

中华人民共和国国家标准

GB/T 43698—2024

网络安全技术 软件供应链安全要求

Cybersecurity technology—Security requirements for software supply chain

2024-04-25发布

2024-11-01 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 I

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 软件供应链安全目标 2

5 软件供应链安全保护框架 2

6 软件供应链安全风险管理要求 3

 6.1 基本流程 3

 6.2 软件供应链安全图谱 3

 6.3 软件供应链安全风险评估 4

 6.4 软件供应链安全风险处置 4

7 需方安全要求 4

 7.1 组织管理 4

 7.2 供应活动管理 5

8 供方安全要求 7

 8.1 组织管理 7

 8.2 供应活动管理 8

附录 A（资料性） 软件供应链安全概述 11

附录 B（资料性） 关键软件资产 15

附录 C（资料性） 组织业务场景分类 16

附录 D（资料性） 软件供应链安全图谱 17

参考文献 19

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。

本文件由全国网络安全标准化技术委员会(SAC/TC 260)提出并归口。

本文件起草单位：中国信息安全测评中心、中国电子技术标准化研究院、华为技术有限公司、国家计算机网络应急技术处理协调中心、中国软件评测中心(工业和信息化部软件与集成电路促进中心)、诺基亚通信系统技术(北京)公司、奇安信网神信息技术(北京)股份有限公司、深信服科技股份有限公司、国网新疆电力有限公司电力科学研究院、麒麟软件有限公司、国家信息技术安全研究中心、国家计算机网络应急技术处理协调中心黑龙江分中心、深圳开源互联网安全技术有限公司、昆仑数智科技有限责任公司、联想(北京)有限公司、浪潮电子信息产业股份有限公司、中国网络安全审查技术与认证中心、杭州默安科技有限公司、北京天融信网络安全技术有限公司、三六零数字安全科技集团有限公司、长扬科技(北京)有限公司、上海观安信息技术股份有限公司、北京奇虎科技有限公司、北京快手科技有限公司、云从科技集团股份有限公司、国网区块链科技(北京)有限公司、国家计算机网络应急技术处理协调中心北京分中心、上海三零卫士信息安全有限公司、北京大学、启明星辰信息技术集团股份有限公司、瀚高基础软件股份有限公司、北京威努特技术有限公司、蚂蚁科技集团股份有限公司、中国信息通信研究院、中电长城网际安全技术研究院(北京)有限公司、北京安普诺信息技术有限公司、杭州安恒信息技术股份有限公司、北京神州绿盟科技有限公司、北京中科微澜科技有限公司、OPPO 广东移动通信有限公司、公安部第一研究所、中国科学院软件研究所、阿里云计算有限公司、湖南泛联新安信息科技有限公司、北京中测安华科技有限公司、中国科学院信息工程研究所、苏州棱镜七彩信息科技有限公司、新华三技术有限公司、工业和信息化部电子第五研究所、北京源堡科技有限公司、北京人大金仓信息技术股份有限公司、上海大学、西安邮电大学、沈阳东软系统集成工程有限公司、中国电子科技集团公司第十五研究所、远江盛邦(北京)网络安全科技股份有限公司、上海文鰐信息科技有限公司。

本文件主要起草人：李守鹏、王欣、王晓萌、王惠莅、薛勇波、吴润浦、林星辰、曾晋、上官晓丽、王嘉捷、万振华、陈冬青、沈蕾、辛伟、唐福宇、董国伟、常远、崔静、叶润国、高金萍、杨慧婷、吴倩、翟艳芬、董军平、王颀、张屹、滕征岑、邱林海、邓辉、郑明、李汝鑫、谢江、张大江、刘磊、梁利、陈靓、廖毅、柴思跃、宋桂香、申永波、孟瑾、白晓媛、孔耀晖、沈锡镛、杨剑、孙世国、李娜、王聪、赵华、韩煜、落红卫、武延军、张亚京、李军、张立、王栋、温婷婷、陈亮、查海平、高庆、姚叶鹏、赵军凯、冯明冉、王春霞、刘健、李汪蔚、林飞、宁戈、张涛、袁明坤、杨廷锋、王琦、王玮琪、杨牧天、李跃、李腾、万娟、吴敬征、王振远、刘井强、肖扬、梁大功、万晓兰、蔡一兵、梁露露、赵晓晖、彭晨、杨毅、张勇、冯全宝、程岩、聂万泉、付艳艳、霍珊珊、刘洋、王晶、权晓文、周浩威。

网络安全技术 软件供应链安全要求

1 范围

本文件确立了软件供应链安全目标，规定了软件供应链安全风险管理和供需双方的组织管理和供应活动管理安全要求。

本文件适用于指导软件供应链中的供需双方开展风险管理、组织管理和供应活动管理，为第三方机构开展软件供应链安全检测和评估提供依据，供主管监管部门参考使用。

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 25069—2022 信息安全技术 术语
- GB/T 36637—2018 信息安全技术 ICT 供应链安全风险管理体系指南

3 术语和定义

GB/T 25069—2022 和 GB/T 36637—2018 界定的以及下列术语和定义适用于本文件。

3.1

软件产品 software product

计算机软件、信息系统或设备中嵌入的软件或在提供计算机信息系统集成、应用服务等技术服务时提供的计算机软件。

注1: 软件产品包含计算机程序代码、规程、相关数据、文档和相关服务。

注2: 本文件中软件产品简称为软件。

[来源: GB/T36475—2018, 3.1.1, 有修改]

3.2

软件产品信息 software product information

软件产品版本、标识、来源、授权以及关联软件等信息的总称。

3.3

需方 acquirer

从其他组织获取软件产品的组织。

注: 本文件中需方指软件产品的购买者和使用者。

[来源: GB/T36637—2018, 3.1, 有修改]

3.4

供方 supplier

开展软件产品开发、交付、运维、废止等生命周期活动的组织。

注1: 本文件中供方指需方的第一级(直接)供应商; 此外, 还包括软件产品的开发商、各级销售和代理商、系统集成商, 也包括软件或应用商店、代码托管平台、第三方下载站点以及基于开源代码提供软件产品的组织等。

注2: 开放源代码社区本身不是供方。

注3:供方与需方共同决定软件产品的生命周期结束时间。

3.5

供应关系 supplier relation

需方(3.3)和供方(3.4)之间为开展业务、提供软件产品而建立的协议、合同等契约关系。

注:在供应链中,上游的需方同时也是下游的供方。

[来源:GB/T36637—2018,3.3,有修改]

3.6

供应活动 supply activity

需方(3.3)和供方(3.4)为维持日常生产基于供应关系(3.5)进行的软件采购、开发、获取、交付、运维、废止等活动的总称。

3.7

软件供应链 software supply chain

需方和供方基于供应关系(3.5),开展并完成软件采购、开发、交付、获取、运维和废止等供应活动而形成的网链结构。

[来源:GB/T 36637—2018,3.4,有修改]

3.8

软件物料清单 software bill of materials

软件产品中所包含的所有组件、相关许可协议的清单,以及所有组件之间依赖关系的描述。

3.9

软件供应链安全图谱 software supply chain security graph

软件产品信息(3.2)、软件物料清单(3.8)、安全信息等内容及其关联关系的描述和表示。

注:一般以文本形式存储,支持通过知识图谱方式展示。

3.10

开放源代码社区 open source community

用于开源代码和数据开发、维护的一种工程组织和运作方式。

注:开放源代码社区也称开源社区或开源代码社区。

3.11

外部组件 external component

由供方以外的组织或人员开发的程序代码、文档或数据,通常是由二进制程序文件或者源代码程序文件构成。

注:外部组件包括软件中使用的开源组件和第三方组件。

4 软件供应链安全目标

软件供应链安全目标是建立软件供应链安全风险管理体系并持续改进,增强软件供应链安全风险、组织管理和供应活动管理能力,防范软件供应链中的供应关系风险(例如:软件供应中断、软件功能受限、软件服务降级等),防范供应活动引入的技术安全风险和知识产权风险(例如:软件漏洞、后门、篡改、伪造、许可协议不合规等),保障业务持续稳定安全运行。

