软件供应链安全保障能力分级测评

服务白皮书

版本：1.0

二〇二五年四月

目　　录

第 1 章 简介

1.1 服务说明

软件供应链安全保障能力分级测评是依据国家标准 GB/T 43698-2024《网络安全技术 软件供应安全要求》，对软件产品的供应链组织管理能力和供应活动管理能力等进行综合评定后，由中国信息安全测评中心（以下简称“测评中心”）给予的能力等级认定。

软件供应链安全保障能力分级测评的测评对象是软件产品，通过对软件产品在采购、研发、交付、运维等软件供应链各阶段的组织管理和供应活动管理状况开展测评，对软件产品相关的组织管理安全和供应活动管理安全状况作出判断，综合评估申请单位作为软件产品的供方或者需方，在开展软件产品相关的各类活动中，是否达到了相应安全保障能力等级要求，是否具备相应等级的软件供应链组织管理安全保障能力、供应活动安全保障能力和软件供应链安全风险防范能力。整个能力等级由低到高共分为三级，分别是一级、二级和三级，三级为最高级。对于通过软件供应链安全保障能力分级测评的软件产品，测评中心将出具测评报告，并颁发软件供应链安全保障能力等级证书。

1.2 目的和意义

基础软件、核心组件停服断供，关键软件预置漏洞后门，开源软件违规使用等软件供应链安全问题不仅严重危害软件产品自身、软件

研发企业及软件产品用户的安全，严重的甚至影响国家安全。例如SonarQube 代码托管平台源代码泄露、Log4J2、XZ-Utils、微软蓝屏事件等软件供应链安全问题，已对全球网络安全造成严重影响。我国基础软件、开源软件同样面临严重的软件供应链安全威胁和挑战，软件供应链安全问题成为当前各行业亟需解决的热点问题。

2024 年，测评中心牵头研制的我国软件供应链安全领域首个国家标准 GB/T 43698-2024《网络安全技术 软件供应链安全要求》获批发布。为切实提升我国软件供应链安全保障能力，测评中心依据国家标准推出软件供应链安全保障能力分级测评服务，旨在通过软件供应链组织管理能力测评、供应活动管理能力测评以及软件产品供应链安全检测多措并举，防范我国软件供应链安全领域面临的供应关系风险、技术安全风险以及知识产权安全风险，提升软件产品供应链安全能力，进而推动构建并完善软件产品供应链安全治理体系，对提升用户单位的软件供应链安全保障能力具有重要意义。

1.3 服务特色

1.3.1 国家权威

测评中心多年来根据国家授权，依据相关法律法规和标准规范对外开展网络安全测评服务，牵头编制了我国软件供应链安全领域首个国家标准 GB/T 43698-2024《网络安全技术 软件供应链安全要求》，率先在行业内数十家单位开展了标准试点应用，具有良好的理论基础和实践基础。

1.3.2 公平公正

测评中心是国家级第三方独立测评机构，不代表任何商业组织的利益，出具的测评报告以事实为依据，以公平、公正、科学、客观为准则。

1.3.3 可靠专业

测评中心具有近三十年的信息安全服务资质、产品安全测评、软件代码安全等领域安全测评业务积累，具有丰富的测评经验和技术基础，具有一批高水平软件安全测评专业技术人员，能够为用户提供可靠、专业的技术服务。

1.4 测评依据

GB/T 43698-2024《网络安全技术 软件供应链安全要求》

1.5 参考标准

1. GB/T 34943-2017《C/C++语言源代码漏洞测试规范》
2. GB/T 34944-2017《Java 语言源代码漏洞测试规范》
3. GB/T 34946-2017《C#语言源代码漏洞测试规范》
4. GB/T 39412-2020《信息安全技术 代码安全审计规范》
5. GB/T 30279-2020《信息安全技术 网络安全漏洞分类分级指南》
6. GB/T 42446-2023《信息安全技术 网络安全从业人员能力基本要求》

第 2 章 测评内容

根据国家标准 GB/T 43698-2024，软件供应链安全保障能力分级测评共分为组织管理安全测评和供应活动管理安全测评两方面测评内容。其中，组织管理安全测评包括机构管理安全、制度管理安全、人员管理安全、供应商管理安全和知识产权管理安全共 5 个测评单元，供应活动管理安全测评包括基本流程安全、软件采购安全、软件开发安全、软件交付安全、软件获取安全、软件运维安全和软件废止安全共 7 个测评单元。

