. 库存管理 - 控制库存水平，以避免过度储备，减少库存持有成本，同时确保供应链的连续性；
6. 运输成本控制 - 找到最佳的运输方式，以减少运输成本；
7. 数据跟踪 - 追踪财务数据，分析供应链中的开支和收益，便于做出改进决策。

必要时，组织应制定财务管理目标，建立财务管理目标评价体系。

## 4.6 电子信息行业供应商管理

4.6.1 总则

通常，在下列活动中，应考虑供应链安全管理因素，并实施控制。

* 1. 供应商开发活动;
	2. 供应商评价活动;
	3. 供应商选择活动;
	4. 供应商提供产品和服务的控制活动;
	5. 供应商绩效监视与再评价活动;
	6. 关系维护活动。

对于这些活动引发的任何必要的措施，组织应保留成文信息。

4.6.2控制类型和程度(或影响供应链活动)
 组织应确保供应商提供的产品和服务不会对组织稳定地向顾客交付合格产品和服务的能力产生不利的影响。
 组织在供应商管理活动中应：
 a)在供应商开发活动中，组织应规定关键供应商开发深度、广度，在供应商技术、质量能力满足组织需求的基础上，应能够形成较为充分的竞争，尽可能的减少孤源与独子线供应商。
 关键、非关键定义参考1S0/TS22318供应链连续性指南。
 关键：如果不能准时、保质地，并且在本制提供产品或服务，会影组织重要业务流程的供应商，甚至一旦供应中断，就会影响组织生存。
 非关键:对其产品或服务的中断有一定容忍度，不会影响组织关键业务的供应商。
 b)供应商评价活动中，组织应规定供方资质能力、经营与合作风险的审查要求与采纳条件，并提供适宜的审查工具。
 c)供应商选择活动中，选与独子线供商或其他风险供应商进行必要性评估，并明确应急对策。
 d)供应商提供产品和服务的控制活动中，应对提供关键产品和服务的供应商实施控制，应从生产能力、生产计划、关键、特殊过程、技术状态变化情况进行监督。
 e)供应商绩效监视与再评价活动中，对于供应商业绩应实施量化评价与考核，并向供应商有效传递，建立供应商退出机制，并实施管理闭环。
 f)关系维护活动中应考虑协作深度与控制力度。
4.6.3供应商管理安全因素
 供应商管理活动中涉及的安全因素主要包括:
 a)缺少合适的供应商，影响组织产品研制进度、质量、成本；

b)供应商数量不足，难以形成充分竞争；

c)关键供应商存在孤源、独子线情况；
d)关键供应商集中在某一地域，当该地域发生自然灾害等不可抗力因素时，存在供应链中断风险；
e)供应商资质能力、经营能力存在风险，不具备履行合同能力;
f)供应商存在诚信与廉洁风险，影响组织产品研制进度、质量、成本；
g)对关键供应商提供产品和服务的过程未采取有效控制措施，关键供应商出现供应风险时，未及时采取措施；
h)供应商评价与考核机制缺失或未形成闭环，难以识别并控制供应商风险;

i)未建立供应商退出机制，存在不符合条件的供应商继续合作。

## 4.7 电子信息行业供应链安全预警与应急管理

组织应建立具备弹性的供应链，在供应链部分失效时，能保持连续供应且能快速恢复到正常供应状态。

组织应识别供应链失效的情况，包括引起失效的因素（威胁和脆弱性）、引发的后果。组织应建立内外部信息共享机制（包括供应商、生产者、分销商、顾客、合作伙伴等），及时发现供应链上的紧急风险。