5 软件供应链安全保护框架

基于软件供应链模型、软件供应链实体角色分析和软件供应链安全构成(见附录 A),确立了软件供应链安全保护框架。该框架规定了供需双方(即“组织”)的软件供应链安全风险、组织管

理和供应活动两个方面规定了需方安全要求和供方安全要求，如图1所示。

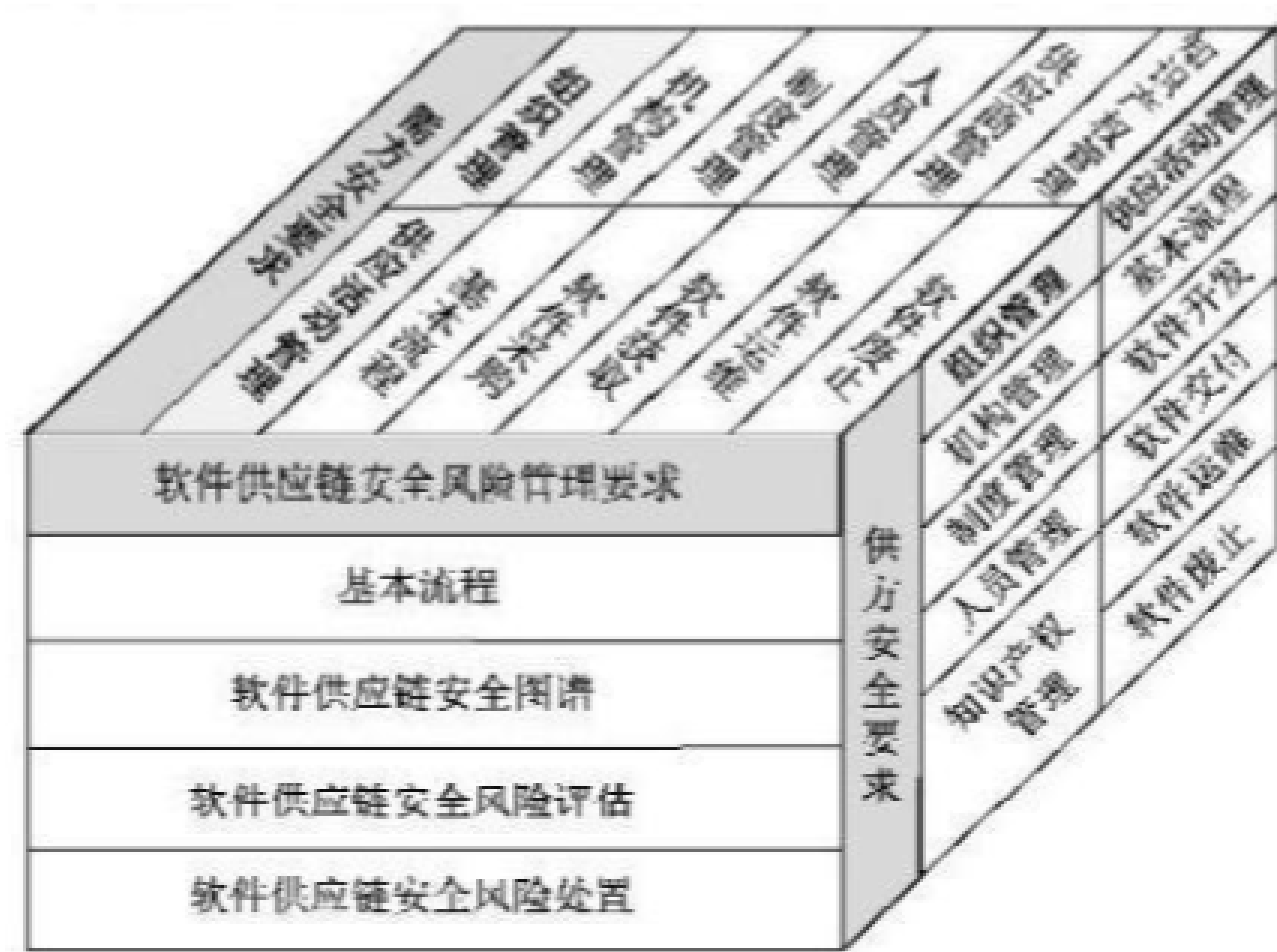


图 1 软件供应链安全保护框架

6 软件供应链安全风险管理要求

6.1 基本流程

基本流程对组织要求如下。

- a) 应确定软件供应链风险管理的目标及策略，按照第7章、第8章安全要求建设软件供应链组织管理和供应活动管理能力。
- b) 应识别软件资产，梳理一般软件资产和关键软件资产(见附录 B)，按照6.2的要求构建软件供应链安全图谱。
- c) 应确定软件供应链风险管理的对象、范围和边界，包括但不限于软件、环境及工具、外部组件等。
- d) 应依据软件供应链安全图谱等建立组织管理、供应活动管理等方面的供应链安全信息采集和跟踪机制。
- e) 应定期或基于安全需求开展软件供应链安全检测和风险评估，依据上述结论采取相应的供应链风险防范、风险缓解或风险消除措施。
- f) 应定期或根据实际业务需要开展软件供应链安全要求执行情况的监督检查，研判 a)~e) 的有效性，并根据研判结果进行调整。

6.2 软件供应链安全图谱

软件供应链安全图谱对组织要求如下。

- a) 应根据不同类别的业务场景(见附录 C)确定软件供应链安全图谱的等级，并清晰准确地构建软件供应链安全图谱(见附录 D):
 - 1) 一般业务场景中构建的软件供应链安全图谱，应至少包含软件产品信息；
 - 2) 重要业务场景中构建的软件供应链安全图谱，应包含1)中信息以及软件来源信息、软件组件成分信息、组件漏洞信息、合规信息等；
 - 3) 核心业务场景中构建的软件供应链安全图谱，应至少包含2)中信息，宜包含软件部署和运行所依赖的其他软件产品信息。
- b) 应定期(至少每年一次)或软件发生重要更新时，及时更新维护软件供应链安全图谱。
- c) 应将软件供应链安全图谱作为重要资产管理，采取相应安全保护措施，防止软件供应链安全图

谱泄露。

6.3 软件供应链安全风险评估

软件供应链安全风险评估对组织要求如下。

- a) 应按照GB/T36637—2018 中6.3风险评估流程，定期开展软件供应链安全风险评估，识别现有或预计产生的组织管理和供应活动管理相关的安全风险，重点关注以下安全风险：
 - 1) 发行版本或升级补丁停止交付或部署；
 - 2) 供方提供的服务部分或完全中断；
 - 3) 激活等软件授权措施受影响导致软件功能降级或服务能力受限；
 - 4) 供应活动在软件中引入的安全风险破坏发行版本或升级补丁的完整性、安全性和合规性。
- b) 应对a)的影响进行研判，至少对如下问题做出明确结论：
 - 1) 是否会影响到现有系统的正常安全运行，以及影响范围的大小；
 - 2) 是否会影响到现有系统的日常维护工作，如：故障排查、故障部件更换、安全事件处置等；
 - 3) 是否会影响到系统的重新部署、备份、迁移、升级、扩容等工作。

6.4 软件供应链安全风险处置

需方应满足第7章安全要求，供方应满足第8章要求，以防范6.3a)中的安全风险或缓解6.3b)中的影响。

7 需方安全要求

7.1 组织管理

7.1.1 机构管理

机构管理对需方要求如下。

- a) 应明确软件供应链安全管理组织机构或人员及其职责范围，提供保障软件供应链安全所需的资源(如有关资金、场地、人力等),并在预算管理过程中予以重点考虑。
- b) 应组织构建并管理软件供应链安全图谱，定期(至少每年一次)开展软件供应链安全检测、风险评估等软件供应链安全风险管理工作，包括但不限于软件成分分析、源代码和二进制代码安全漏洞分析和6.3等。
- c) 应及时制定、修订、宣贯、执行各项软件供应链安全管理制度、流程以及机制。
- d) 对于重要或核心业务场景，宜设立专职软件供应链管理机构开展软件供应链安全管理工作。

