软件供应链安全保障能力分级测评

申请指南

二〇二五年四月

目　录

一、引言

中国信息安全测评中心（以下简称“测评中心”）是经中央批准成立、代表国家开展信息安全测评的职能机构，依据国家有关产品质量认证和信息安全管理的政策、法律、法规，管理和运行国家信息安全测评体系。

中国信息安全测评中心的主要职能是：

1. 为信息技术安全性提供测评服务；
2. 信息安全漏洞分析和信息安全风险评估；
3. 信息技术产品、信息系统和工程安全测试与评估；
4. 信息安全服务和信息安全人员资质测评；
5. 信息安全技术咨询、工程监理与开发服务；
6. 《中国信息安全》出版。

软件供应链安全保障能力分级测评是中国信息安全测评中心依据国家标准GB/T 43698-2024《网络安全技术 软件供应链安全要求》，通过访谈交流、文档分析、现场核查和技术检测等方式，对软件产品供应链全流程的组织管理能力和供应活动管理能力所开展的等级测评服务。

二、测评依据

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》，对申请单位的基本资格、软件产品的供应链组织管理能力和供应活动管理能力等方面进行综合评定后，由中国信息安全测评中心给予的能力等级认定。

三、等级划分

软件供应链安全保障能力分级测评是对软件产品供应链安全保障综合实力的客观评价，分级测评的测评对象是软件产品，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。各能力等级对应的安全保障能力如下。

一级：申请单位初步认识到软件供应链安全的重要性，在开展相应软件供应活动中，软件产品具备抵御一定软件供应链安全风险的能力。在组织管理方面，建立了基本的软件供应链安全保障策略和流程；在软件供应活动方面，具有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，软件产品能够防范一定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：申请单位充分认识到软件供应链安全的重要性，在开展相应软件供应活动中，软件产品具备抵御较强软件供应链安全风险的能力。在组织管理方面，建立了较完善的软件供应链安全保障机制；在软件供应活动方面，具有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，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。

三级：申请单位高度重视软件供应链安全，软件产品具备全面抵御软件供应链安全风险的能力。在组织管理方面，建立了完善的软件供应链安全保障体系；在软件供应活动方面，具有全流程软件供应链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，软件产品能够防范软件供应链技术风险、知识产权风险和供应中断风险。

四、测评要求

申请软件供应链安全保障能力分级测评的单位需要在基本资格、软件供应链组织管理能力、软件产品供应活动管理能力等几方面符合 GB/T 43698-2024《网络安全技术 软件供应链安全要求》及相应等级要求。

基本资格测评通过对申请单位基本情况的审核，确保申请单位为符合国家法律法规的独立法人实体，具有一定规模和开展软件供应活动的基础资源。组织管理安全测评共包括机构管理安全、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共包括基本流程安全、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、需方的基本测评内容和对应安全要求数量如如表 3-1 所示。但是，若供方在软件供应活动中涉及软件采购、软件外包等情况，需方涉及自主软件开发活动时，还需在基本测评内容外，增测与相应活动有关的测评内容，申请单位应在业务申请表中进行勾选。若测评过程中发现软件产品涉及基本测评内容外的其他测评内容但未主动申请时，将直接影响最终测评结果，相应后果由申请单位自行承担。

表 4-1　基本测评内容

序号	测评类型	基本测评内容	需方安全要求	供方安全要求
1	组织管理	机构管理安全	4	3
2		制度管理安全	6	5
3		人员管理安全	6	5
4		供应商管理安全	8	—
5		知识产权管理安全	3	2
6	供应活动管理	基本流程安全	3	3
7		软件采购安全	11	—

序号	测评类型	基本测评内容	需方安全要求	供方安全要求
8		软件开发安全	—	12
9		软件交付安全	—	12
10		软件获取安全	5	—
11		软件运维安全	12	8
12		软件废止安全	6	3