由于国标对软件产品供、需双方的总体安全要求不同，面向供、需各方的测评内容存在差异，因此，测评采用了分角色测评的思路，申请单位需根据实际情况，首先确定自身在开展软件产品供应活动中的角色，即需确定是作为软件产品的供方还是需方申请本项服务。供、需各方基本测评内容如图 2-1 和图 2-2 所示。但是，在实践应用中，由于不同企业、不同产品的软件供应活动可能存在较大差异，供方在软件供应活动中，也可能涉及软件采购、软件外包等情况，需方也可能涉及自主软件开发活动。因此，除基本测评内容外，申请单位还应根据自身实际，确定是否需要在基本测评内容基础上，增测与相应活动相关的测评内容。测评过程中，测评组将依据国标，通过文档分析、人员访谈、现场核查、技术验证测试等方式，综合评估软件产品的软件供应链安全保障能力。

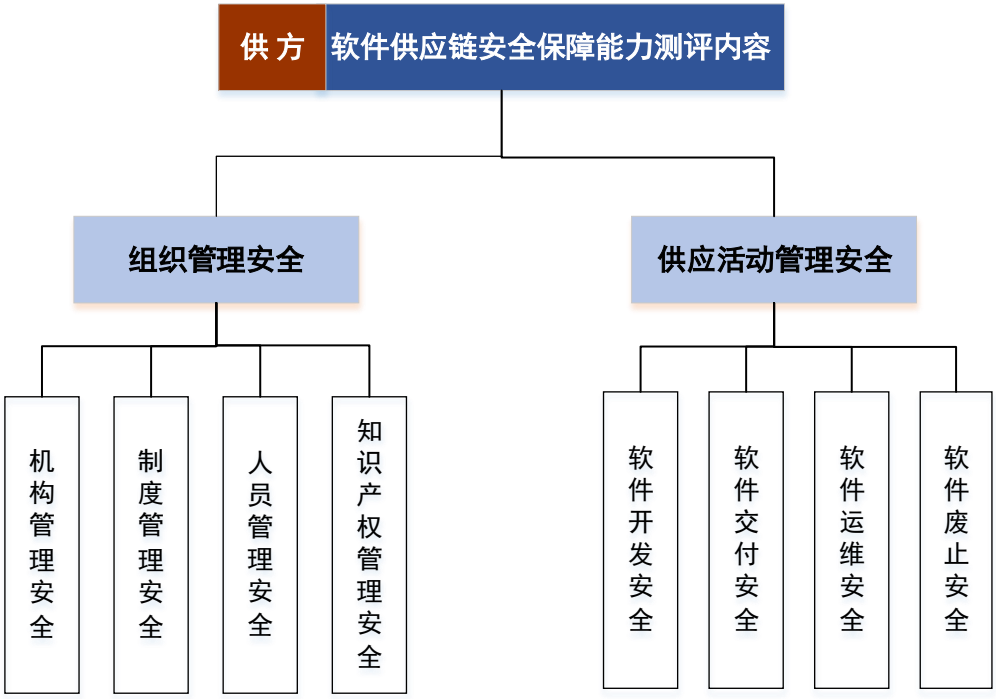

图 2-1 供方基本测评内容

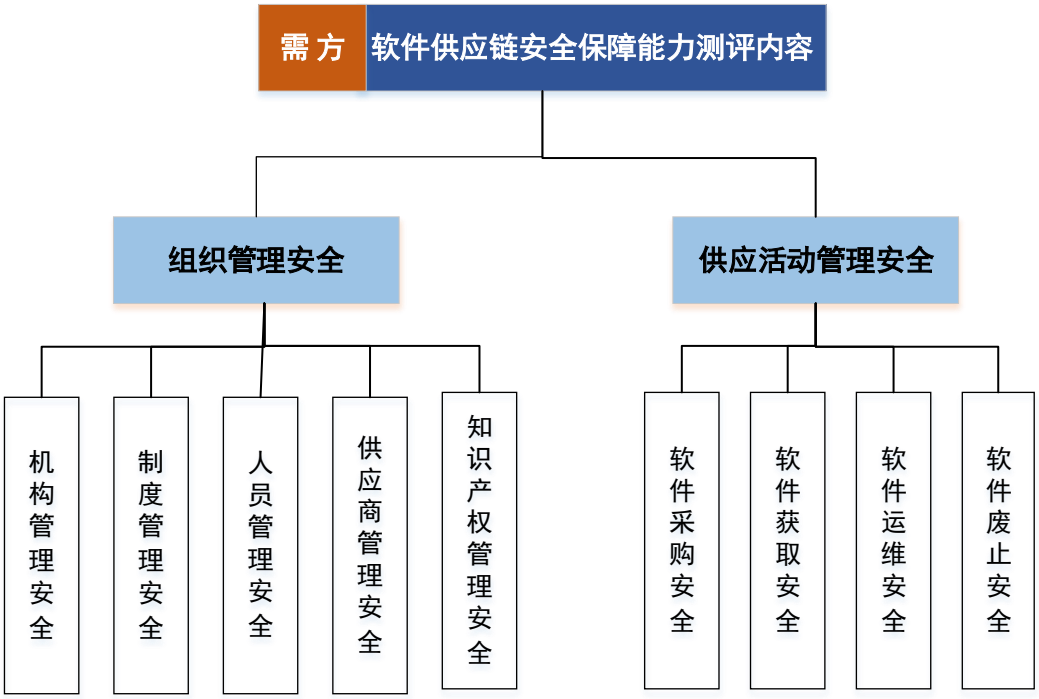

图 2-2 需方基本测评内容

2.1 组织管理安全测评

组织管理安全测评主要针对软件产品供应链中的组织管理安全进行测评，测评内容包括机构管理安全、制度管理安全、人员管理安全、供应商管理安全和知识产权管理安全共 5 个测评单元。测评组通过对申请单位提交的文档资料的分析，对软件产品的供应链组织管理能力做出基本判断，再通过现场核查等方式评估软件产品的供应链组织管理能力水平状况。

2.1.1 机构管理安全

机构管理安全重点针对软件产品的供应链安全相关机构设置、权限划分、任务分工、资源保障等机构管理状况进行测评。

2.1.2 制度管理安全

制度管理安全重点针对软件产品生命周期过程中形成的供应活动安全管理、人员管理、知识产权管理等方面相关制度的制修订及宣贯执行能力进行测评。

2.1.3 人员管理安全