7.1.2 制度管理

制度管理对需方要求如下。

- a) 应确定软件供应链安全的总体方针、安全制度和策略(可作为单独的文件，也可作为相关文件中的一部分),至少包括软件资产管理、软件供应链安全风险识别处置、监督检查等内容。
- b) 应制定软件供应链安全风险持续监测、风险评估和事件响应制度，明确不同等级安全事件的报告、处置、响应的流程和机制，规定安全事件的现场处理、事件报告和后期恢复等要求。
- c) 应制定软件采购、获取、运维、废止等供应活动安全管理制度，例如安全开发、交付部署和验收、故障处理和升级维护等管理制度、规程或机制。
- d) 应将软件供应链安全相关内容纳入人员管理制度，例如人员权限、能力、资质、背景、技能培训等；对于重要岗位人员(如采购人员、安全测试人员、配置管理人员、漏洞管理人员等)应明确

并开展背景审查工作的要求。

- e) 应制定供应商管理制度，包括但不限于供应商资质审核、供应商分类分级、供应商不良行为处理等。
- f) 应制定知识产权管理制度，包括但不限于软件授权证书、专利、软件著作权、许可协议等内容。

7.1.3 人员管理

人员管理对需方要求如下。

- a) 应明确人员需具备的软件供应链实体要素的识别和安全分析能力，如软件资产识别分析、软件漏洞挖掘、后门检测、访问控制管理、完整性保护等。
- b) 应划分人员的职责定位、权限级别，采用最小授权机制并建立操作规范，创建操作日志。
- c) 应定期(至少每年一次)开展软件供应链安全和保密培训，培训内容包括但不限于a)和b)中涉及的内容。
- d) 应建立并执行离职离岗人员账号、权限、材料的交接和清理机制和规程。
- e) 对于核心业务场景，宜配置软件供应链安全保障团队，并根据需要开展相关人员的背景调查。
- f) 对于核心业务场景，宜具备防范各类软件供应链安全风险能力，例如软件供应链恢复、未知安全漏洞分析、软件持续供应能力分析等。

7.1.4 供应商管理

供应商管理对需方要求如下。

- a) 应分类分级建立合格的供应目录，对供应目录及相关信息进行集中管理，并定期或按照实际需求进行更新维护。
- b) 应优先选择供应目录中满足条件的供应商。
- c) 根据软件供应链中供应关系、供应活动的不同，供应商应符合8.2的安全要求。
- d) 应制定供应商选择策略和制度，对供应商进行风险分析，包括但不限于背景、资质、能力以及能否持续安全提供产品或服务等方面的风险。
- e) 应要求供方开展软件供应链安全检测和风险评估工作，明确相关内容和范围；确需第三方机构的，应明确对第三方机构的能力、资质等要求。
- f) 应要求供方配合相关部门开展软件供应链安全审查、监督和检查。
- g) 应在供应关系、供应商股权等信息发生变更时，对变更带来的安全风险进行评估，并采取相应的风险控制措施。
- h) 应建立供应商替代方案或具备相应软件的自主维护能力，防范软件供应链中断风险。

7.1.5 知识产权管理

知识产权管理对需方要求如下。

- a) 应防止因知识产权问题导致的法律风险，或具备防范相应法律风险的能力和机制。
- b) 应充分熟悉所使用或在研软件产品和服务的知识产权，对知识产权进行规范管理，防止侵权。
- c) 在核心业务场景中，宜对所使用的软件产品或服务相关的国内外知识产权情况进行详细识别分析，建立相关知识产权风险的应对方案。

7.2 供应活动管理

7.2.1 基本流程

基本流程对需方要求如下。

- a) 应在开展供应活动前，以协议、合同等方式与供方建立供应关系。
- b) 应在协议、合同等文件中明确对供应活动的安全要求，并签署相应的保密协议。
- c) 应按照约定的内容和范围开展软件供应活动管理。

7.2.2 软件采购

软件采购对需方要求如下。

- a) 应邀请软件供应链安全、网络空间安全等领域专家(或具备相应网络空间安全能力的评标人员)参与招标采购过程。
- b) 应结合软件应用的实际业务场景，明确对软件供应链安全图谱的要求；需要供方提供软件供应链安全图谱的应明确图谱的内容，如安全图谱的等级、可追溯层级等。
- c) 应根据国家和行业已发布标准以及自身业务要求制定软件的安全需求基线和防护架构，如软件应具备的安全防护能力、保护个人信息和重要数据等不被泄露的能力。
- d) 应确定所采购软件的授权使用期限及相应的技术协助要求，在授权方式可选的条件下，明确软件的激活、授权需求，优先选择离线永久激活模式，其次是完全在国内线上永久激活，再次是完全在国内实现的周期性线上激活、国外线上激活(永久或周期性)。
- e) 应制定从多个源厂商获得兼容的产品和服务的方案，确保软件来源的多样性。对于单一来源的软件，应制定风险消减措施。
- f) 对于定制研发软件，应要求供方具备安全开发相关资质或建立安全开发规范，建立和维护安全的开发环境、建立工具和设备的的安全管理和准入控制等。
- g) 应要求供方提供验证产品是否来自原厂商且获得许可的途径或方法。
- h) 应明确对运维技术团队及相应技术能力的要求，包括但不限于风险监测识别、漏洞修复、完整性保护、安全测试等。
- i) 应要求软件开发、交付、部署、测试等工具和设备具备可操作的替代方案。
- j) 应考虑政治、外交、贸易、自然灾害、公共安全事件等不可抗力导致供应中断时的可替代策略。
- k) 应明确软件供应链安全检测和风险评估的范围，例如软件资产识别、源代码和二进制代码安全漏洞分析、软件成分分析等；涉及第三方机构的应明确第三方机构的资质能力。

7.2.3 软件获取

软件获取对需方要求如下。

- a) 应对软件进行端到端的完整性验证。
- b) 应对所获取软件进行全面安全检测和风险评估，例如源代码安全漏洞分析、二进制代码安全漏洞分析、容器镜像安全分析、软件成分分析和6.3等，确保所获取软件符合约定的安全要求。
- c) 应确保获取的软件不存在已公开漏洞未修复的情况；对于存在已公开漏洞未修复的，应要求供方及时修复或采取相应缓解措施，并提供漏洞处置报告。
- d) 对于定制研发软件，宜掌握关键软件、组件的代码结构和技术原理；对于需要二次开发、独立维护的应获取软件源代码和相关知识产权的授权，并妥善保管。
- e) 对于定制研发软件，应要求厂商提供软件相关技术资料，包括但不限于中文版运行维护、二次开发、软件使用的场景和条件、权限和授权机制，软件使用说明书、技术分析报告等技术资料。
注1:技术分析报告包括但不限于源代码、二进制代码、组件等供应链安全分析报告。
注2:软件技术资料中设置声明条款，说明采购第三方软件、开源限制性、知识产权等情况。