4.1 基本资格要求

申请单位应为符合国家法律法规的独立法人实体，具有处于有效期内的国家工商行政管理部门颁发的营业执照，未被列入信用中国网站严重失信名单、重大税收违法失信名单，具有一定规模和开展软件供应活动的基础资源，参与软件产品供应活动的主要人员应具备相关领域的工作经验、专业素养等。

4.2 组织管理安全基本能力要求

4.2.1 机构管理安全

1. 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；
2. 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；
3. 能及时制定、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。

4.2.2 制度管理安全

1. 具有软件供应链安全的总体方针、安全制度和策略；
2. 具有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；
3. 具有软件开发、交付、运维、废止等供应活动的安全管理制度；
4. 将软件供应链安全相关内容纳入人员管理制度，对于重要岗位人员明确并开展背景审查工作的要求；
5. 具有知识产权管理制度。

4.2.3 人员管理安全

1. 明确软件供应链安全技术人员需具备的实体要素的识别和安全分析能力；
2. 具有人员的职责定位和权限级别的划分规则，以及相关操作规范和操作记录；
3. 具备防范各类软件供应链安全风险能力；
4. 开展软件供应链安全和保密培训的情况；
5. 具有离职离岗人员的管理要求。

4.2.4 供应商管理安全

1. 具有分类分级的供应目录，能够定期或按需进行更新维护；
2. 优先选择供应目录中满足条件的供应商；
3. 根据供应关系、供应活动的不同，针对供方具有软件开发、交付、运维、废止等安全要求；
4. 具有供应商选择策略和制度，以及供应商风险分析记录；
5. 明确供方开展软件供应链安全检测和风险评估工作的要求；
6. 明确供方配合相关部门开展软件供应链安全审查、监督和检查的要求；
7. 在供应关系、供应商股权等信息发生变更时，具有相应的风险评估及控制措施等要求；
8. 具有供应商替代方案或具备相应软件的自主维护能力。

4.2.5 知识产权管理安全

1. 具有保障被测评软件相关知识产权不受侵犯的制度和策略；
2. 明确软件产品相关知识产权情况以及管理要求，以及如何防范知识产权风险。

4.3 供应活动安全基本能力要求

4.3.1 基本流程安全

1. 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；
2. 在协议、合同等文件中对供应活动提出安全要求，以及签署相应的保密协议；

3. 按照协议、合同等文件中约定的内容和范围开展软件供应活动。

4.3.2 软件开发安全

1. 开展软件开发的安全保障分析，或具备安全开发资质；
2. 将软件作为组织资产进行管理；
3. 构建软件供应链安全图谱；
4. 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；
5. 具有软件的安全需求基线和防护架构；
6. 保障软件所使用外部组件的安全；
7. 具有外部组件的使用审批机制；
8. 持续跟踪所使用的工具、外部组件的使用状态、安全状态；
9. 保障难以验证来源的工具、外部组件的安全；
10. 具有安全可控的软件开发工作场所和环境；
11. 保障开发/测试工具和设备的安全和可替代性；
12. 开展软件供应链安全检测和风险评估工作。

4.3.3 软件采购安全

1. 明确参与招标采购过程中，邀请具备软件供应链安全、网络空间安全能力的专家；
2. 明确供方提供软件供应链安全图谱内容的要求；
3. 具有软件安全需求基线和防护架构，符合国家和行业已发布标准以及自身业务要求；
4. 明确所采购软件的授权使用期限及相应的技术协助要求；
5. 具有从多个源厂商获得兼容的产品和服务的方案，或对于单一来源的软件，具有风险消减措施；
6. 对于定制研发软件，明确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、建立工具和设备的安全管理和准入控制等要求；
7. 明确供方提供验证产品是否来自原厂商且获得许可方法的要求；
8. 明确对运维技术团队及相应技术能力的要求；
9. 明确软件开发、交付、部署、测试等工具和设备具备替代方案的要求；

