ICS 35.020
L 70

团　　体　　标　　准

T/GDCSA 013—2022

重要信息基础设施（软件）供应链安全检查评估指南

Specification for security inspection and evaluation of important information infrastructure (Software) supply chain

2022－12－28 发布　　2022－12－28 实施

北京网络空间安全协会
广东省网络空间安全协会　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。

本文件由绿盟科技集团股份有限公司提出。

本文件由北京网络空间安全协会和广东省网络空间安全协会归口。

本文件起草单位：绿盟科技集团股份有限公司、深圳供电局有限公司信息中心、深圳大学、广东电网有限责任公司信息中心、广东关键信息基础设施保护中心、广州华南信息安全测评中心、广东新兴国家网络安全和信息化发展研究院、网安联认证中心有限公司、网安联信息技术有限公司。

本文件主要起草人：林小博、肖岩军、林勇忠、刘威、江魁、胡斌、黄珊珊、邓巍、程宏振、黄丽玲、崔磊、赖智全、沈伍强、张伟、戴尚锟、邢静、黎韵婷、李俊宾、毛翠芳、蔡俊珊。

引　言

随着经济全球化和信息技术的快速发展，网络产品和服务供应链已发展为遍布全球的复杂系统，任一网络产品组件、任一供应链环节出现问题，都有可能影响重要信息基础设施。保障重要信息基础设施安全的一个重要方面是要确保重要信息基础设施使用的网络产品和服务的供应链安全。

近年来，国家互联网信息办公室等12个部门联合发布了《网络安全审查办法》（以下简称“审查办法”），要求关键信息基础设施运营者采购网络产品和服务，影响或可能影响国家安全的，应当进行网络安全审查。审查办法作为落实《网络安全法》第三十五条提出的网络安全审查制度的重要制度文件，将重点关注关键信息基础设施采购网络产品和服务可能带来的国家安全风险，确保关键信息基础设施供应链安全。

重要信息基础设施（软件）供应链安全涉及了网络产品和服务从无到有再到废弃的整个生命周期，不仅包含传统的生产、仓储、销售、交付等供应链环节，还延伸到产品的设计、开发、集成等生命周期，以及交付后的安装、运维等过程。本文件以网络安全审查制度为基础，为重要信息基础设施（软件）供应链安全检查评估提供标准，以确保能够建立安全可靠的重要信息基础设施（软件）供应链，保障国家安全、国计民生和公共利益。

重要信息基础设施（软件）供应链安全检查评估指南

1 范围

本文件规定了重要信息基础设施（软件）供应链安全检查评估的原则、内容和流程，并规范了检查评估活动及其工作任务。

本文件适用于行业监管部门或第三方等机构开展指导重要信息基础设施（软件）供应链安全检查评估工作，同时也适用重要信息基础设施运营单位开展软件供应链安全自查评估。

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 25069-2022 信息安全技术 术语

3 术语和定义

下列术语和定义适用于本文件。

3.1

重要信息基础设施 important information infrastructure

对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能危害国家安全、国计民生、公共利益的信息基础设施。

3.2

软件供应链 software supply chain

为满足供应关系通过资源和过程将需方、供方相互连接的网链结构，可用于将网络产品和服务提供给需方。

3.3

软件供应链安全 software supply chain security

软件供应链上软件设计与开发的各个阶段中来自本身的编码过程、工具、设备或供应链上游的代码、模块和服务的安全，以及软件交付渠道安全的总和。

3.4

检查评估 inspection assessment

由重要信息基础设施运营者自行发起或者由上级主管机关发起并委托安全服务机构进行的一项评估活动，其目的是依据国家有关法律法规和标准，对网络产品和服务的供应链安全状况进行检测评估。

［来源：GB/T 25069-2022，3.290，有修改］

3.5

需方 acquirer

从其他组织获取网络产品和服务的组织或个人。本文中的需方特指为重要信息基础设施运营单位。

3.6

供方 supplier

提供网络产品和服务的组织。

注 1：供方也可称供应商、供应方。

注 2：供方可以是内部或外部的组织。

4 检查评估原则

a） 标准性原则：重要信息基础设施（软件）供应链安全检查评估的实施方法严格遵循国际国内系列标准、 监管要求和最佳实践进行；

b） 规范性原则：整个过程按照项目实施规范进行，从项目资料、输出报告、实施人员及技术支持等方面应做到规范化管理；

c） 完整性原则：重要信息基础设施（软件）供应链安全检查评估的调研和所涉及的范围、内容均能够完整地覆盖软件供应链管理整个生命周期全过程；

d） 保密性原则：保密性原则是重要原则。对服务过程中获知的任何重要信息基础设施运营者系统信息均属秘密信息，不得泄露给第三方单位或个人，不得利用这些信息进行任何侵害重要信息基础设施运营者的行为；对服务的报告提交不得扩散给未经授权的第三方单位或个人；

e） 最小影响原则：评估中涉及技术评估工作应尽可能小地影响系统和应用的正常运行，不会对正常的运行和业务的正常提供产生显著影响。

5 检查评估内容

产品安全技术检测主要内容包括产品固件、源代码、运行基础环境等风险点的安全技术检测。

管理评估主要内容包括组织管理、流程与政策、供应商管理、人员管理、产品漏洞管理、源代码安全管理、产品安全开发管理和统一安全管理共 8 个方面。如表 1 所示，但不限于表 1 内容，可结合客户业务情况、侧重点进行增加。