7.2.4 软件运维

软件运维对需方要求如下。

- a) 应确定运维方案，包括运维团队、运维内容和范围、运维流程等内容。
- b) 应确保软件及运行环境持续稳定可用，保障软件完整性和访问控制策略正常。
- c) 应建立可追溯台账，对软件产品或服务整个使用过程进行记录、检测和维护，及时更新维护软件供应链安全图谱。
- d) 应将软件作为组织资产进行管理，保障软件安装、升级维护时从安全可控的渠道获取软件安装包、升级包、补丁包，并开展相应的可用性、安全性及完整性检测分析，在确保符合要求后进行软件安装、更新升级，并同步更新相关配置。
- e) 应在约定的环境中使用软件，对软件及其运行环境进行安全配置，并记录相关信息。
- f) 应明确运维人员的访问权限级别，对其访问范围和授权期限进行严格区分，确定不同权限人员尤其是厂商、外包等非自有维护人员，开展软件运维的内容和边界。
- g) 应对授权期限进行管理，禁止使用超过授权使用期限或维保期限的软件；确需使用的应定期评估并处置其安全风险。
- h) 应对软件运维工具、运维环境等进行安全检测和风险评估，及时发现并处置软件中断供应、停止授权、停止提供产品升级等供应关系风险，漏洞、后门等技术安全风险以及知识产权风险。
- i) 应收集软件供应链的安全风险信息，发现安全缺陷、漏洞等风险时，应当立即采取补救措施，并按照规定及时向有关主管监管部门报告。
- j) 应依据实际业务场景的业务连续性和灾难恢复计划，制定可接受的恢复时间和恢复目标，并确定防范供应中断和服务中断等风险的安全策略。
- k) 应开展软件供应链相关范围内的数据安全检测分析和风险评估等工作，防止因软件漏洞引起的信息泄露、数据泄露、篡改和损毁等安全事件发生。
- l) 应对软件外联网络地址、域名数据等进行检测和分析，及时发现产品后门植入、擅自提高权限等违规操作。

7.2.5 软件废止

软件废止对需方要求如下。

- a) 应制定软件废止处理规程，例如软件停用和卸载、软件供应链安全图谱归档、信任关系清除以及数据备份、迁移和销毁等，并按照规程开展相应工作。
- b) 应移除准入控制措施和策略中与所废止软件相关的信息，例如软件、人员、设备等要求和规则；对于不适合清除的应制定相应的控制措施和策略。
- c) 应具备软件废止后防止软件泄露、数据泄露的安全保障能力。
- d) 对于软件产品废止并替换为新产品的，应要求新产品的供方支持数据迁移到新的软件产品。
- e) 涉及数据销毁的，宜参照GB/T37988—2019 中第11章的要求进行数据销毁、防止对存储的数据进行修复而导致的数据泄露风险。
- f) 废止工作完成后应进行安全检测，确保除例外的要求和规则外，软件及其相关信息被完全废止，

8 供方安全要求

8.1 组织管理

8.1.1 机构管理

机构管理对供方要求如下。

- a) 应明确软件供应链安全管理组织机构或人员及其职责范围，提供保障软件供应链安全所需的

资源(如有关资金、场地、人力等),并在预算管理过程中予以重点考虑。

- b) 应组织构建并管理软件供应链安全图谱,定期(至少每年一次)开展软件供应链安全检测、风险评估等软件供应链安全风险管理工作,包括但不限于软件成分分析、源代码和二进制代码安全检测和6.3等。
- c) 应及时制定、修订、宣贯、执行各项软件供应链安全管理制度、流程以及机制。

8.1.2 制度管理

制度管理对供方要求如下。

- a) 应确定软件供应链安全的总体方针、安全制度和策略(可作为单独的文件,也可作为相关文件中的一部分),至少包括软件资产管理、软件供应链安全风险识别、处置、监督检查等内容。
- b) 应制定软件供应链安全风险的持续监测、风险评估和事件响应制度,并明确不同等级安全事件的报告、处置、响应的流程和机制,规定安全事件的现场处理、事件报告和后期恢复等要求。
- c) 应制定软件开发、交付、运维、废止等供应活动的安全管理制度,例如安全开发、交付部署和验收、故障处理和维护升级等管理制度、规程或机制。
- d) 应将软件供应链安全相关内容纳入人员管理制度,例如人员权限、能力、资质、背景、技能培训等内容;对于重要岗位人员(如安全测试人员、配置管理人员、漏洞管理人员等)应明确并开展背景审查工作的要求。
- e) 应制定知识产权管理制度,包括但不限于软件授权证书、专利、软件著作权、许可协议等内容。

8.1.3 人员管理

人员管理对供方要求如下。

- a) 应明确人员需具备的软件供应链实体要素的识别和安全分析能力,例如软件资产识别分析、软件漏洞挖掘、后门检测、访问控制管理、完整性保护等。
- b) 应划分人员的职责定位、权限级别,采用最小授权机制并建立操作规范,创建操作日志。
- c) 应具备防范各类软件供应链安全风险能力,如软件供应链恢复、未知安全漏洞分析、软件持续供应能力分析等。
- d) 应定期(至少每年一次)开展软件供应链安全和保密培训,培训内容包括但不限于a)~c)中涉及的内容。
- e) 应建立并执行离职离岗人员的账号、权限、材料等交接、清理的机制和规程。

8.1.4 知识产权管理

知识产权管理对供方要求如下。

- a) 应防止因知识产权问题导致的法律风险,或具备防范相应法律风险的能力和机制。
- b) 应充分熟悉所提供软件的知识产权,对知识产权进行规范管理,防止侵权。

8.2 供应活动管理

8.2.1 基本流程

基本流程对供方要求如下。

- a) 应在开展供应活动前以协议、合同等方式与需方建立供应关系。
- b) 应在协议、合同等文件中明确对供应活动的安全要求,并签署相应的保密协议。
- c) 应按照约定的内容和范围开展软件供应活动管理。

8.2.2 软件开发

软件开发对供方要求如下。

- a) 参照GB/T30998—2014 的第6章开展软件开发的安全保障分析，或具备安全开发资质，例如信息安全服务资质(安全开发类)、软件安全开发服务资质等。
- b) 应将软件作为组织资产进行管理，制定和实施防盗版的策略和规程，开发过程中对文件、组件、开发工具等采取访问控制、完整性保护等安全机制。
- c) 应构建软件供应链安全图谱，记录软件产品信息、软件物料清单、安全漏洞等信息，并保障其完备性和准确性。
- d) 应基于软件供应链安全图谱，建立和维护可追溯性的策略和程序，记录和保留外部组件的原始供应方、开源社区或开发贡献者等相关信息，可追溯至上游供应商。
- e) 应确定软件的安全需求基线和防护架构，保障软件具备安全防护、保护个人信息和重要数据不被泄露等能力。
- f) 应承诺所使用的外部组件不存在已公开漏洞未修复的情况；对于存在已公开漏洞未修复的，应及时修复漏洞，或采取缓解防御措施，或提供漏洞分析和处置报告。
- g) 应建立外部组件的使用审批机制，对来源于开放源代码社区和第三方的代码、组件和软件进行完整性验证、安全检测和依赖关系分析，并对开源代码进行安全评价；建立自有的开源和第三方组件库，并标明使用等级(如优选、可选、限选、禁选等)，保障外部组件来源可靠、安全风险可消除或控制。
- h) 应持续跟踪所使用的工具、外部组件的使用状态、安全状态；对于存在安全风险的，应及时通报，并及时采取更新、修复等措施，完善软件供应链安全图谱信息；对于缺乏维护或即将废止的组件应采取停用、废止等处置措施。
- i) 对于难以验证来源的工具、外部组件，应禁止使用；确需使用的应醒目标注，说明原因，通过安全检测和风险评估后方可使用。
- j) 应建立安全可控的软件开发工作场所，搭建并使用专用的开发环境；涉及多个开发环境的应进行必要的逻辑隔离。
- k) 应建立开发/测试工具和设备白名单，采用安全检测、正版授权验证、官方完整性校验等措施进行白名单准入控制，保障核心开发工具、核心组件有可替代方案或自主可控。
- l) 应选择供需双方约定的方式开展软件供应链安全检测和风险评估工作，例如源代码安全检测、二进制代码安全检测、软件成分分析、知识产权分析、数据安全能力成熟度分析等。

8.2.3 软件交付

软件交付对供方要求如下。

- a) 应确保交付软件的真实性、准确性、完整性，采取措施保护信息不被篡改和泄露，并提供所交付软件的完整性验证措施或方法。
- b) 应按约定方式对交付软件实行安全部署和配置，提供部署方法、安全配置基线和软件供应链安全图谱等信息。
- c) 应承诺所交付软件不存在已公开漏洞未修复的情况；对于存在已公开漏洞未修复的，应及时采取缓解措施，并提供漏洞处置报告。
- d) 应配合开展所交付软件的功能、性能、完整性及安全性等验收测试并对软件进行数字签名，开展包括但不限于供应关系、供应活动的安全检测和风险评估，以及可持续供应能力、安全漏洞等安全检测和风险评估，确保符合约定的安全要求。
- e) 对于所交付软件，应禁止交付约定范围外的内容，如开启无关功能、捆绑无关软件等，并承诺不