人员管理安全重点针对软件产品供应链相关人员的岗位管理、权限管理、技能培训、离岗管理、团队建设、绩效考核等方面的安全保障能力进行测评。

2.1.4 供应商管理安全

供应商管理安全重点针对在软件供应商选择、评估、审核、监督等方面的安全保障能力进行测评。

2.1.5 知识产权管理安全

知识产权管理安全重点针对软件产品涉及的开源许可协议、软件著作权、专利、授权等方面的知识产权管理能力进行测评。

2.2 供应活动管理安全测评

供应活动管理安全测评主要针对软件产品供应链中的供应活动管理安全进行测评，测评内容包括基本流程安全、软件采购安全、软件开发安全、软件交付安全、软件获取安全、软件运维安全和软件废止安全共 7 个测评单元。测评组通过对申请单位提交的文档资料的分析，对申请单位在开展软件产品相关的软件供应活动管理能力做出基本判断，再通过现场核查等方式评估软件产品供应链的实际安全能力水平状况，同时，根据测评实际情况，对已开展的软件供应链安全检测、测试等工作进行技术验证测试。

2.2.1 基本流程安全

基本流程安全主要针对软件产品供应活动中软件产品供应链关系建立、供应活动执行等基本工作流程安全保障能力进行测评。

2.2.2 软件采购安全

软件采购安全主要针对软件产品采购过程中，软件产品相关的采购人员、采购方案、以及各项供应活动的安全规划等方面的安全保障能力进行测评。

2.2.3 软件开发安全

软件开发活动是供方供应活动中最核心、最重要的过程，软件开发安全测评重点针对在软件需求分析、设计、编码、集成、测试等阶段开展的应用程序安全、开发基础设施安全、外部组件安全等安全保障能力进行测评。其中，开发基础设施安全是指软件开发过程中涉及的开发环境、编译构建环境、调试分析环境、持续集成和持续交付环境、代码库、知识库等软件开发基础设施的安全。外部组件安全是指软件开发过程中保障软件产品所使用的开源组件、商业组件等外部组件的安全。

