ICS 35.240.01
L70

团　　体　　标　　准

T/ISC 0019—2022

移动互联网应用程序（App）数据安全测评服务机构能力评定准则

Capability determination criteria for mobile Internet applications data security assessment service organization

2022－11－01 发布　　2023－02－01 实施

中　国　互　联　网　协　会　　发 布

目　　次

前　言

本标准按照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这些专利的责任。

本标准由中国互联网协会归口。

本标准主要起草单位：中国信息通信研究院、中国电子技术标准化研究院、中国软件评测中心、国家工业信息安全发展研究中心

本标准主要起草人：王丹辉、解伯延、谢玮、魏薇、陈湉、刘行、高超、唐刚、秦晓磊、余宇舟、张渊、秦博阳、钟子呈

移动互联网应用程序(App)数据安全测评服务机构能力评定准则

1 范围

本标准针对移动互联网应用程序数据安全测评服务机构的基本条件、规模与资产、人员构成和素质、经验业绩、组织与管理、质量保证、项目管理、技术能力、专业培训等方面，进行了基线统筹和细化明确，为机构资格评定的申请、评审、监督管理等流程与日常管理事项实施提供指引。

本标准适用于对开展App数据安全测评的服务机构进行能力资格评定。

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。

《通信网络安全服务能力评定管理办法》

规范性文件 《App违法违规收集使用个人信息行为认定方法》

GB/T 35273—2020 《信息安全技术 个人信息安全规范》

GB/T 37988—2019 《信息安全技术 数据安全能力成熟度模型》

YD/T 2669—2013 《电信网和互联网第三方安全服务能力评定准则》

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本文件。

3.1.1 移动互联网应用程序 mobile internet Application

安装、运行在智能移动终端上的应用程序。

3.1.2 数据安全 data security

通过管理和技术措施，确保数据有效保护和合规使用的状态。

[来源：GB/T 37988—2019，定义 3.1]

3.1.3 个人信息 personal information

以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息。

[来源：GB/T 35273-2020，定义 3.1]

3.2 缩略语

下列缩略语适用于本文件。

App 移动互联网应用程序 mobile Internet Application

CISP 注册信息安全专业人员 Certified Information Security Professional

CISSP 信息系统安全专业认证 Certification for Information System Security Professional

PMP 项目管理专业人士资格认证 Project Management Professional

CPMP 中国项目管理师 China Project Management Division

4 能力评定原则

App数据安全测评服务能力是对App数据安全测评服务机构的客观评价，直接反应了服务机构的资格、水平和能力。

App数据安全测评服务能力评定要求是对App数据安全测评服务机构的资格状况、经济实力、技术水平、管理能力、服务队伍等方面的具体衡量和评价。

5 能力评定评审机构

组建能力评定评审机构，负责App数据安全测评服务机构资格及能力等级进行评定、开展培训考试及日常管理工作。能力评定评审机构成员由各相关单位App数据安全、法务领域专家组成，专家至少来自3家不同单位，人数不少于5名。

6 能力评定要求

6.1 基本条件

申请App数据安全测评服务机构能力评定的服务机构应具备的基本条件包括：

a) 在中华人民共和国境内注册成立(港澳台地区除外)。
b) 由中国公民投资、中国法人投资或者国家投资的，具有独立法人资格及相关部门颁发的合法经营资格的企事业单位(港澳台地区除外)。
c) 从事涉密服务的机构须满足国家保密机关的相关要求。
d) 近 3 年经营状况良好，财务数据真实可信，可提供在中华人民共和国境内登记注册的会计师事务所出具的近三年财务审计报告。
e) 法人及主要业务、技术人员无违法犯罪记录。
f) 拥有健全的组织机构和管理体系，有专门从事 App 数据安全测评服务的部门或团队；配备相应的 App 数据安全测评专业人员。
g) 具有固定的办公场所。

6.2 规模与资产要求

6.2.1 C 级

a) 单位正式编制员工应不少于 15 人；
b) 产权关系明晰，注册资金（或开办资金）实缴不少于 100 万元人民币。

6.2.2 B 级

a) 单位正式编制员工应不少于 50 人；
b) 产权关系明晰，注册资金（或开办资金）实缴不少于 500 万元人民币。

6.2.3 A 级

a) 单位正式编制员工应不少于 100 人；
b) 产权关系明晰，注册资金（或开办资金）实缴不少于 3000 万元人民币。

6.3 人员构成和素质要求

6.3.1 C 级

a) 了解 App 安全基本情况、数据安全和个人信息安全法律法规要求、相关标准，承接过 App 安全测评相关服务项目或撰写过相关研究报告；
b) 从事 App 安全相关工作的人员至少 10 名，其中大学本科以上学历不少于 50%；
c) 专职从事 App 数据安全测评服务的人员至少 5 名，至少应有 2 名具备 2 年以上测评经验的专业人员；
d) 建议 2 名以上专业人员具备 CISP、CISSP 等相关资质（非必要）。