组织应建立供应链冗余机制，特别是在生产能力、库存环节、资金使用等方面保持适度的冗余，提高应对紧急情况的能力。

组织应建立供应链应急机制，制定应急预案，在突发事件或风险发生之前，尽量消除各种隐患，减少风险或应急事件的发生。在风险发生时，将损失有效地控制在可接受的范围内。

 组织应根据内外部环境，及时开展应急演练，评估供应链风险控制状况。在发生紧急情况时实施应急措施，同时评估措施的效果，必要时重新评审应急预案。

组织应开展应急保障工作，包括：人力资源保障、财力保障、物资/设备保障、交通运输保障、技术保障等；

组织应保持应急管理的文件化信息。

## 4.8 电子信息行业供应链安全监测

组织应制定针对供应链安全实施监测的控制程序,在供应商管理、生产/服务管理、物流管理、质量管理、数据安全、存储和销售、法律合规、业务连续等方面对供应链安全绩效进行监测。安全监测需要考虑如下内容的规定，包括但不限于：

1. 确定对供应链安全监测的范围；
2. 确定定性和定量监测的内容；
3. 确定主动监测（如组织确定的安全活动）和被动监测（如紧急情况或安全事件）的内容，确定安全目标是否实现；
4. 确定安全监测的方法和技巧；
5. 识别并控制用于安全监测需要使用的安全设备，必要时，提供书面程序说明如何进行安全测量，并宜采用恰当的方法校准和维护安全设备；
6. 需要使用的信息系统、软件或工具的要求；
7. 明确安全监测的时间、记录、和人员要求；
8. 由安全监测产生的纠正和预防行为要求，以及对监测信息的收集、分析、保存、公布等处置要求。

## 4.9 电子信息行业供应链安全数据和信息化管理

4.9.1供应链数据信息安全管理

组织应对供应链相关数据信息进行分级管理，按照分级后的数据重要度采取相应的数据安全管理措施。
 组织在供应链运行过程中，产生的数据信息一般包含但不限于:产品或服务基础信息、供方基础信息、物资选用信息、产品或服务采购信息、技术质量信息、产品或服务用途、合同书、招标书、计划书等，其中可能包括产品和服务的用途、部分产品和服务的进度信息、技术指标、数量、用户、物资运输的时间、交货地点、运输方式、押运、路线、车次(航班)等重要信息，可能涉及不同程度的商业核心数据信息。
 组织的产品或服务涉及国家或商业关键数据信息时，应控制背景、用途等敏感内容，不得向供应商或其他相关方提供必须的技术以外的敏感信息数据，如必须提供时，应按符合国家和组织规定的程序提供。组织应与相关方签订保密协议，在与相关方咨询、交流过程中，应采取降密、脱密措施，隐藏产品和服务的实际用途，控制国家和商业秘密的知悉范围，并不得涉及以下内容:
 a)组织研制和生产中涉密产品和服务的完整名称、型号、技术指标、用途、布局情况、试验场所、研发生产计划、交付计划和价格成本等;
 b)组织的生产能力、生产数量;
 c)组织关键、敏感的采购渠道与物流渠道。
 组织应对涉及供应链安全的数据信息进行权限管理，设置查询、借阅权限，同时涉及国家或商业采购相关信息，应严格控制传递与知悉范围，国家秘密禁止在互联网上留存或传递相关信息，商业秘密应按组织规定在互联网上传递并采取安全保护措施。
4.9.2供应链信息化安全管理
 组织应建立并使用供应链信息化系统，在提高供应链运行效能的同时，对供应链安全采取风险识别与监视测量。
 组织应通过信息化实现本标准所明确的全部或部分供应链安全因素。
 组织应参照 GB/T36637 信息安全技术ICT供应链安全风险管理指南，以及国家《信息安全等级保护管理办法》规定，开展供应链信息化建设。