2.2.4 软件交付安全

软件交付安全重点针对在交付软件的内容、范围、渠道以及部署等方面的安全保障能力及合同的满足情况进行测评。

2.2.5 软件获取安全

软件获取安全主要针对在软件完整性验证、安全检测、技术资料获取等履约验收方面的安全保障能力进行测评。

2.2.6 软件运维安全

软件运维安全重点针对软件产品的运营、维护、排障、更新、应急处置等方面安全保障能力进行测评，具体测评内容包括运维环境安全、运维策略安全、运维数据安全、运维人员安全和运维变更安全等多方面。

2.2.7 软件废止安全

软件废止安全重点针对在软件产品的生命周期结束之前，对已产生的软件程序、代码、资料、文档等进行销毁、封存、存档等方面安全保障能力的测评，具体测评内容包括软件卸载与停用安全、软件与数据销毁安全、数据备份与迁移安全等多方面。

第 3 章 测评等级

3.1 等级划分

软件供应链安全保障能力分级测评的能力等级由低到高共分为三级，分别是一级、二级和三级，三级为最高级，各测评等级对应能力水平如下。对于通过软件供应链安全保障能力测评的软件产品，测评中心将针对该软件产品出具测评报告，并颁发该软件产品对应等级的软件供应链安全保障能力等级证书。

一级：申请单位初步认识软件供应链安全的重要性，在开展软件产品相关的软件供应活动中，建立了基本的软件供应链安全保障策略和工作流程，具有一定的组织管理安全保障能力；实施了基本的软件供应链安全保障措施，构建了符合基础级要求的软件供应链安全图谱，掌握了软件产品的成分，相应软件产品具有防范一定程度的软件供应链技术风险、知识产权风险和供应中断风险的能力。

二级：申请单位充分认识软件供应链安全的重要性，在开展软件产品相关的软件供应活动中，建立了较完善的软件供应链安全保障策略和工作流程，具有较好的组织管理安全保障能力；实施了较完善的软件供应链安全保障措施，构建了符合通用级要求的软件供应链安全图谱，相应软件产品能够防范因采用外部软件或组件而引入的软件供应链技术风险、知识产权风险和供应中断风险，具备抵御较强软件供应链安全风险的能力。

三级：申请单位高度重视软件供应链安全，在开展软件产品相关的软件供应活动中，建立了完善的软件供应链安全保障体系；采用了覆盖软件产品供应链全流程的安全保障措施和技术手段，构建了符合增强级要求的软件供应链安全图谱，相应软件产品具备全面抵御软件供应链安全风险的能力。

3.2 评分方法

按照一定规则，采用累加计分法，分别计算组织管理类安全测评指标得分和供应活动类安全测评指标得分，最后将各项得分相加作为最终得分，满分为 100 分。其中，测评指标分为符合、部分符合、不符合和不适用等四种情况，只有符合和部分符合的测评指标可参与计分。

