ICS 35.020
L 70

团　　体　　标　　准

T/GDCSA 00*—2022

重要信息基础设施供应链安全检查评估规范

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

2022－00－00 发布　　2022－00－00 实施

******* 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***提出。

本文件由***归口。

本文件起草单位：***。

本文件主要起草人：***。

本文件为首次发布。

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。

2020 年 4 月 27 日，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），要求重要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，将重点关注重要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，确保重要信息基础设施供应链安全。

重要信息基础设施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供应链，保障国家产业安全、经济安全和社会长治久安。

重要信息基础设施供应链安全检查评估规范

1 范围

本文件规定了重要信息基础设施供应链安全检查评估的依据与原则、评估流程、现场评估方法、评估内容与服务输出等内容。

本文件适用于开展指导重要信息基础设施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重要信息基础设施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，凡是标注日期的引用文件，仅注明日期的版本适用于本文件。凡是不注明日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 25069-2010 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指南

GB/T 37980-2019 信息安全技术 工业控制系统安全检查指南

信息安全技术 关键信息基础设施网络安全保护要求

20173587-T-469 信息安全技术 关键信息基础设施安全检查评估指南

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 critical 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，可能严重危害国家安全、国计民生、公共利益的信息设施。

3.2

供应链 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

安全检查 security inspection

以查代促、以查促改、以查促管、以查促防，旨在推动提高信息安全工作能力和防护水平。

3.4

评估 assessment

系统化的检验一个实体满足所规约的需求的程度。当用于可交付件时，与评价是同义。

4 评估依据与原则

4.1 评估依据

开展重要信息基础设施供应链安全检查评估需遵循的要求及标准，包括但不限于：

a) 填写《运营者供应链安全管理风险自查表》；

b) 遵循网络安全、网络安全审查相关法律法规；

c) 依照 GB/T 36637-2018、20173585-T-469 、20173587-T-469。

4.2 评估原则

a) 标准性原则：重要信息基础设施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客户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客户的行为；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的影响系统和应用的正常运行，不会对正在的运行和业务的正常提供产生显著影响。

5 安全检查评估流程

5.1 评估范围与目的

5.1.1 评估范围

基于重要信息基础设施开展网络产品和服务全生命周期评估，从产品测评、产品认证、供应商评估、安全审查等多项措施强化供应链安全管理。

5.1.2 评估目的

重要信息基础设施供应链安全检查评估旨在帮助企业了解其供应商，发现可能的第三方风险及自身管理缺陷问题，并提出相应的整改建议，加强供应链安全管理，防范供应链风险。

5.2 评估实施流程

5.2.1 前期沟通与资料收集

a) 信息沟通，资料收集。与被评估单位进行沟通进度安排，确定评估范围、评估方法和评估工作计划安排，了解被评估单位业务情况，获取评估所需制度文档、系统状况等相关资料信息。

b) 环境准备。对重要供应链产品准备技术检测涉及的环境，包括协调供应商准备测试环境，协调测试时间窗口等。

5.2.2 现场评估

现场评估分两个评估活动，分别为技术检测、管理评估：

a) 技术检测。主要通过代码审计、漏洞扫描、软件安全分析进行验证产品的安全性。
b) 管理评估。对第一阶段获取的制度文档进行文审，初步分析被评估单位供应链管理落实情况，并设计人员访谈的思路与问题，开展人员访谈及现场查看工作，评估供应链管理控制措施的有效性。

5.2.3 交付物输出

通过对产品安全技术检测和安全管理自查结果梳理，整理风险点列表，出具相关报告。

5.2.4 协助整改与监督检查支持

a) 协助整改。分析上一阶段交付物输出，对被评估单位提供整体建议，协助企业建立安全隐患整改方案。
b) 监督检查支持。为企业现场监督检查提供支撑。

6 现场评估方法

6.1 产品安全技术检测

6.1.1 代码审计

人工源代码审计（由具备丰富的安全编码及应用安全开发经验的人员，根据一定的编码规范和标准，针对应用程序源代码，从结构、脆弱性以及缺陷等方面进行审查）和工具源代码审计。

6.1.2 漏洞扫描

通过相应评估工具对企业供应链产品相关的脆弱性进行安全检查，以发现目标可能存在的安全隐患。

6.1.3 渗透测试

通过渗透测试，发现产品中存在的安全隐患。

6.1.4 软件安全分析

通过相应供应链安全分析系统，对开源组件及软件进行漏洞分析、后门分析，识别存在的漏洞、被植入的后门木马、访问的风险域名等问题。

6.2 管理评估

6.2.1 问卷调查

以电子邮件的方式向供应商发放供应商调查内容清单，收集供应商基本情况，了解和掌握供应商信息安全管理状况，识别其在开展项目活动重存在的风险点，同时为后续各阶段的工作提供基础数据与资料。

6.2.2 文档审查

通过对文档审查，了解供应链管理落实情况，对于标准中的要求，是否在制度流程上得以控制，特殊的业务要求是否明确说明原因等。

6.2.3 业务参与与风险梳理

根据供应商参与业务系统工作流程需求，整理出相应风险点列表，为人员访谈和技术检查做好准备。

6.2.4 人员访谈

对相关人员进行现场访谈，询问供应商工作中检查点内容是如何实现的，实现的具体要求及相关制度规定落实情况等。

6.2.5 控制措施有效性验证

针对部分重要检查点，通过对其进行制度文审、人员访谈外，还需要结合现场检查，确认该检查点是否与制度规定、人员访谈结果一致。对于现场检查工作（具体实施见 6.1 产品安全技术检测内容）评估控制措施的有效性，做出是否符合自查要求的最终判断。

7 评估内容与服务输出

7.1 评估内容

产品安全技术检测主要内容包括：对产品的销售许可证及其第三方安全检测的检查以及产品技术风险点检测。

管理评估主要内容主要包括：8 个模块、37 个细则。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
重要信息基础设施供应链评估	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
	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。

7.2 服务输出

重要信息基础设施供应链安全检查评估最终的输出物为：

a) 项目实施计划；
b) 重要信息基础设施供应链产品安全技术评估报告；
c) 重要信息基础设施供应链管理能力风险评估报告；

d) 重要信息基础设施供应链安全评估问题清单。

过程文档包括：《XX 系统漏洞扫描报告》、《XX 系统安全基线配置核查报告》、《XX 系统渗透测试报告》、《XX 代码审计报告》。