附录A.1（资料性附录）

电子信息企业供应链管理关键指标

|  |  |  |
| --- | --- | --- |
| 性能特征 | 性能特征定义 | 衡量指标 |
| 供应链可靠性 | 在正确的时间、将正确的产品以正确的质量、正确的包装送到正确的地点的能力 | 签单返回及时率 |
| 订单发货及时率 |
| 供应链的柔性 | 供应链面对市场变化获得和维持竞争优势的灵活性 | 交付周期 |
| 生产周期 |
| 供应链成本 | 供应链运营所耗成本 | 采购成本降低比率 |
| 产品保证/物流成本 |
| 退货处理成本 |
| 供应链管理的资产利用率 | 一个组织为满足需求利用资本的有效性，包括各项资本的利用：固定资本和运营资本 | 生产存货周转率(次/年) |
| 超长期存货比例/金额 |
| 交货及时性 | 在一定时期内供应链各节点准时交货（或服务）次数占其总交货次数的百分比 | 准时交货率 |
| 产品质量 | 供应链各节点提供的质量合格的产品（服务）数量占产品（服务）总产量的百分比 | 产品质量合格率 |
| 产销经营状况 | 在一定时期已经销售的产品总量与可供销售的工业产品总量之比 | 产销率 |
| 供应链整体运营状况 | 在一定时间内，企业供应链各节点已生产的产品数（或提供的服务）与其下游节点（或用户）对该产品（或服务）的需求量的比值 | 产需率 |
| 需求响应程度 | 供应链各节点产品出产（或服务）的出产节拍或出产间隔时间 | 产品出产（或服务）循环期 |
| 资金利用 | 某时间段的出库总金额（总数量）与该时间段库存平均金额（或数量）的比。是指在一定期间（一年或半年）库存周转的速度 | 库存周转率 |

附录A.2（资料性附录）

电子信息企业供应链安全关键指标

组织应基于策略、程序、过程和处理的程度，识别源于内外部的供应链安全相关的关键信息，建立关键信息清单，确保：

a）提供充足的资源。

b）保持对与安全相关的漏洞和威胁的分析以及供应链安全风险评估，确定风险等级。

c）针对电子产品研发安全、生产安全、储存安全、信息安全、资金安全等环节要建立相应的安全策略，降低安全漏洞，并保持相关记录

d）保持任何安全处置缺陷的期限并限制其影响；

|  |
| --- |
| A.2电子信息企业供应链安全关键信息表 |
| 目标：供应链安全的关键信息的控制 |
| A.2.1 | 威胁识别完整性 | 控制：供应链安全威胁和漏洞，威胁和漏洞的识别和分析 |
| A.2.2 | 风险评估准确性 | 控制：供应链安全风险评估，确定风险等级，针对电子产品研发安全、生产安全、储存安全、信息安全、资金安全等环节要建立相应降低安全漏洞的安全策略和方案，并保持相关记录 |
| A.2.3 | 配置资源可用性 | 控制：供应链安全策略资源配备，配备资源，确保可用 |
| A.2.4 | 安全处置有效性 | 控制：供应链安全业务影响分析，识别所有安全处置的缺陷及期限，并限制其影响 |
| A.2.5 | 安全评估充分性 | 控制：供应链的安全表现评估，收集所有有关责任、规程、事态、评估、决策、响应的证据 |
| A.2.6 | 事件管理有效性 | 控制：事件管理，安全事件管理、改进成果物 |

附录A.3（资料性附录）

电子信息企业供应链安全风险计算方法

组织应基于策略、程序、过程和处理的程度，保持对与安全相关的漏洞和威胁的分析以及供应链安全风险评估，确定风险等级，风险等级确定方法:

1. 建立风险准则，包括接受准则以及风险评估实施准则；
2. 识别供应链安全风险，分析并评估风险发生后可能导致的潜在后果以及实际发生时的潜在后果,确定风险级别；
3. 分析风险优先级，确定风险处置排序；
4. 确定需要处理的风险；