3.3 测评通过标准

软件供应链安全保障能力分级测评通过标准如下：

一级：组织管理和供应活动管理满足一级部分或全部测评指标，得分不少于 80 分，软件供应链安全图谱符合基础级图谱要求；

二级：组织管理和供应活动管理满足二级部分或全部测评指标，得分不少于 80 分，软件供应链安全图谱符合通用级图谱要求；

三级：组织管理和供应活动管理满足三级部分或全部测评指标，得分不少于 80 分，软件供应链安全图谱符合增强级图谱要求。

第 4 章 服务流程

4.1 工作流程

软件供应链安全保障能力分级测评的具体工作流程可分为业务受理、测评准备、测评实施和证书发放共四个阶段，如图 4-1 所示。

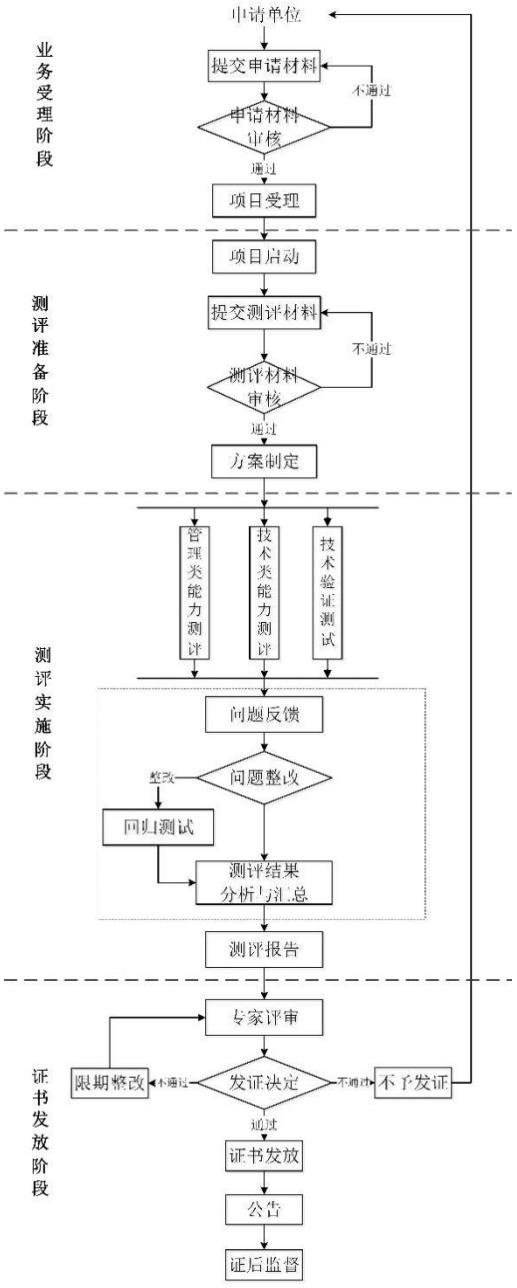

图 4-1 测评流程图

1）业务受理阶段

申请单位应首先到测评中心网站查看并下载《软件供应链安全保障能力分级测评申请书》和《软件供应链安全保障能力分级测评申请指南》及有关附件，了解测评流程及相关要求，并根据自身实际情况，确定拟申请的产品名称、服务内容、测评等级等内容。

申请单位应按照申请指南要求填写分级测评申请书，加盖公章后与申请书中要求的其他相关材料一并提交给测评中心。测评中心业务受理部门将对申请单位提交的所有材料进行形式化审查。通过审查的业务申请将被受理并进入下一阶段，未通过审查的，测评中心将提出反馈意见，申请单位在补充完善后，需再次提出服务申请。业务受理过程中，如遇严重问题的，测评中心可拒绝接受相关服务申请。

2）测评准备阶段

测评中心针对已受理的服务申请，将正式启动分级测评工作，成立项目组，明确项目负责人和项目联系人。项目组将根据分级测评工作需求，积极与申请单位进行沟通，提出更加具体的测评需求，并制定项目测评方案。申请单位应积极配合项目组相关准备工作，因申请单位原因造成的时间延误由相关单位自行承担。如遇严重问题的，测评中心可出具书面情况说明，暂停项目执行。

3）测评实施阶段

测评项目组将根据审核通过后的项目测评方案，综合采用人员访谈、文档分析、现场核查和技术检测等方式，针对申请单位在软件产

品生命周期过程中的组织管理和供应活动管理状况进行测评，对申请单位软件供应链安全保障能力进行综合评定。测评过程中，申请单位需提供必要的支持，以完成现场核查、技术验证测试等测评工作。

所有测评指标的测评工作完成后，项目组将对测评结果进行综合评定，并给出初步测评结果。对评定结果为不符合的测评指标，测评中心将要求申请单位限期整改。申请单位完成整改并向测评中心提交整改报告后，测评中心将开展一次回归测试，对整改结果进行验证；逾期未整改的，视作放弃整改。测评中心基于初测和回归测试的结果，给出最终测评结果，并出具测评报告。

4）证书发放阶段

测评中心将组织专家委员会对测评结果进行评审，评审通过后，对于测评结果为通过的软件产品，测评中心将针对该软件产品出具正式测评报告，并颁发该软件产品对应等级的软件供应链安全保障能力等级证书并在测评中心网站、报刊杂志（中国信息安全）、公众号（国家信息安全服务资质）等媒体上予以公告；对于测评结果为未通过的软件产品，测评中心将只出具正式测评报告。