6.3.2 B 级

a) 了解 App 安全基本情况、数据安全和个人信息安全法律法规要求、相关标准，承接过 App 安全测评相关服务项目或撰写过相关研究报告；
b) 从事 App 安全相关工作的人员至少 20 名，其中大学本科以上学历不少于 70%；
c) 专职从事 App 数据安全测评服务的人员至少 8 名，至少应有 3 名具备 2 年以上测评经验的专业人员；
d) 具有 App 安全和个人信息安全相关规范或标准编制经验人员至少 1 名；
e) 建议 2 名以上专业人员具备 CISP、CISSP 等相关资质（非必要）。

6.3.3 A 级

a) 了解 App 安全基本情况、国内外数据安全和个人信息安全法律法规要求、相关标准、发展趋势，承接过 App 安全测评相关服务项目或撰写过相关研究报告；
b) 从事 App 安全相关工作的人员至少 30 名，其中大学本科以上学历不少于 90%；
c) 专职从事 App 数据安全测评服务的人员至少 12 名，至少应有 5 名具备 2 年以上测评经验的专业人员；
d) 具有 App 安全和个人信息安全相关规范或标准编制经验人员至少 3 名；
e) 建议 3 名以上专业人员具备 CISP、CISSP 等相关资质（非必要）。

6.4 经验业绩要求

6.4.1 C 级

a) 应具备 1 年以上的 App 测评业务实践经验；

b) 近 2 年间完成 5 次以上 App 测评、咨询类相关服务（可依据合同或测评报告）；
c) 近 1 年没有出现因各阶段验收未通过或企业自身原因而废止的测评服务项目。

6.4.2 B 级

a) 应具备 2 年以上的 App 测评业务实践经验；
b) 近 2 年间完成 10 次以上 App 测评、咨询类相关服务（可依据合同或测评报告）；
c) 至少有 3 个涉及 App 测评、咨询等相关服务内容、金额超过 10 万元人民币的项目，或至少承接过行业主管部门委托的 1 项相关支撑或研究任务（可依据合同或任务书）；
d) 近 2 年没有出现因各阶段验收未通过或企业自身原因而废止的测评服务项目。

6.4.3 A 级

a) 应具备 2 年以上的 App 测评业务实践经验；
b) 近 2 年间完成 15 次以上 App 测评、咨询类相关服务（可依据合同或测评报告）；
c) 至少有 6 个涉及 App 测评、咨询等相关服务内容、金额超过 10 万元人民币的项目，或至少承接过行业主管部门委托的 2 项相关支撑或研究任务（可依据合同或任务书）；
d) 近 2 年没有出现因各阶段验收未通过或企业自身原因而废止的测评服务项目。

6.5 组织与管理要求

6.5.1 C 级

a) 具有健全的组织与管理体系；
b) 建立人员管理程序，明确岗位与职责，定期对测评服务人员进行教育培训。

6.5.2 B 级

a) 具有专门从事 App 安全测评服务的部门或团队。
b) 对项目实施过程中获取、保存、传播和销毁商业秘密信息等方面作出明确规定。

6.5.3 A 级

a) 具有专门从事 App 安全测评服务的部门或团队，并成立 2 年以上。
b) 具有专门制定和宣贯保密制度的部门或团队，对项目实施过程中涉及处理商业秘密信息的全过程有明确且行之有效的控制手段。

6.6 质量保证要求

6.6.1 C 级

a) 建立并落实质量管理办法；
b) 能够自行评估服务质量的状况，并能对服务质量进行持续改进；
c) 建立相关投诉、应急响应服务机制。

6.6.2 B 级

a) 配备专职部门或人员制定质量保证体系，针对质量管理建立宣传及培训机制。
b) 质量体系应针对项目开始至项目结束各个环节，设立准确有效且较为完善的控制手段。

6.6.3 A 级

a) 参照 ISO27001 标准、GB/T 22080-2016 标准制定完善的信息安全管理体系规范，或者参照 ISO9001 标准、GB/T 19000-2016 标准制定完善的质量管理体系规范。
b) 配备专职部门或人员制定完整的质量保证体系，针对质量管理建立宣传及培训机制，具备完善且行之有效的控制手段。