注意本节中的风险与供应链安全的风险有关。与管理体系有效性相关的风险和机遇在正文6.1中进行了阐述。

附录A.4（资料性附录）

电子信息企业供应链安全威胁清单

|  |  |  |
| --- | --- | --- |
| 类型 | 描述 | 示例 |
| 恶意篡改 | 在ICT供应链的设计、开发、采购、生产、仓储、物流、销售、维护、返回等某一环节，对ICT产品或上游组件进行恶意篡改、植入、替换等，以嵌入包含恶意逻辑的软件或硬件 | 恶意程序、硬件木马、外来组件被篡改、未经授权的配置、供应信息篡改 |
| 假冒伪劣 | ICT产品或上游组件存在侵犯知识产权、质量低劣等问题 | 不合格产品、未经授权的生产、假冒产品 |
| 供应链中断或终止 | 由于人为或自然的原因，造成ICT产品和服务的供应量或质量下降，甚至出现ICT供应链中断或终止 | 人为或自然的突发事件中断、基础设施故障、国际环境影响、不正当竞争行为、不被支持的组件 |
| 信息泄露 | 供应链上传递的敏感信息被非法泄露 | 供应链的共享信息、商业秘密泄露 |
| 违规操作 | 供方的违规操作行为 | 供应商违规收集或使用用户数据、滥用大数据分析、非法远程控制用户产品、影响市场秩序 |
| 其他威胁 | 供应链的全球分布性为供应链安全带来了新的威胁或挑战 | 需方安全风险控制能力下降、法律法规差异性挑战、全球化供应链管理挑战 |

附录A.5（资料性附录）

电子信息企业供应链安全脆弱性清单

|  |  |  |
| --- | --- | --- |
| 类型 | 子类 | 示例 |
| 供应链生命周期的脆弱性 | 开发阶段脆弱性 | 产品和服务在设计、开发阶段可能存在安全隐患，如：产品和服务设计时未对安全需求、安全威胁进行分析，开发时未遵循安全开发流程，没有建立完善的配置管理控制产品或组件的变更，没有适当的操作流程来检测伪造品、替换零件，合作或外包开发没有明确安全要求，第三方软件使用前没有进行安全检查等 |
| 供应阶段脆弱性 | 产品和服务在生产、集成、仓储、交付等供应阶段可能存在安全隐患，如：采购时无法识别被篡改或伪造的组件，生产环境的物理安全访问控制不严，采用了不可靠或不安全的仓储商，运输时产品被植入、篡改或替换，供应商未经授权私自预装程序等 |
| 运维阶段脆弱性 | 产品和服务在运维阶段可能存在安全隐患，如：产品返回维修时被植人、篡改或替换，缺乏对安全漏洞的应急响应能力，售后人员盗窃用户数据等供应链基础设施的脆弱性 |
| 供应链基础设施的脆弱性 | 供应链管理脆弱性 | 供应链安全管理缺乏或管理不严，可能存在安全隐患，如：未完全建立供应链安全管理制度和流程，缺乏供应链安全责任部门和人员，在选择供应商时未考虑网络安全要求，没有对供应商的绩效和安全风险进行定期评估，缺乏对外包项目、外包人员的安全规定等 |
| 供应链信息系统脆弱性 | 组织的供应链信息系统，可能存在安全隐患，如：未对供应商访问供应链相关信息进行访问控制，个人信息保护未满足相关法规标准要求，未对个人信息访问和使用进行控制，供应链信息不透明或阻塞，信息系统存在漏洞等 |
| 上下游脆弱性 | 供应链、供应商安全能力参差不齐，供应链整体安全水平不高，如：一些供应商的产品安全标准和供应链安全管理流程缺乏，也有的供应商不能及时发现安全缺陷并进行修复和响应等；由于上游供应商安全能力不足、产品市场被部分企业垄断、部分下游供应商安全检测能力有限、长期合作独家供应商造成依赖等原因，导致下游供应商难以控制和追溯上游的供应链风险 |
| 供应链物理安全脆弱性 | 厂房、仓库、数据中心、机房的位置，缺少抵御自然灾害或人为破坏等的能力 |

附录A.6（资料性附录）

电子信息企业供应链安全事件后果分类

参考文件“GB/T 38702-2020 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”后果基于以下因素考虑，包括：经济影响或合同违约、业务连续性、违规、人员伤亡、环境影响。