表 1 管理评估主要内容

项目	内容
重要信息基础设施（软件）供应链安全检查评估	组织管理
	流程与政策
	供应商管理
	人员管理
	产品漏洞管理
	源代码安全管理

项目	内容
	产品安全开发管理
	统一安全管理

在进行内容评估时，宜使用具有多维度评估功能的工具，工具功能包括不限于支持对开源组件、市场采购、定制开发等类型的组件进行安全性测试。

6 检查评估流程

6.1 工作准备

工作准备活动的目标是明确检查评估对象，检查评估工作中需要使用到的工具，充分调研检查评估对象所属行业的相关标准及政策文件，确定检查评估工作任务。

输入：检查通知单模板。

任务描述：

a) 检查评估人员准备本次检查评估过程中将用到的工具，形成检查评估工具清单。其中技术检测工具包括但不限于软件组成分析工具、软件静态安全分析工具、软件动态安全测试工具、交互式应用安全测试工具、漏洞扫描工具等，管理评估工具包括但不限于各类调研表单、人员访谈纲要等。

b) 检查评估人员调试本次检查评估过程中将用到的所有工具，确保在现场检查评估活动中能够有效、准确、全面。

c) 检查评估组织方要求重要信息基础设施运营单位提供基本资料，初步了解被检查单位情况，包括但不限于被检查单位的基本情况、网络产品和服务等，并形成供应链软件产品清单（参考分类：开源软件、商用软件、自主研发软件）和供应商清单。

d) 对接重要信息基础设施运营单位安全管理机构和安全管理负责人，调研和梳理确定检查评估对象的必要资料，明确检查评估工作计划、范围及检查评估内容，下发检查通知单。

输出：检查评估工具清单、供应链软件产品清单、供应商清单、检查通知单。

6.2 方案编制

方案编制活动的目标是整理工作准备活动中获取的供应链软件产品清单和供应商清单，确定现场检查评估的具体对象，为现场检查评估活动提供最基本的文档和指导方案。

输入：检查评估工具清单、供应链软件产品清单、供应商清单。

任务描述：

a) 根据供应链软件产品清单中产品属性不同，包括市场采购、定制开发和开源组件等，明确检查评估对象，以及针对检查评估对象开展检查评估的具体指标，选取适合的检查评估工具。

b) 根据确定的检查评估对象和指标，形成现场检查表单。

c) 准备现场首次会相关文档资料，包括但不限于启动会 PPT、会议记录表单、会议签到表单等。

d) 形成检查评估方案。

输出：现场检查表单、现场首次会相关文档资料、检查评估方案。

6.3 现场检查

6.3.1 现场准备

现场准备活动的目标是确定现场检查工作计划并保障现场检查顺利实施。

输入：现场首次会相关文档资料、检查评估方案。

任务描述：

a) 召开检查评估现场首次会，介绍现场检查评估工作安排，相关方对检查评估计划和检查评估方案中的内容和方法等进行沟通。

b) 检查相关方确认现场检查需要的各种资源，包括检查评估配合人员和需要提供的检查评估环境等。

输出：现场首次会会议纪要、现场检查工作计划。

6.3.2 现场检查

现场检查活动的目标是依据检查评估方案实施现场检查评估工作，取得报告编制活动所需的、足够的证据和资料，所采用的方法包括软件产品技术检测和管理检查评估。

6.3.2.1 软件产品技术检测

软件产品技术检测的目标是运用多种技术手段，识别软件及其组件中存在的漏洞和风险。

输入：检查评估方案、现场检查表单。

任务描述：

a) 利用 SCA（Software Composition Analysis）软件成分分析技术，识别和清点开源软件的组件依赖清单，检测存在的已知安全漏洞及潜在的许可证授权风险，形成开源组件安全检测记录。

b) 利用 SAST（Static Application Security Testing）静态应用程序安全测试技术，检测软件源代码安全漏洞，形成软件静态安全检测记录。

c) 利用 DAST（Dynamic Application Security Testing）动态应用程序安全检测技术，发现软件及其运行环境存在的安全漏洞，形成软件动态安全检测记录。

d) 通过 IAST（Interactive Application Security Testing）交互式应用程序安全检测技术，发现软件存在的安全漏洞，形成软件交互式安全检测记录。