4.2 服务接口

资质评估处是软件供应链安全保障能力分级测评服务的业务受理部门和证书发放部门，是软件供应链安全保障能力分级测评服务的对外沟通联系接口，负责软件供应链安全保障能力分级测评服务的业务受理、组织开展专家评审、发放测评报告和等级证书等工作。

4.3 资料提交

申请单位应根据服务要求提交相关资料，资料主要包括软件供应链安全相关制度文件、台账记录、图谱资料以及技术分析报告等内容。详细内容请参考：

（1）《软件供应链安全保障能力分级测评申请书》

（2）《软件供应链安全保障能力分级测评申请指南》

4.4 服务交付物

本服务的交付物为《软件供应链安全保障能力测评报告》和《软件供应链安全保障能力等级证书》，证书有效期为 3 年。

第 5 章 工作量及建议报价

5.1 基础报价

各测评等级对应的测评周期和建议报价如表 5-1 所示。其中，测评周期为参考时间，且由于申请方原因（如资料补充需要的时间，或因测评项整改等）造成的时间延误不计算在测评周期内。

表 5-1 工作量估算及建议报价

服务项	测评周期	建议报价
软件供应链安全保障能力一级	约 25~50 个工作日	20 万元
软件供应链安全保障能力二级	约 35~60 个工作日	30 万元
软件供应链安全保障能力三级	约 45~80 个工作日	40 万元

5.2 特殊测评需求

5.2.1 测评内容增加

除表 5-1 约定的测评内容外，根据申请单位及软件产品供应链实际情况，需增加测评内容的，例如申请单位为软件产品的供方，但是在软件产品的生产研制过程中，涉及软件外包、采购等情况时，须增加相应测评指标，测评周期和测评费用也将适当调整。

5.2.2 测评时间限定

加急测评，即测评时间限定为低于工作量预算时间的，则定价根据工作量酌情增加 20%至 50%。

5.2.3 测评方法限定与其它

根据测评方法限定与其它要求的特殊性，酌情商榷增加比例。

附录 相关术语

[1] **软件产品**：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，包括一系列计算机程序代码、数据及相关文档和服务。

[2] **软件产品信息**：关于软件产品的各类描述性数据，包括软件产品版本、标识、来源、授权以及关联软件等信息的总称。

[3] **需方**：软件产品的购买者和使用者。

[4] **供方**：开展软件产品开发、交付、运维、废止等生命周期活动的组织。如需方的第一级（直接）供应商，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，但开放源代码社区本身不是供方。

[5] **供应关系**：需方和供方之间为开展业务、提供软件产品而建立的协议、合同等商业联系，涉及双方在软件供应活动中的权利、义务、责任等内容。

[6] **软件供应链**：需方和供方基于供应关系，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。

[7] **软件物料清单**：详细记录软件产品中包含所有组件的清单，包括开源组件、第三方组件、版本、依赖关系、来源、许可协议等内容。

[8] **外部组件**：软件运行所依赖的由供方以外的组织或人员提供的软件组件或服务，如开源组件、第三方插件、商用组件等。

[9] **软件供应链安全图谱**：以可视化或结构化的方式展示软件产品信息、软件物料清单、安全信息等内容及其关联关系的描述和表示。

注 1：软件供应链安全图谱是分级测评的重要测评内容，一级要求构建了符合国标基础级要求的软件供应链安全图谱，掌握软件产品的基本成分；二级要求构建了符合通用级要求的软件供应链安全图谱；三级要求构建了符合增强级要求的软件供应链安全图谱。

注 2：根据国标 GB/T 43698-2024，软件供应链安全图谱分为基础级、通用级、增强级共三个等级，各等级图谱需要记录的实体要素及说明如下表所示：

软件供应链安全图谱实体要素清单表

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、自主研制		√	√
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	软件开发、运维、交付等			√
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		√	√
26	安全信息	技术安全	软件漏洞			√	√
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				可选
30			其他安全问题				可选
31		合规安全	开源许可协议			√	√
要素合计（项）					6	21	25