* 经济影响或合同违约：供应链安全事件造成公司经济方面的损失或不能满足与客户约定的产品交付要求
* 业务连续性：供应链安全事件对公司业务连续性造成的影响
* 违法法律法规或客户的要求：供应链安全事件导致公司违反相关法律法规（例如：保密法、垄断法）或客户除产品交付外的其他要求（例如：采购来源、信息安全等）

|  |  |
| --- | --- |
| **后果等级** | **后果** |
| **经济影响或合同违约** | **业务连续性** | **违反法律法规或客户要求** |
| **低** | 对公司经济方面的损失较小或不会造成公司违约 | 对公司的业务连续性基本没有影响 | **不会**导致公司违反相关法律法规或客户要求 |
| **中** | 对公司经济方面有一定损失或可能造成公司部分履约受阻 | 对公司业务连续性有一定影响 | **会**导致公司违反部分客户要求 |
| **高** | 对公司经济方面的损失很大或造成公司无法履约 | 造成公司业务中断 | **会**导致公司违反相关法律法规或客户要求 |

附录A.7（资料性附录）

电子信息企业供应链安全事件发生可能性分类

事件发生可能性分类：参考GB/T 24420-2009

注：因为不知道前面章节编写人员如何计算风险值及风险判定，因此暂时先分为5级。后续可以根据需要调整。

|  |  |
| --- | --- |
| 等级 | 可能性 |
| 1 | 不可能 |
| 2 | 不大可能 |
| 3 | 可能 |
| 4 | 非常可能 |
| 5 | 确定 |