6.7 项目管理要求

6.7.1 C 级

a) 具有成文的项目管理办法，并符合相关项目管理标准；
b) 项目管理过程记录完整、可追溯。

6.7.2 B 级

a) 建立项目管理体系，并配备制度宣传和培训机制；
b) 项目管理体系应针对人和项目有明确的责权分工，有比较明确和完善的项目过程控制记录；
c) 建议 1 名以上专业人员具备 PMP、CPMP 等相关资质（非必要）。

6.7.3 A 级

a) 项目管理制度应对项目立项、审批过程有明晰表述；
b) 项目管理制度应对项目过程有控制方法或有依据标准，应有对过程中发生的项目变更或变化进行管理的手段；
c) 项目管理制度应对项目完成后的审计、验证、考核等内容有管理办法；
d) 具备项目管理制度落实的证据，可以但不限于电子文档、会议记录、过程管理表格等。
e) 建议 2 名以上专业人员具备 PMP、CPMP 等相关资质（非必要）。

6.8 技术能力要求

6.8.1 C 级

a) 初步具备 App 数据安全风险测评能力，能够对 App 权限调用行为、数据传输情况、本地数据加密存储等进行分析；
b) 具备依据《App 违法违规收集使用个人信息行为认定方法》进行 App 个人信息安全测评的能力；
c) 具有能够进行 App 安全测评的相关工具，并具备相应的使用能力；
d) 具有进行 App 安全测评所必须的实验环境。

6.8.2 B 级

a) 具备基础级 App 数据安全风险测评能力，应覆盖但不限于《移动互联网应用程序（App）数据安全测评能力要求》要求的源文件安全、数据存储安全、数据交互安全、数据安全防护机制基础级测评内容；
b) 具备依据《App 违法违规收集使用个人信息行为认定方法》进行 App 个人信息安全测评的能力；
c) 具有专门进行 App 安全测评的相关工具且通过能力评定评审机构评定；
d) 具有进行 App 安全测评所必须的实验环境。

6.8.3 A 级

a) 具备 App 数据安全测评风险能力，应覆盖但不限于《移动互联网应用程序（App）数据安全测评能力要求》要求的源文件安全、数据存储安全、数据交互安全、数据安全防护机制全部测评内容；
b) 具备依据《App 违法违规收集使用个人信息行为认定方法》进行 App 个人信息安全测评的能力；
c) 具备对 App 数据安全风险、个人信息安全问题进行跟踪和研判，及时优化 App 测评方案的能力。
d) 具有较为完善的自动化测评工具，覆盖 App 安全及个人信息安全主要测评需求，且通过能力评定评审机构评定；
e) 具有进行 App 安全测评所必须的实验环境。

6.9 专业培训要求

6.9.1 C 级

a) 具有系统的对员工进行法律法规、安全技术、项目管理、保密规章制度的培训机制和计划，并能有效组织实施与考核。
b) 专职从事 App 数据安全测评的人员定期参加培训。每年保证不少于 20 学时，有明确过程记录。培训后通过考试的人员人数占全量的 40%以上。

6.9.2 B 级

专职从事 App 数据安全测评的人员定期参加培训。每年保证不少于 30 学时，有明确过程记录。培训后通过考试的人员人数占全量的 60%以上。

6.9.3 A 级

专职从事 App 数据安全测评的人员定期参加培训。每年保证不少于 40 学时，有明确过程记录。培训后通过考试的人员人数占全量的 80%以上。

6.10 禁止性要求

不具有申请 App 数据安全测评服务机构资格的情况包括：
a) 经营状况不良，无法提供专业机构出具的财务审计报告。
b) 近三年内企业有违法违规记录，相关监管部门有公示记录。
c) 近三年因 App 安全测评服务质量因素导致安全事件，被主管部门通报或遭到客户投诉未能妥善解决的。
d) 从事 App 安全测评服务的人员有违法违规操作记录，并遭到法律制裁或客户投诉未能妥善解决的。
e) 近三年内存在其他未被能力评定评审机构认可的整改效果不良记录。

7 能力评定申请

7.1 能力评定等级申请

App数据安全测评服务能力分为三个级别，由低到高依次是C级、B级、A级能力。在本标准中，高等级能力的评定要求涵盖了低等级能力评定要求的所有方面，符合较高等级能力评定要求可不经通过较低能力评定直接申请。