在软件中设置后门，或利用软件的便利条件非法获取用户数据、控制和操纵用户系统和设备，不会利用软件的依赖性谋取不正当利益，不在未授权情况下对软件进行升级或更新换代；对于约定的远程访问控制措施，应采取必要技术手段和管理措施确保远程控制过程的安全性。

- f) 应及时提供交付环节变化的通报，以及相关的交付途径安全性分析报告，并对可能造成严重后果的变化，快速采取补救措施。
- g) 应交付需方购买软件的使用授权，例如许可证、产品序列号、许可协议等。
- h) 应保障所交付软件使用的外部组件获取途径安全性、自身安全性、组件可持续服务等，提供与软件一致的质量、安全、服务承诺，并按照协议提供承诺、说明、认证证明、分析报告、资质证明等相关材料。
- i) 对)于定制研发软件，应交付包括但不限于软件源代码，中文版运行维护、二次开发、软件使用的场景和条件、权限和授权机制，以及软件使用说明书、技术分析报告等技术资料。
注1:技术分析报告包括但不限于源代码、二进制代码、组件等供应链安全分析报告。
注2:软件技术资料中设置声明条款，说明采购第三方软件、开源限制性、知识产权等情况。
- j) 对于定制研发或者自主研发软件，应妥善保管 i) 中的内容，并依据相关规定或合同文件，不将软件全部或部分泄露到授权以外的范围，并签署保密协议。
- k) 应对软件分包、集成等工作的安全负责。
- l) 应开展全面的软件供应链安全检测，例如源代码安全检测、二进制代码安全检测和容器镜像安全检测等，缓解或消除软件供应链安全风险。

8.2.4 软件运维

软件运维对供方要求如下。

- a) 应确保软件在授权期内持续稳定可用，保障软件完整性和访问控制策略正常。
- b) 应协调软件原厂、供应商、集成商等共同开展软件运维工作。
- c) 应建立并维护可追溯台账，及时更新维护软件供应链安全图谱信息。
- d) 应识别授权即将到期或超过授权、维保期限仍在使用的软件，定期开展安全风险检测和风险评估，及时向需方发送风险提醒，并协助处置发现的安全风险。
- e) 应定期(至少每年一次)开展软件供应链安全检测和风险评估，例如软件本身、运维工具、运维环境、软件外联网络地址、域名以及数据安全等安全检测和风险评估，及时发现并处置软件中断供应、停止授权、停止提供产品升级等持续供应风险，漏洞、后门以及数据泄露、篡改和损毁、信息泄露、擅自提高权限等安全风险，并按照有关规定向相关部门报告。
- f) 应在生产地、注册地所在国家或地区出现因政治、外交、贸易、自然灾害、公共安全事件等不可抗力导致供应中断时，及时采取应对措施，或在需方采用替代方案时积极给予协助。
- g) 应禁止向未授权者提供运维相关数据，或将相关数据用于运维以外的目的。
- h) 应明确软件供应链运维人员对软件供应链的访问权限，确定不同权限人员开展软件运维的内容和边界。

8.2.5 软件废止

软件废止对供方要求如下。

- a) 应协助需方开展软件卸载、停用及数据备份、迁移、销毁等工作。
- b) 应具备防止软件泄露、数据泄露的安全保障能力。
- c) 对于软件废止并替换为新软件的，新软件应采取如下措施支持数据迁移到新的软件：
 - 1) 制定软件数据迁移计划，并确保数据安全迁移；
 - 2) 在数据迁移完成后，对废止软件进行数据清除和卸载，对废止软件进行安全处理。

附录 A
(资料性)
软件供应链安全概述

A.1 软件供应链模型

软件供应链是一种由供应关系、供应活动构成的网链结构。软件供应链至少包含一层供应关系，一种实体可以有多种角色。以软件采购为例，当需方直接从软件开发厂商采购软件时，供应链中包含开发商(供方)和采购商(需方)两种实体角色，此时软件供应链仅包含一层供应关系；当需方采购定制研发软件产品时，定制过程中需外包或采购部分功能模块，此时软件供应链可能存在多层供应关系，外包方(供方)和定制开发方(需方)、定制开发方(供方)和软件采购方(需方)，定制开发方具备了供方和需方两种角色；软件供应链中最细粒度的供应关系仅包含一层供应关系。软件供应链模型示意图如图 A.1 所示。

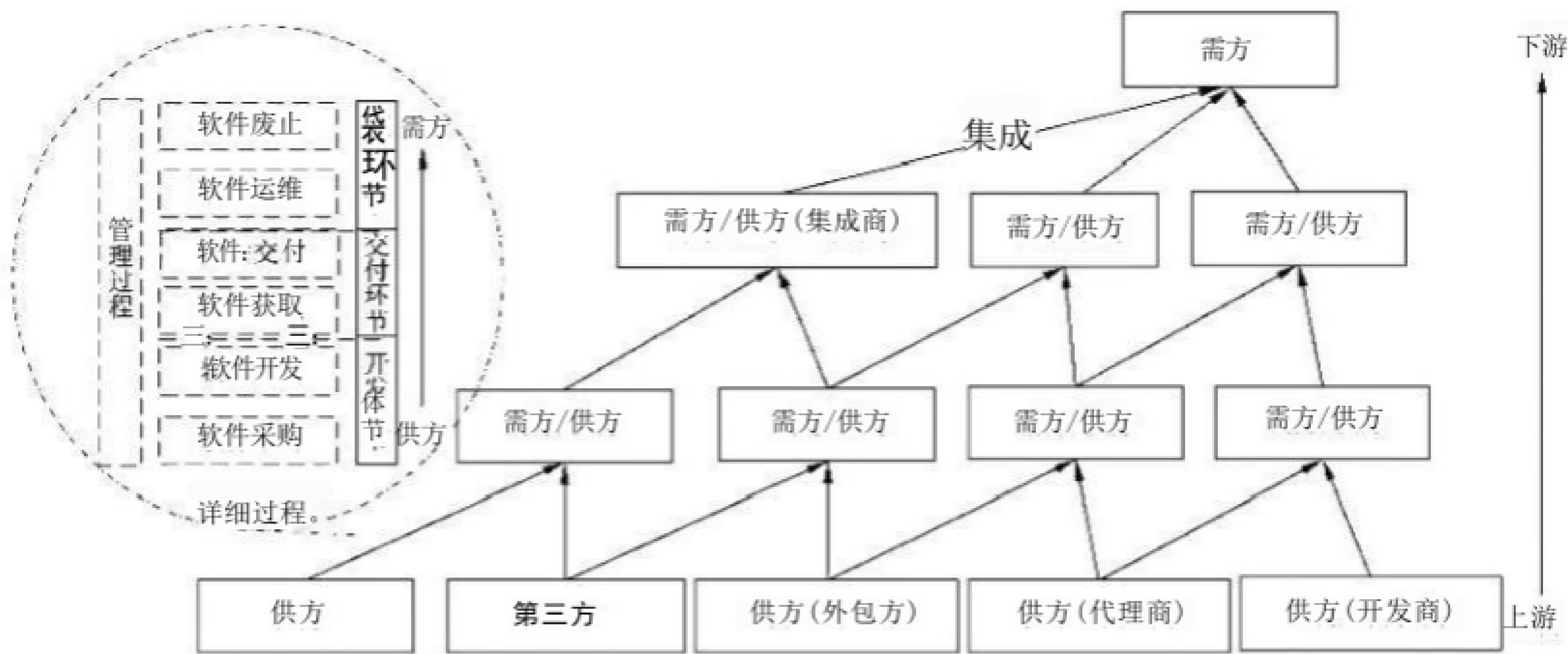


图 A.1 软件供应链模型示意图

A.2 软件供应链实体角色分析

软件供应链主要相关实体角色是供方和需方。在特定条件下，第三方机构将参与供方和需方的相关活动。其中，第三方机构在软件供应链中主要根据供需双方的安全要求开展软件供应链安全检测、评估、咨询等服务，在此过程中第三方机构作为服务提供方属于供方角色范畴。软件供应链中供方、需方和第三方机构间的关系如图 A.2 所示。