附录A.8（资料性附录）

电子信息企业供应链安全风险处置模型



附录A.9（资料性附录）

电子信息企业供应链紧急情况清单

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 紧急情况类型 | 紧急情况概述 | 解决措施概述 | 备注 |
| 1 | 自然灾害 | 地震、洪水、台风等非可控自然灾害可能会影响供应链中的物流和生产，供应链可能会被中断或者受到影响。 | 应建立备用仓储设施和备用物流渠道，提前储备物资和备件，制定应急预案并进行常规化演练。 | 自然环境风险 |
| 2 | 突发事件 | 火灾、爆炸、恐怖袭击、人为因素等可能会对供应链造成影响 | 应加强安全管理，建立紧急联系机制，制定应急预案并进行演练。 | 政治风险 |
| 3 | 政治环境稳定性 | 政治稳定性的变化可能会影响供应链中的区域贸易和物流，政治环境的变化可能会影响某些国家或地区的供应链，例如贸易限制、关税税率的改变等。 | 应关注政治形势变化，加强全球、区域风险评估，寻找备用供应商和备用物流渠道。 | 政治风险 |
| 4 | 贸易争端 | 贸易争端可能导致关税上涨或限制贸易，从而影响供应链中的进口和出口 | 应开展多元化贸易，寻找备用供应商和备用物流渠道，加强与政府的沟通和合作。 | 政治风险经济风险 |
| 5 | 营商环境稳定性 | 区域营商环境优劣及变化情况对供应链会产生基础影响至严重影响 | ①应关注区域营商环境。②应加强与区域政府的沟通与合作。③应制定营商环境变化的应对措施及应急机制。 | 政治风险 |
| 6 | 卫生事件 | 疫情、病毒 | 应加强卫生防护，建立健全的疫情应对机制，制定应急预案并进行演练，寻找备用供应商和备用物流渠道。 | 自然风险政治风险经济风险 |
| 7 | 原材料供应中断（短缺） | 企业在生产过程中可能会面临原材料短缺的情况，导致生产停滞。 | ①应实行多元化供应链：通过提供多元化供应链，以便检索不同的原料来源，以克服因疫病情或其他非计划因素使单一来源受到影响所带来的供应问题。②应建立优化库存控制结构：建立库存地图和库存监控系统，以便定期地、实时地跟踪库存状况和需求趋势，确保有足够的库存足生产和交付需求。③应加强风险管理：电子信息企业应该建立更为完善的风险管理策略，以便预测潜在的损害和降低风险性。④应增加商业适应性：尽管主要依赖商业环境和市场需求侧，但企业可以采取对应措施来加速适应新的商业环境，例如通过引入技术或制度来改善流程和生产。⑤应协作灵活合作：与供应链中的供应商、物流公司、物料供应商和客户建立更加灵活和密切的伙伴关系，以在面临异常情况时能够更好地合作和互助。⑥应加强信息收集：及时了解政策变化、天气预报等信息，以便及时做调整。 | 供需合作风险 |
| 8 | 供应商不稳定 | 企业从不同的供应商采购组件内原材料或零部件，如果某一个或几个供应商突然无法按时供货，企业的生产线将受到影响。 | ①应实时监控供应商状况：定期监控供应商的经营状况，及时了解供应商的财务状况和供应能力，避免出现供应商不稳定供应的情况。②应建立供应链风险管理机制：建立和完善供应链风险管理机制，对供应商的风险进行评估，制定应对策略，提前做好准备。③应建立备用供应商：建立多个备用供应商，减少对某一供应商的依赖，以减轻供应商稳定性风险对企业带来的影响。 | 供需合作风险 |
| 9 | 物流运输 | 供应商提供的原材料或零部件需要通过物流渠道运输至企业，如果运输过程中发生了意外或者停滞，会对企业的生产造成影响。 | ①应确保仓库库存：保证仓库中的库存，避免因为物流延误导致缺料情况。②应实现多渠道物流：建立多渠道物流模式，采用多家物流公司或者不同方式的物流运输，以避免任何一种物流方式出现问题而影响企业的生产运营。③应建立时间冗余机制：制定合理的物流计划，事先预留一定的物流时间冗余，以便在物流延误出现的情况下，能够更好地应对。 | 信息流风险市场风险物流风险 |
| 10 | 阶段需求变化 | 市场需求有变化，导致某个产品或零部件的需求量增加或减少，企业需要及时调整生产线和采购计划。 | ①应加强市场预测和市场研究：加强市场预测和市场研究，尽可能提前了解市场变化趋势，及时预测市场需求变化。②应灵活生产：根据市场需求变化的情况，灵活生产，适时调整生产计划，保证生产运营的效率。③应实现供应链协同：与供应链各方建立紧密的协同合作，共同分享市场需求变化带来的挑战，共同制定应对策略，以应对市场需求变化。 | 市场风险需求风险 |
| 11 | 交付延误 | 由于运输和原材料供应方面的问题，电子信息企业无法按照承诺的时间交付产品，这可能导致严重的后果。 |  | 合作风险管理风险市场风险 |
| 12 | 订单取消 | 如果交付延误持续较长时间，购买方有可能选择取消订单，不仅会造成生产线的浪费，更可能会影响企业声誉。 |  | 合作风险管理风险市场风险 |
| 13 | 生产环节故障 | 生产环节突发故障会导致生产环节的停滞 | ①应定期维护和保养是预防生产环节故障的重要手段，可以定期维护设备，检查设备是否正常运行。②应保证备用设备就位：备用设备就位可以在生产环节突发故障时快速替换现有设备。在选择备用设备时，应该考虑设备的适应性、可用性和性价比等因素。③应制定应急预案：在生产环节故障发生时，可以根据应急预案快速启动相应的措施，以便保证生产环节的正常运转。 | 管理风险 |

|  |
| --- |
|  |
|  |

附录B（资料性附录）

电子信息企业供应链相关法律法规

1. 国务院办公厅关于积极推进供应链创新与应用的指导意见【国办发〔2017〕84号】
2. 国务院办公厅关于印发“十四五”现代物流发展规划的通知【国办发〔2022〕17号】
3. 八部门联合印发《关于规范发展供应链金融 支持供应链产业链稳定循环和优化升级的意见》【银发〔2020〕226号】
4. 商务部等8单位关于印发《全国供应链创新与应用示范创建工作规范》的通知【商流通函〔2022〕123号】
5. 商务部等8单位关于开展全国供应链创新与应用示范创建工作的通知（2021年03月30日）