10. 具有不可抗力导致供应中断时的可替代策略；
11. 明确软件供应链安全检测和风险评估的范围。

4.3.4 软件获取安全

1. 具有软件完整性验证措施；
2. 开展全面的软件供应链安全检测和风险评估，确保所获取软件符合约定的安全要求；
3. 确保获取的软件不存在已公开漏洞未修复的情况，或要求供方及时修复或采取相应缓解措施；
4. 对于定制研发软件，明确关键软件、组件的代码结构和技术原理，具有软件源代码和相关知识产权的授权；
5. 具有软件相关技术资料。

4.3.5 软件交付安全

1. 保障交付软件的真实性、准确性、完整性；
2. 实行安全部署和配置；
3. 保障软件所使用外部组件的安全；
4. 开展所交付软件的功能、性能、完整性及安全性等验收测试；
5. 具有安全承诺，保证交付范围的安全性；
6. 具有交付途径的安全保障措施，在交付环节发生变化时具有安全分析报告；
7. 交付需方购买软件的使用授权；
8. 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；
9. 对于定制研发软件，应交付相应的技术资料；
10. 对于定制研发或者自主研制软件，具有安全保护措施保障技术资料的安全性；
11. 对软件分包、集成等工作的安全负责；
12. 开展全面的软件供应链安全检测。

4.3.6 软件运维安全

1. 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；
2. 能够协调软件原厂、供应商、集成商等共同开展软件运维工作；
3. 具有并维护可追溯台账，及时更新维护软件供应链安全图谱信息；
4. 针对授权即将到期或超过授权或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；
5. 定期开展软件供应链安全检测和风险评估；
6. 不可抗力导致供应中断时，具有应对措施，或在需方采用替代方案时能够给予协助；
7. 具有运维相关数据的安全管理措施；
8. 明确软件供应链运维人员对软件供应链的访问权限。

4.3.7 软件废止安全

1. 具有软件卸载、停用及数据备份、迁移、销毁等操作说明；
2. 具有防止软件泄露、数据泄露的安全保障能力；
3. 对于软件废止并替换为新软件的，具有软件数据迁移计划以及对废止软件进行安全处理的措施。