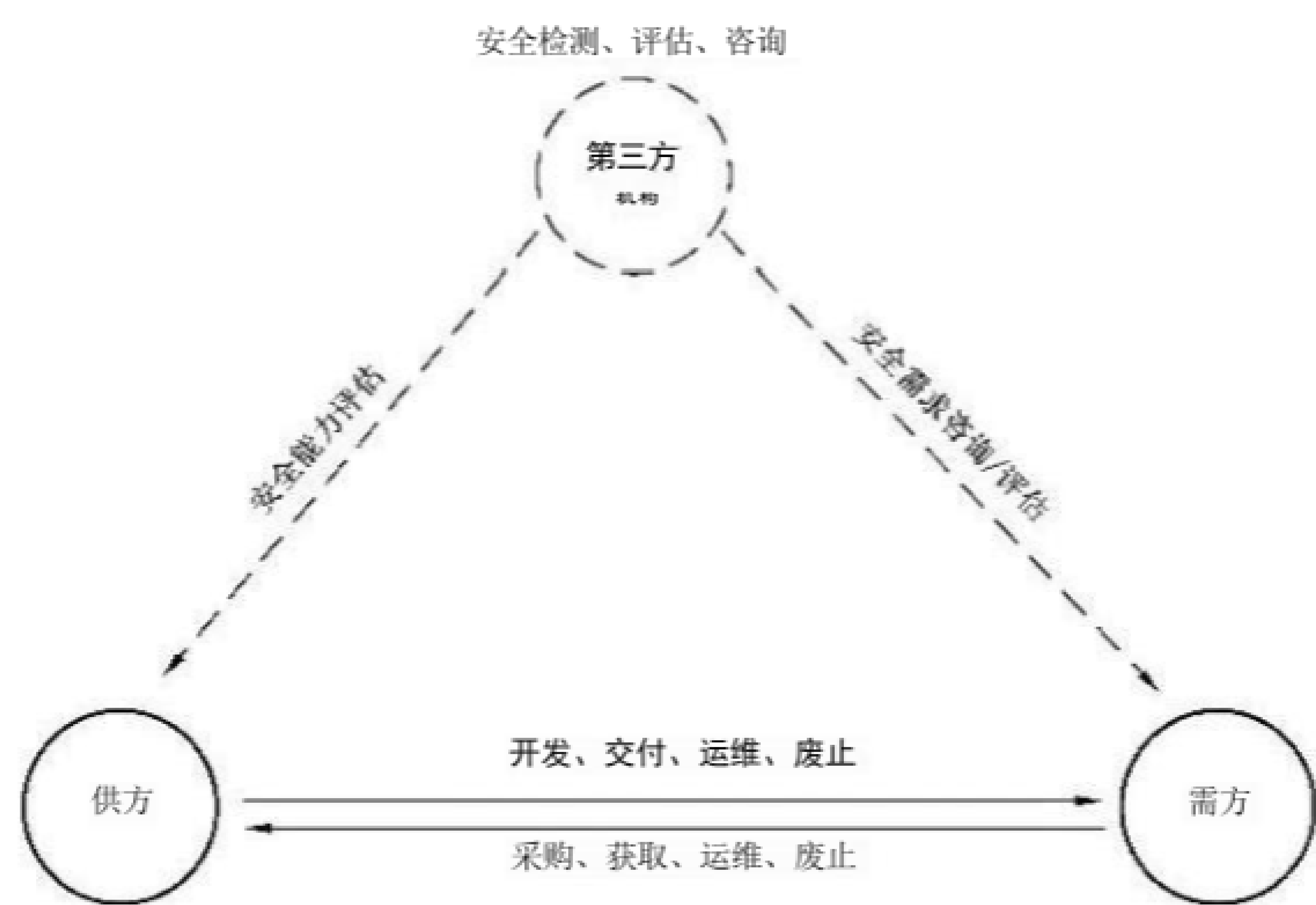


图 A.2 软件供应链实体角色关系图

A.3 软件供应链安全构成

A.3.1 概述

软件供应链安全包括实体角色与活动、环节与供应活动、安全风险等内容，如图A.3 所示。

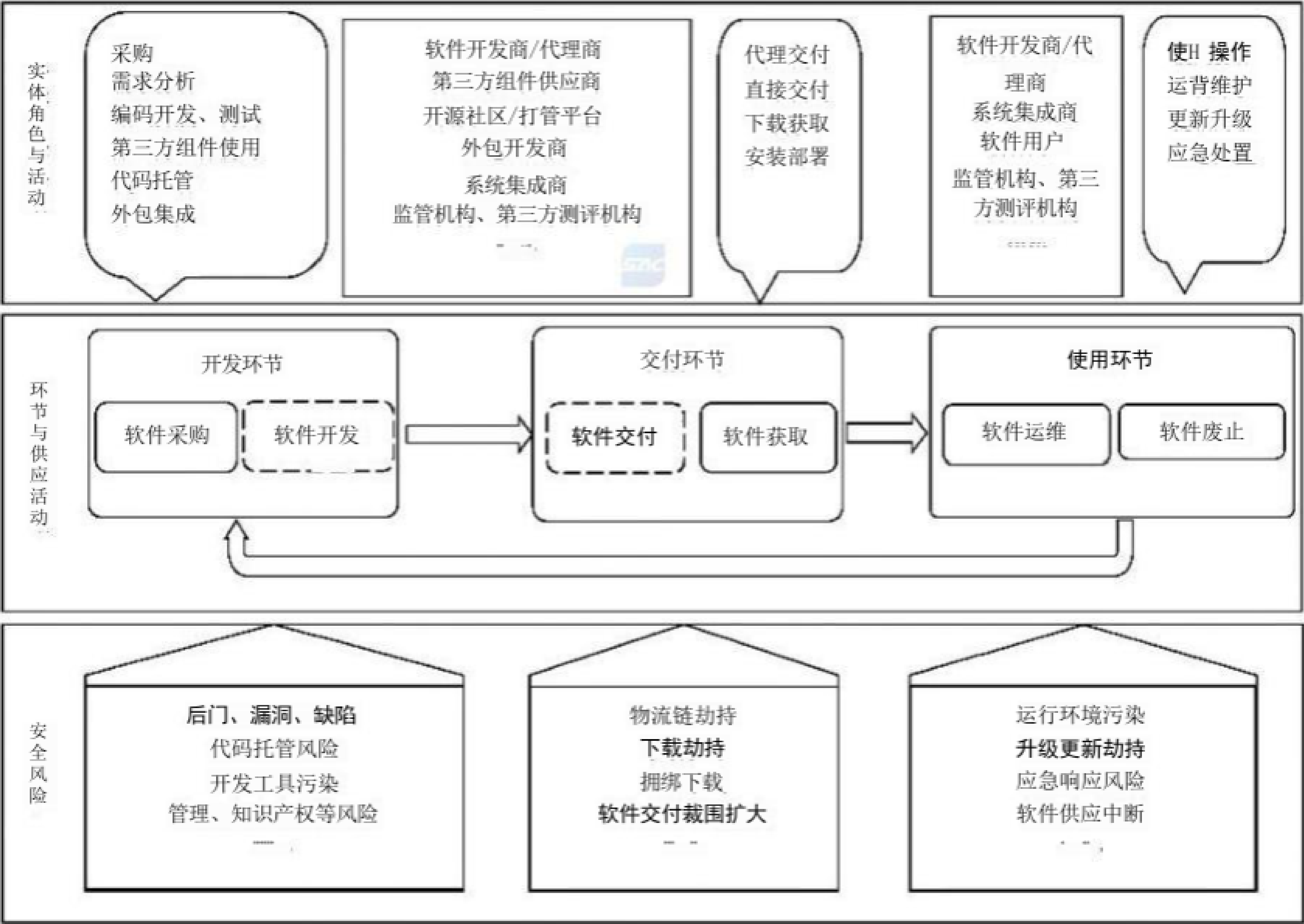


图 A.3 软件供应链安全构成示意图

A.3.2 软件供应链环节与供应活动

软件供应链主要包括三个环节，分别是开发环节、交付环节和使用环节。软件供应链安全以软件供应链环节为主线，以风险管理为总体依据，指导供需双方开展组织管理和供应活动管理工作。软件供应链中的供应活动包括软件开发、软件采购、软件交付、软件获取、软件部署、软件使用、软件运维和软件废止。根据实体角色的不同，在各个环节中供需双方涉及的供应活动不同。需方和供方涉及的各个供应活动的相关描述如表 A.1 所示。