符合能力评定要求中所有C级条款要求，可申请评定为C级App数据安全测评服务机构。

符合能力评定要求中所有B级条款要求，可申请评定为B级App数据安全测评服务机构。

符合能力评定要求中所有A级条款要求，可申请评定为A级App数据安全测评服务机构。

7.2 申请材料提交

申请App数据安全测评能力评定的服务机构可对照能力评定级别，向能力评定评审机构提交正式申请材料，包括：

a) 《App 数据安全测评服务机构能力评定申请书》。

b) 《企业法人营业执照》或《事业单位法人登记证书》复印件、组织机构代码证复印件、税务登记证复印件（如已完成“三证合一”工作的，提交加载统一社会信用代码的新版营业执照复印件）。

c) 法人代表或负责人身份证复印件。

d) 固定办公场所证明材料。

e) App 安全测评服务组织管理、经验业绩、技术能力、项目管理、质量保证及保密等方面能力证明材料。

f) 配备的专职业务 App 数据安全测评人员情况说明。

以上申请材料除提交纸质版本以外，还需通过App数据安全测评能力开放平台在线提交电子版申请材料。如上述要求的申请材料形式（纸质版本和电子版本）之一缺失，视作申请单位未提交申请。

7.3 预审与意见反馈

能力评定评审机构对提交的能力评定申请材料进行预审，于三十个工作日内反馈预审意见。对于通过预审的申请机构，正式启动能力评定评审。

8 能力评定评审

8.1 评审原则

能力评定评审机构应当遵循客观公正、科学准确、统一规范和避免不必要重复的原则组织开展能力评定评审工作。

8.2 培训

通过App数据安全测评服务机构能力评定预审的申请单位，向能力评定评审机构申请进行培训及考评。能力评定评审机构联合有关单位对通过申请预审的App数据安全测评服务机构开展培训，培训内容包括通信行业主管部门工作要求、测评标准、操作实施流程、测评工具使用、报告编制等。

8.3 考评

培训结束后，由能力评定评审机构联合有关单位对App数据安全测评服务机构进行能力考评。具体形式包括书面与现场考评。考评通过的机构人员有权在App数据安全测评报告上签字。

a) 书面考评主要是考察App数据安全测评服务机构对App数据安全测评相关工作及要求的知悉程度，包括通信行业主管部门工作要求、测评标准、操作实施流程、报告编制等内容。

b) 现场考评主要是 App 数据安全测评服务机构实际开展相关业务 App 数据安全测评的能力，包括人员操作使用评估工具熟练度、评估流程实施的规范程度等内容。

8.4 评审合格标准

书面考评与现场考评均采用百分制计分，六十分及格。书面与现场考评均及格，视为通过评审。

8.5 结果公示

能力评定评审机构根据预审结果和考评成绩做出评定决定，向通过评审的App数据安全测评服务机构颁发《App数据安全测评服务机构能力评定书》（以下简称《能力评定书》），并将有关结果予以公示，公示期为三个工作日，任何组织或个人对公示的情况有异议的可以在公示期内将书面意见(加盖公章)反馈至工作组。

9 能力评定监督管理

9.1 能力评定监督的频次和方式

能力评定评审机构对获得《能力评定书》的App数据安全测评服务机构进行监督管理。管理方式包括对测评服务机构提交的材料进行监督评审与现场测评能力监督评审。管理频度为所有等级每年度（不超过12个月）进行一次材料监督评审，A级及以上每两年进行一次现场监督评审，B级、C级每三年进行一次现场监督评审。当获得能力评定的机构发生重大变更、事故或客户投诉时，可增加现场监督评审的频次。

9.2 能力评定监督的结论

对于通过能力评定监督评审的App数据安全测评服务机构，做出维持原能力评定等级《能力评定书》有效的决定；否则，视不达标情况，做出降低能力评定等级、暂停或撤销《能力评定书》的决定。

9.3 《能力评定书》管理

9.3.1 《能力评定书》有效期

能力评定等级为A级的，《能力评定书》有效期为两年。能力评定等级为B级或C级的，《能力评定书》有效期为三年。在《能力评定书》有效期期间，获得《能力评定书》的数据安全评估服务机构如持续满足本标准要求，且通过监督评审的，可保持证书有效。