五、测评流程

5.1 总体流程

软件供应链安全保障能力分级测评业务分为业务申请、测评准备、测评实施和证书发放共四个阶段，如图 5-1 所示。

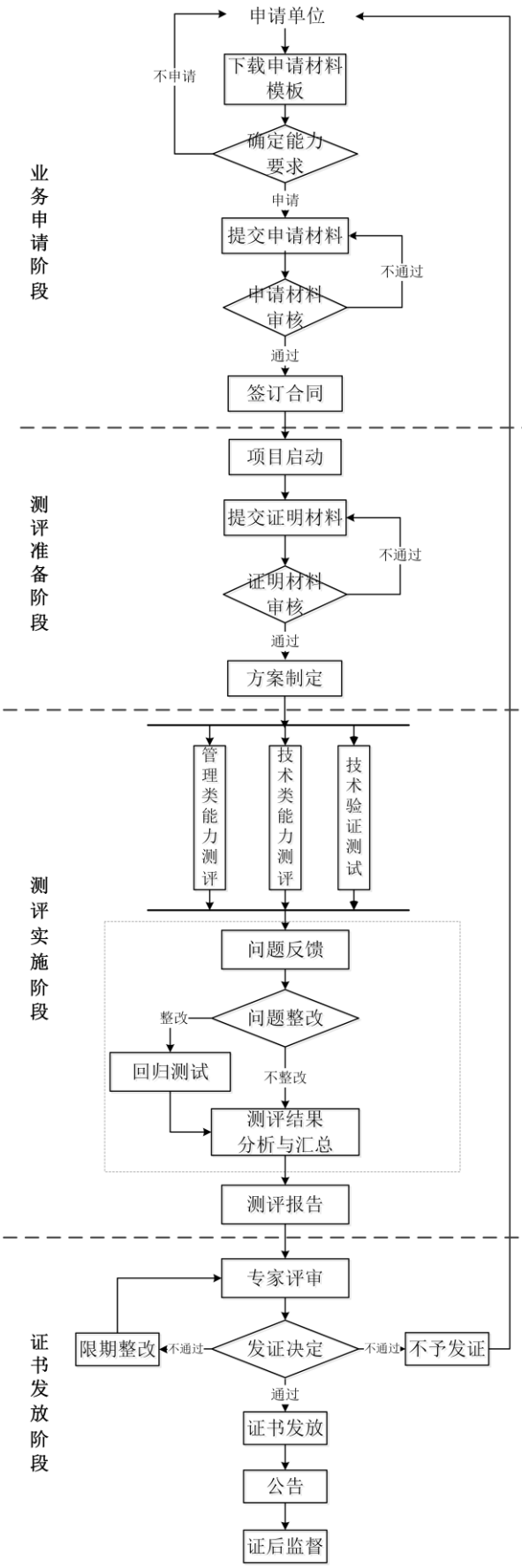
申请单位
下载申请材料模板
不申请
确定能力要求
申请
提交申请材料
不通过
申请材料审核
通过
签订合同
业务申请阶段
项目启动
提交证明材料
不通过
证明材料审核
通过
方案制定
测评准备阶段
管理类能力测评
技术类能力测评
技术验证测试
问题反馈
整改
问题整改
回归测试
不整改
测评结果分析与汇总
测评报告
测评实施阶段
专家评审
限期整改
不通过
发证决定
不通过
不予发证
通过
证书发放
公告
证后监督
证书发放阶段

图 5-1　业务流程图

5.2 业务申请

申请单位应首先到测评中心官方网站查看并下载《软件供应链安全保障能力分级测评申请书》、《软件供应链安全保障能力分级测评申请指南》及有关附件，对照测评要求，**准确填写软件产品基本信息、申请服务内容和申请等级**，以上信息与测评报告、等级证书有关内容一致，业务一旦成功受理后，**相关信息无法任意修改**。

申请单位向测评中心正式提交服务申请书及相关材料后，测评中心业务受理部门将对材料进行审核，并根据提交材料的实际情况提出反馈意见。申请方应根据反馈意见进行补充或修改。通过审核后，测评中心将执行受理审批流程，与申请方签订测评协议，并与申请单位进一步沟通费用缴纳、测评准备等事宜。

5.4 测评准备

合同签订后，测评中心将成立测评项目组，与申请单位对接项目启动事宜。申请单位需进一步提供全面详细的能力证明材料并开展测评准备。同时，测评人员将对申请单位已提交的材料进行技术审核，判定材料内容是否符合要求。若未通过审核，测评人员将提出反馈意见，待申请单位修改完善后，测评项目组将制定项目测评方案，启动测评实施工作。

5.4 测评实施

测评实施阶段主要完成管理类能力测评、技术类能力测评、技术验证测试、综合评定和专家评审等五方面工作。测评方案确定后，测评组将严格按照测评方案开展测评工作，必要时可要求申请单位提供技术支持或配合完成有关操作。测评过程中发现的属于申请单位的问题情况，测评组将出具问题通知单，并交由申请单位签字确认。

针对测评过程中发现的安全问题，申请单位可选择进行回归测试或者主动放弃权益。通常情况下，每次测评只有 1 次回归测试（合同中另行约定的除外）。如申请单位需进行回归测试，则应在收到回归测试通知单后及时反馈。超过合同约定次数或服务期限的回归测试，需申请方支付额外的费用，具体费用将根据发现问题的复杂或难易程度等核算工作量来收取，双方另行商议。

5.4.1 管理类能力测评

管理类能力测评是对申请书、证明材料等资料进行符合性审查，是对软件产品相关的软件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确定软件供应链组织管理能力水平状况。