附录C（资料性附录）

电子信息行业物料分类表

电子信息行业物料的分类方式采用大类+小类+物料描述的方式，共分为12个大类

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 物料大类 | 编号 | 物料小类 | 编号 | 描述（物理特性） | 备注 |
| 电阻 | 01 | 贴片-封装0201 | 01 | 0.6\*0.3\*0.23mm,0.05, 1/20W | 长\*宽\*高，精度，功率 |
| 贴片-封装0402 | 02 | 1\*0.5\*0.3mm,0.05, 1/16W |
| 贴片-封装0603 | 03 | 1.6\*0.8\*0.4mm,0.05, 1/16W |
| 贴片-封装0805 | 04 | 2\*1.25\*0.5mm,0.05, 1/10W |
| 贴片-封装1206 | 05 | 3.2\*1.6\*0.55mm,0.05, 1/8W |
| 贴片-封装2010 | 06 | 5\*2.5\*0.55mm,0.05, 1/2W |
| 贴片-封装2512 | 07 | 6.4\*3.2\*0.55mm,0.05, 1W |
| 插件-封装1/8W | 08 | AXIAL-0.3,7.6mm | 焊盘中心距-英寸距离，对应长度 |
| 插件-封装1/4W | 09 | AXIAL-0.4,10.2mm |
| 插件-封装1/2W | 10 | AXIAL-0.5,12.7mm |
| 插件-封装1W | 11 | AXIAL-0.6,15.2mm |
| 插件-封装2W | 12 | AXIAL-0.8,20.3mm |
| 插件-封装3W | 13 | AXIAL-1,25.4mm |
| 插件-封装5W | 14 | AXIAL-1.4,30.5mm |
| 插件-封装5W以上 | 15 | —— | —— |
| 压敏电阻 | 16 | —— | —— |
| 热敏电阻 | 17 | —— | —— |
| 电容 | 02 | 贴片-瓷片电容 | 01-05 | —— | —— |
| 贴片-电解电容 | 06 | —— | —— |
| 贴片-安规电容 | 07 | —— | —— |
| 插件-瓷片电容 | 10 | —— | —— |
| 插件-电解电容 | 11 | —— | —— |
| 插件-安规电容 | 12 | —— | —— |
| 插件-薄膜电容 | 13 | —— | —— |
| 电感 | 03 | 插件电感 | 01 | —— | —— |
| 滤波线圈 | 02 | —— | —— |
| 电抗器 | 03 | —— | —— |
| 电抗电感 | 10 | —— | —— |
| 集成电路 | 04 | 贴片IC | 01 | —— | —— |
| 插件IC | 11 | —— | —— |
| 印制板 | 05 | 单面板 | 01 | —— | —— |
| 双面板 | 02 | —— | —— |
| 多层板 | 03 | —— | —— |
| 线材 | 06 | 电力线 | 01 | —— | —— |
| 信号线 | 02 | —— | —— |
| 传感器 | 03 | —— | —— |
| 电缆 | 04 | —— | —— |
| 接插件 | 07 | 端子排 | 01 | —— | —— |
| 插头 | 02 | —— | —— |
| 插座 | 03 | —— | —— |
| 插片 | 04 | —— | —— |
| 插针 | 05 | —— | —— |
| 短接块 | 06 | —— | —— |
| 非标电子元器件 | 08 | 变压器 | 01 | —— | —— |
| 继电器 | 02 | —— | —— |
| 保险丝 | 03 | —— | —— |
| 二极管 | 04 | —— | —— |
| 三极管 | 05 | —— | —— |
| 可控硅 | 06 | —— | —— |
| 桥堆 | 07 | —— | —— |
| 功率模块 | 08 | —— | —— |
| 开关器件 | 09 | —— | —— |
| 互感器 | 10 | —— | —— |
| 放电管 | 11 | —— | —— |
| 晶振 | 12 | —— | —— |
| 跳线 | 13 | —— | —— |
| 垫高块 | 14 | —— | —— |
| 标准件 | 09 | 螺钉 | 01 | —— | —— |
| 螺母 | 02 | —— | —— |
| 弹垫 | 03 | —— | —— |
| 垫片 | 04 | —— | —— |
| 塑料柱 | 05 | —— | —— |
| 辅助材料 | 10 | 固定胶 | 01 | —— | —— |
| 三防漆 | 02 | —— | —— |
| 绝缘垫片 | 03 | —— | —— |
| 导热硅脂 | 04 | —— | —— |
| 热缩套管 | 05 | —— | —— |
| 胶水 | 06 | —— | —— |
| 胶带 | 07 | —— | —— |
| 双面胶 | 08 | —— | —— |
| 焊锡 | 09 | —— | —— |
| 包装件 | 11 | 纸箱 | 01 | —— | —— |
| 泡沫 | 02 | —— | —— |
| 气泡袋 | 03 | —— | —— |
| 捆扎带 | 04 | —— | —— |
| 印刷品 | 12 | 标贴 | 01 | —— | —— |