表 A.1 软件供应链环节和供应活动

环节名称	供应活动	实体角色	活动描述
开发环节	软件采购	需方	通过文件、协议或合同的方式确定软件供需双方的关系，软件采购将对软件供应链中后续供需双方的供应活动的总体要求进行阐释、说明和约定
	软件开发	供方	软件供应链的供方进行软件的设计、编码、集成、测试等活动，形成满足需方要求的软件
交付环节	软件交付	供方	供方通过特定的方式或渠道将软件交付至需方
	软件获取	需方	需方从供方获取软件，并开展软件验收等工作
使用环节	软件运维	供方 需方	为保障软件的正常运行，软件供应链的供方和需方开展运营、维护、排障、更新、应急处置等工作
	软件废止	供方 需方	在软件生命周期结束之前，供需双方对上述活动中产生的程序、代码、资料、文档等进行销毁、封存、存档等处理工作

A.3.3 软件供应链安全风险

A.3.3.1 概述

在软件供应链各个供应活动中均可能引入安全风险，主要分为供应关系风险、技术风险和知识产权风险3类。其中，供应关系风险主要是指供应中断，技术风险主要指软件漏洞、软件后门、恶意篡改和信息泄露等，知识产权风险主要指假冒伪劣、不合规等安全风险。

A.3.3.2 供应中断和降级

因自然等不可抗力、政治、外交、国际经贸等原因造成上游软件、使用许可、知识产权授权等交付途径中断，交付物的功能、性能降级。

A.3.3.3 软件漏洞

软件漏洞通常被认为是软件生命周期中出现的设计错误、编码缺陷以及运行故障。

A.3.3.4 软件后门

主要包括以下内容。

- a) 供方预留
在软件产品中预置且未向需方声明的用于管理、运维、调试等接口，如果被泄露，攻击者会通过预置接口获得软件或操作系统的访问权限。
- b) 攻击者恶意植入
攻击者入侵供应链环节，在供应链环节中修改软件组件以植入恶意后门，达到捆绑恶意代码、下载劫持、网络劫持、物流链劫持、升级劫持等目的。

A.3.3.5 恶意篡改

主要包括以下内容。

- a) 恶意代码植入
在需方不知情的情况下，在软件产品或供应链中的组件、外部工具(开发、测试、运维等工具)中植入具有恶意逻辑的可执行文件、代码模块或代码片段。
- b) 供应信息篡改
在供方不知情的情况下，篡改软件供应链上传递的供应信息，如销售信息、商品信息、软件构成信息等。

A.3.3.6 假冒伪劣

供方提供未经产品认证、检测的软件或组件，或未按照声明和承诺提供合格的产品。

A.3.3.7 信息泄露

软件供应链信息被有意或无意地泄露，如软件上游供应商、下游需方的信息可能涉及商业秘密，供应链信息存在被泄露的风险。

A.3.3.8 供应链劫持

供应链劫持是普遍存在的一种供应链污染，安全风险突出，涉及捆绑恶意代码、下载劫持、网络劫持、物流链劫持、升级劫持等。

A.3.3.9 知识产权非法使用

未经授权而生产、销售、发布软件或组件，导致软件产品的全部或部分被泄漏到授权以外的范围，如盗版软件、违反开源许可使用的软件、违反协议进行的二次开发等。

A.3.3.10 开源许可违规使用

主要包括以下内容。

- a) 无开源许可证
软件产品发布时缺少开源许可证类型，包括但不限于 LGPL、Mozilla、GPL、BSD、MIT、Apache 等许可证。
- b) 使用不规范
软件产品发布时不符合相应许可协议的规范和要求，包括但不限于没有遵循开源许可证协议，开源组件修改后许可信息丢失，存在无许可信息的开源片段代码等。

A.3.3.11 其他风险

由于软件供应链内外部人员、软件供应链全球性等特点带来的风险或挑战。

附录 B
(资料性)
关键软件资产

B.1 概述

关键软件资产主要指具有或直接依赖包含至少一项特定关键功能属性的软件，比如处理重要数据、涉及特权操作等。

B.2 关键软件资产清单

在重要业务场景和核心业务场景中梳理关键软件资产，建立关键软件资产清单，并将关键软件资产所依赖的其他软件纳入关键软件资产清单。

B.3 关键软件资产供应链梳理

关键软件资产供应链梳理的信息，主要包括以下内容。

- a) 产品发布版本号。
- b) 产品原厂。
- c) 产品生命周期。
- d) 产品补丁发布计划。
- e) 产品交付途径。
- f) 产品部署方式(在线或离线)。
- g) 产品授权(或许可)方式、年限。
- h) 产品中所包括的外部组件清单，及其源供应商。
- i) 产品发行版本是否有激活等技术性版权控制措施。如有，还需进一步梳理如下信息：
 - 1) 激活版本和未激活版本是否有功能差异；
 - 2) 激活是线上完成还是离线完成；
 - 3) 激活是否需要原厂提供的凭据、数据等，这些凭据、数据丢失或损坏后能否以及如何恢复；
 - 4) 激活是永久激活还是定期激活；
 - 5) 是否有去激活机制，去激活是否需要原厂参与；
 - 6) 是否允许重新激活，重新激活过程是否可以离线完成。
- j) 产品部署版本和补丁从原厂交付到需方、并部署到需方信息系统的所有经过的交付节点(环节)列表，明确如下信息：
 - 1) 原厂是否提供交付环节端对端数据完整性保护措施；
 - 2) 交付环节之间是否提供点对点的完整性保护措施；
 - 3) 每一个交付环节是否有防止交付物被修改的措施。

对产品中包括的核心外部组件，需要软件供应商提供外部组件源供应商与其之间的供应链信息，至少包括上述 a)~j) 项信息。

附录 C
(资料性)
组织业务场景分类

组织根据软件是否应用于关键信息基础设施、软件资产分类、场景价值3个要素对业务场景分类，具体流程如下：

- a) 根据国家相关规定确定软件是否应用于关键信息基础设施(关基)；
- b) 结合软件在实际业务中的重要程度，将其确定为一般软件资产、关键软件资产(见附录B)；
- c) 根据a)和b)的结果确定场景的价值为较低、较高和很高；
- d) 场景价值较低的为一般业务场景，场景价值较高的为重要业务场景，场景价值很高的为核心业务场景，如表 C.1 所示。

表 C.1 业务场景分类

场景分类结果	应用于关键信息基础设施	软件资产分类	场景价值	场景说明	软件供应链安全图谱
一般业务场景	否	一般	较低	仅涉及个人或组织安全或利益数据的业务场景下的软件供应链： 1) 业务场景价值较低； 2) 受到损害后仅对法人或组织安全造成损害，影响范围较小	基础级
重要业务场景	否	关键	较高	行业或社会广泛使用的，涉及行业或社会重要数据业务场景下的软件供应链： 1) 在行业或社会广泛使用，业务场景价值较高； 2) 受到破坏后损害组织、公共利益或社会安全	通用级
	是	一般			
核心业务场景	是	关键	很高	全社会使用非常广泛、国家重要领域、要害部门等关键信息基础设施中涉及国家安全和国计民生的软件供应链： 1) 用户为全社会、国家重要领域、要害部门，业务场景价值很高； 2) 涉及国家安全和国计民生，受到破坏后损害国家安全或严重损害社会安全	增强级