输出：软件组件安全检测记录、软件静态安全检测记录、软件动态安全检测记录、软件交互式安全检测记录。

6.3.2.2 安全管理评估检查

安全管理评估检查的目标是通过对被检查单位人员访谈及管理文档审查。

输入：检查评估方案、现场检查表。

任务描述：

a) 通过检查评估人员与被检查评估对象有关人员（个人/群体）进行交流、讨论等活动，获取相关证据，了解有关信息。检查软件供应链管理制度和流程的制定、执行、监督、维护情况，以及人员对本岗位相关的管理制度和流程的理解，形成管理调研访谈记录。

b) 通过调取软件供应链安全相关的组织管理、流程与政策、供应商管理、人员管理、产品漏洞管理、源代码安全管理、产品安全开发管理、统一安全管理的制度、策略、操作规程记录等文档是否齐备，形成管理文档审查记录。

输出：管理调研访谈记录、管理文档审查记录。

6.3.2.3 填写检查表

填写检查表的目标是对现场检查过程中获得检查记录进行分析，形成单项检查评估记录，为报告编制活动提供支撑。

输入：现场检查表、软件组件安全检测记录、软件静态安全检测记录、软件动态安全检测记录、软件交互式安全检测记录、管理调研访谈记录、管理文档审查记录。

——检查评估人员在现场检查评估取得过程输出结果后，还需对过程检查评估记录进行分析，填写单个检查评估项的检查证据。

输出：现场检查结果记录。

6.3.2.4 结果确认和资料归还

结果确认和资料归还的目标是对检查过程中得到的检查记录进行确认，并归还检查过程中借阅的文档。

输入：现场检查结果记录。

a) 召开检查评估现场结束会，检查评估双方对检查评估过程中得到的证据源进行现场沟通和确认。

b) 检查评估单位归还检查评估过程中借阅的所有文档资料，并由提供者签字确认。

输出：现场结束会会议纪要。

6.4 报告编制

报告编制活动的目标是对现场检查获得的各记录及现场检查表汇总分析，形成检查评估结论并编制报告。

输入：现场检查结果记录。

任务描述：

a) 分析单个检查评估项的检查证据，并与要求内容的预期结果相比较，给出单项检查评估结果和符合度判定。如果检查评估证据表明所有要求内容与预期结果一致，则判定该项的单项检查评估结果为符合；如果检查评估证据表明所有要求内容与预期结果不一致，判定该项的单项检查评估结果为不符合：否则判定该项的单项检查评估结果为部分符合。

b) 检查评估结果最终以报告的形式输出，形成检查评估报告。报告基本内容包括但不限于检查评估对象基本情况描述、检查评估结果说明。其中基本情况描述包括检查评估对象基本信息，检查评估结果的概括描述，对检查评估对象软件供应链安全状况的总体评价及主要建议；检查评估结果包括对现场检查评估的单项结果整体评估判定后的详细描述。

输出：安全检查评估报告见（附录 A）。

附 录 A
（资料性）
重要信息基础设施（软件）供应链安全检查评估（模板）

（一） 报告首页

内容应包括：

1、 报告名称

2、 组织单位

3、 实施单位

4、 时间

（二） 报告正文

内容应包括：

1、 检查评估总体情况

包括检查评估对象基本信息，检查评估结果的概括描述，对被检查评估单位软件供应链安全状况的总体评价及主要建议。

2、 软件产品技术检查评估结果说明

包括供应链软件产品清单，各产品安全物料清单，发现的安全问题说明和描述。

根据技术检查评估结果对重要信息基础设施（软件）供应链安全技术方面存在的主要安全威胁、安全漏洞和隐患进行说明，对产品技术检查评估中发现的具体安全问题进行描述。

例：软件产品技术检查评估发现的安全问题 XXX 的详细说明和描述。

3、 软件供应链管理检查评估结果说明

包括软件供应链管理检查评估总体介绍，检查评估结果说明。

a) 针对结果综合统计检查项的符合、不符合、部分符合、不适用的项个数。

b) 根据软件供应链管理检查评估结果，对重要信息基础设施（软件）供应安全管理方面存在的主要安全问题进行说明、总结该组织在软件供应链安全管理风险点进行描述。

例：本次管理检查评估结果综合统计如下：

符合：X 个

不符合：X 个

部分符合：X 个

不适用：X 个

1) 不符合项 XXX 的详细说明和描述

2) 部分符合项 XXX 的详细说明和描述

3) 不适用项 XXX 的详细说明和描述

……

根据以上安全检查评估结果，总结软件供应链管理存在的风险点如下：

1) XXX

2) XXX

……

4、 整改建议

针对被检查评估单位软件供应链安全的现状和问题，提出完善的软件供应链安全管理制度和技术防护措施的总体意见；针对检查评估中发现的具体问题，逐个提出解决措施建议。

参考文献

[1] GB/T 28448-2019 信息安全技术网络安全等级保护测评要求

[2] GB/T 36637-2018 信息安全技术 ICT 供应链安全风险管理指南

[3] 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

[4] GB/T 39204-2022 信息安全技术 关键信息基础设施安全保护要求