9.3.2 《能力评定书》续期申请

申请能力评定资质续期的App数据安全测评服务机构在《能力评定书》到期前三个月内完成申请，应提交以下审查材料：

a) 近两年间受托开展的 App 数据安全测评服务的报告。
b) App 数据安全测评服务机构的评估人员配备与变更情况、开展培训情况、与评估相关的软硬件能力条件变更情况等。

能力评定评审机构于三十个工作日内反馈评审意见，因续期评审流程延长导致《能力评定书》超出有效期的，在续期评审完成前，App数据安全测评服务机构可正常使用《能力评定书》开展App数据安全测评服务。

对于通过能力评定监督评审的App数据安全测评服务机构，能力评定评审机构做出维持原能力评定等级《能力评定书》有效或升高能力评定等级的决定；否则，视不达标情况，做出降低能力评定等级、

暂停或撤销《能力评定书》的决定。能力评定评审机构按照续期情况为App数据安全测评服务机构更换《能力评定书》，并予以公示。

若获得能力评定的App数据安全测评服务机构对组织机构变更、安全事故情况或客户投诉信息进行隐瞒，将取消续期资格。

9.3.3 暂停《能力评定书》

获得能力评定的App数据安全测评服务机构有下列情形之一，能力评定评审机构暂停其《能力评定书》：

a) 未按规定接受监督评审；
b) 违规使用《能力评定书》，且造成不良影响；
c) 监督评审中发现严重不达标项；
d) 未及时向能力评定评审机构报备组织机构等变更情况、安全事故情况、客户投诉信息及其他重大情况。

《能力评定书》暂停时间一般为三个月。在暂停期间，数据安全评估服务机构可提出恢复证书的申请，并经能力评定评审机构审核、批准后方可使用证书。

9.3.4 撤销《能力评定书》

获得能力评定的App数据安全测评服务机构有下列情形之一，能力评定评审机构撤销其《能力评定书》：

a) 《能力评定书》暂停期间，未在规定时间内完成整改并通过审核；
b) 违规使用《能力评定书》，造成重大不良影响；
c) 出现严重责任事故、被投诉且经核实，造成重大不良影响；
d) 其他需要撤销《能力评定书》的情况。

《能力评定书》撤销后，App数据安全测评估服务机构应交回《能力评定书》，能力评定评审机构予以公示。

9.3.5 注销评定证书

获得能力评定的App数据安全测评服务机构因自身原因不再维持《能力评定书》，可提出注销《能力评定书》的申请，能力评定评审机构应及时给予注销。

《能力评定书》注销后，App数据安全测评服务机构应交回《能力评定书》，能力评定评审机构予以公示。

10 行为规范

10.1 申请移动互联网应用程序（App）数据安全测评服务机构行为规范

申请能力评定的移动互联网应用程序（App）数据安全测评服务机构在预审及评审环节应遵守公平竞争原则，不得提供虚假信息，不得对能力评定评审机构进行贿赂。

10.2 能力评定评审机构行为规范

能力评定评审机构在能力评定评审过程中应严格遵循本标准要求；在实施监督管理过程中不得玩忽职守、滥用职权、徇私舞弊；不得以任何理由或者方式向App数据安全测评服务机构收取费用或者变相收取费用。

10.3 移动互联网应用程序（App）数据安全测评机构行为规范

移动互联网应用程序（App） A/B/C级数据安全测评机构，应在对App测评后，及时将测评结果反馈到互联网协会，通报给电信运营商。

11 其它相关要求

11.1 针对数据安全测评服务机构

能力评定过程中，App数据安全测评服务机构有违反本标准10.1所述行为而被举报投诉，且经能力评定评审机构核查确实存在过错的，则对该App数据安全测评服务机构和相关人员进行通报批评，情节严重或拒不整改的，将取消能力评定评审资格。

获得能力评定后，App数据安全测评服务机构没有按照相适应的能力等级进行App数据安全测评服务，造成严重安全事件或被电信管理机构投诉、检查发现重大问题的，给予暂停使用《能力评定书》三至六个月、降级、直至撤销《能力评定书》的处罚。

获得能力评定后，App数据安全测评服务机构应正确使用《能力评定证书》，对于涂改、伪造、出借、转让或出卖《能力评定书》的将给予警告、暂停使用或撤销《能力评定证书》的处罚；情节严重涉嫌犯罪的，由相关部门追究其法律责任。

11.2 针对能力评定评审机构

在能力评定过程中，若能力评定评审机构成员有违反本标准10.2所述行为而被举报投诉，且经核查确实存在过错的，由所在单位给予警告或行政处分；情节严重涉嫌犯罪的，由相关部门追究其法律责任。