参考文献

[1] GB/T 19004 追求组织的持续成功 质量管理方法

[2] GB/T 19010 质量管理 顾客满意 组织行为规范指南

[3] GB/T 19012 质量管理 顾客满意 组织处理投诉指南

[4] GB/T 19013 质量管理 顾客满意 组织外部争议解决指南

[5] GB/Z 27907 质量管理 顾客满意 监视和测量指南

[6] GB/T 19015 质量管理体系 质量计划指南

[7] GB/T 19016 质量管理体系 项目质量管理指南

[8] GB/T 19017 质量管理体系 技术状态管理指南

[9] ISO 10008 Quality management-Customer satisfaction-Guidelines for business-to- consumer electronic commerce transactions

[10] GB/T 19022 测量管理体系 测量过程和测量设备的要求

[11] GB/T 19023 质量管理体系文件指南

[12] GB/T 19024 质量管理 实现财务和经济效益的指南

[13] GB/T 19025 质量管理 培训指南

[14] GB/Z 19027 GB/T 19001-2000的统计技术指南

[15] ISO 10018 Quality management—Guidelines on people involvement and competence

[16] GB/T 19029 质量管理体系咨询师的选择及其服务使用的指南

[17] GB/T 24001 环境管理体系要求及使用指南

[18] GB/T 19011 管理体系审核指南

[19] ISO 31000 Risk management-Principles and guidelines

[20] ISO 37500 Guidance on outsourcing

[21] ISO/IEC 90003 Software engineering一Guidelines for the application of ISO 9001： 2008 to computer software

[22] IEC 60300-1 Dependability management—Part 1 ：Guidance for management and application

[23] IEC 61160 Design review

[24] Quality management principles

[25] Selection and use of the. ISO 9000 family of standards

[26] ISO 9001 for Small Businesses—What to do

[27] Integrated use of management system standards

[28] [www.iso.org/tcl76/sc02/public](http://www.iso.org/tcl76/sc02/public)

[29] [www.iso.org/tcl76/ISO](http://www.iso.org/tcl76/ISO) 9001 AuditingPracticsGroup

[30] GB/T2882.2 信息技术服务 运行维护 第二部分 交付规范

[31] GB/T 11457 信息技术 软件工程术语

[32] ISO/IEC20000-1 信息技术 服务管理 服务管理体系要求

[33] GB/T22080 信息技术 安全技术 信息安全管理体系要求

[34]中电联字（2015）1号 信息系统集成及服务资质认定管理办法（暂行）

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_