附录 D
(资料性)
软件供应链安全图谱

D.1 图谱构成

软件供应链安全图谱包含软件产品信息、软件物料清单和安全信息3方面内容。其中，安全信息是指软件物料清单中的组件、代码中存在的技术安全和合规安全信息。软件供应链安全图谱可由需方、供方或者第三方机构构建或生成。

D.2 实体要素

根据图谱构成将软件供应链实体要素分为3个一级分类，8个二级分类，详细分类信息参考表 D.1，表中“√”建议必选。

表 D.1 软件供应链安全图谱实体要素清单

序号	一级分类	二级分类	实体要素名称	说明	基础级	通用级	增强级
1	软件产品信息	软件基本信息	软件名称	官方发布的软件名称	√	√	√
2			完整性验证	完整性标识	√		
3				数字签名、数字证书		√	√
4			软件版本	官方发布的版本信息	√	√	√
5			引入组件数量	开源、第三方、自主研发		√	√
6			标记信息	重要数据、关基、重要信息系统	√	√	√
7			软件供应链基础设施	开发、测试、运行库、工具等			可选
8		软件来源	供方	直接供应商	√	√	√
9			源开发商	开发者			√
10		软件授权	期限	有效期限	√	√	√
11			方式	许可证、序列号		√	√
12		关联软件	软件1, 软件2, ……	软件产品信息			√
13	软件物料清单	清单信息	唯一标识	唯一标识方法、数字签名等		√	√
14			生成阶段	软件供应活动			√
15			时间戳	生成时间		√	√
16		软件成分信息(组件1、组件2、 ……)	生成者	需方、供方或第三方机构		√	√
17			许可协议	许可协议信息		√	√
18			组件名称	组件名称		√	√
19			组件唯一标识	唯一标识		√	√
20			组件版本	官方发布的版本信息		√	√
21			组件来源	组件提供商		√	√
22				源供应商			可选
23			组件引用关系	直接引用		√	√
24				间接引用			√
25			组件调用位置	组件的使用位置		√	√

表 D.1 软件供应链安全图谱实体要素清单 (续)

序号	一级分类	二级分类	实体要素名称	说明	基础级	通用级	增强级
26	安全信息	技术安全	软件漏洞	A. 3. 3. 3		√	√
27			漏洞修复	漏洞补丁信息		√	√
28			漏洞利用	漏洞利用信息			可选
29			假冒伪劣	A. 3. 3. 6			可选
30			其他安全问题				可选
31		合规安全	开源许可协议	A. 3. 3. 10		√	√
要素合计(项)					6	21	25

D.3 软件供应链安全图谱元素关系

软件供应链安全图谱可以准确描述组织中软件产品信息、软件物料清单和安全信息之间的关系，以及其中所包含元素之间的关系。其中，软件与软件之间存在调用关系，软件和组件存在直接或间接引用关系，组件与组件之间为引用关系，软件或者组件与安全信息之间为存在关系。如图 D.1 所示。

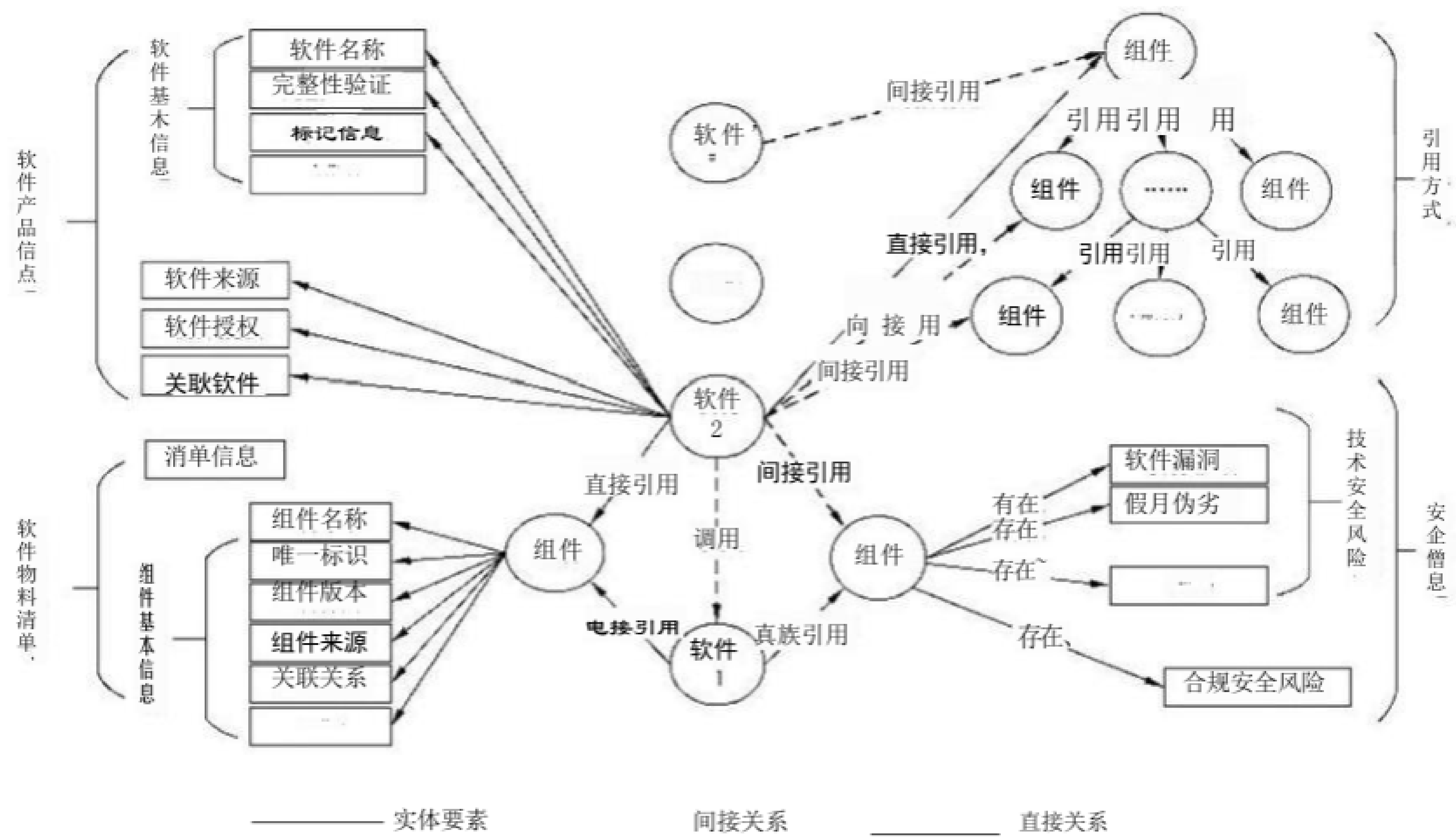


图 D.1 软件供应链安全图谱元素关系示意图

参 考 文 献

[1]GB/T 30998—2014 信息技术 软件安全保障规范

[2] GB/T 32921—2016 信息安全技术 信息技术产品供应方行为安全准则

[3] GB/T 36475—2018 软件产品分类

[4] GB/T 37970—2019 软件过程及制品可信度评估

[5] GB/T 37988—2019 信息安全技术 数据安全能力成熟度模型

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

[7]ISO/IEC 27036-2 Information technology—Security techniques—Information security for supplier relationships—Part 2:Requirements

[8] ISO/IEC 27036-3 Information technology—Security techniques—Information security for supplier relationships—Part 3:Guidelines for information and communication technology supply chain security

[9] NIST 800-161 Supply Chain Risk Management Practices for Federal Information Systems and Organizations