5.4.2 技术类能力测评

技术类能力测评是对申请书、证明材料等资料中的供应活动管理能力做出基本判断，再通过现场核查等方式确定软件产品相关的软件供应活动管理能力水平状况。

5.4.3 技术验证测试

技术验证测试是为确认软件产品相关的软件供应安全检测技术能力和软件供应链安全图谱管理能力，通过执行一定的技术测试，进一步核实和确认软件产品供应活动中实现了相应的管理要求。在完成管理类和技术类能力测评后，测评中心将与申请单位沟通技术验证有关事宜，在条件许可的前提下，测评项目组对申请单位提供的源代码、软件等开展验证测试。

5.4.4 综合评定

在综合评定阶段，将依据管理类能力测评、技术类能力测评和技术验证结果，对软件产品的供应链组织管理能力和供应活动管理能力，以及测评所要求的其他内容进行分析与汇总，反馈初步测评结果。

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。

5.4.5 专家评审

测评中心将组织技术专家对测评报告及相关材料进行评审，就申请单位软件产品的供应链安全保障能力的测评结果进行评议，并最终做出是否通过的决定。

5.5 证书发放

测评结果在通过专家评审并准予发证后，测评中心将开展等级证书的制作、

审批和发放，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。

六、资料提交说明

申请本项业务时，申请单位须提交《软件供应链安全保障能力分级测评申请书》及相关材料。针对申请书中要求的第七项：“必要的证明材料”，如材料涉及申请单位内部敏感信息，在业务受理阶段，申请单位可仅提供材料清单；成功受理后，再向测评中心提供具体材料。

七、证后监督

软件供应链安全保障能力等级证书的有效期为 3 年，申请单位在获得软件供应链安全保障能力等级证书后，仍需持续完善软件供应链安全保障体系，以保障目标软件具有相应等级的软件供应链安全风险防范能力。证书有效期内，测评中心将根据工作安排，对已获证的软件产品及申请单位进行不定期的抽样检查，确保软件产品的供应链安全保障能力。

一旦发现已获证软件产品的申请单位存在违法违规、不履行软件供应链安全保障要求的保障措施等情况时，测评中心有权视申请单位违规情节轻重予以以下处置：警告、限期整改、取消证书等。

八、申诉与投诉

任何组织或个人若对测评中心所作的测评过程、测评结果、测评报告等有异议时，可向测评中心提出书面申诉。申诉内容经测评中心初步审查确认有效后，测评中心将会组织与所申诉、投诉事项无利益相关的人员进行调查，并在调查基础上做出处理。

测评中心若收到针对已获证单位的投诉时，一经核实，将视投诉情况的严重程度及时予以处理，并保留不再向有关单位予以发放相关等级证书的权利，有关投诉情况和处理结果将告知被投诉单位。被投诉单位应妥善处理因自身不当行为而发生的投诉，保留相关记录并采取有效措施予以应对，测评中心将在必要时查阅被投诉单位的投诉记录。

九、获证单位档案

测评中心将针对每个获证单位建立相关档案，项目资料将保存 10 年。

十、费用及周期

软件供应链安全保障能力分级测评业务采用分等级收费的方式，不同等级所需的测评周期和测评费用不同，正常情况下，各测评等级对应的测评周期和服务报价如表 10-1 所示。其中，测评周期为参考时间，受企业规模、软件产品复杂程度、问题整改等因素影响，存在较大的不确定性，且因申请方原因（如资料补充需要的时间，或因测评项整改等）而造成的时间延误不计算在测评周期内。

表 10-1 测评费用与周期

服务内容	测评周期	服务报价
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

十一、联系方式

名　称：中国信息安全测评中心资质评估处

地　址：北京市海淀区上地西路 8 号院 1 号楼（邮编：100085）

咨询电话：010－82341582 或 82341551

中心网站：http://www.itsec.gov.cn

服务资质公众号：国家信息安全服务资质