ICS 35.240.99
CCS L67

T/CCIASC

中 国 计 算 机 行 业 协 会 团 体 标 准

T/CCIASC 0029—2024

数据安全评估服务能力评定规范

Specification for Capability Evaluation of Data Security Assessment Services

2024－12－20 发布　　2024－12－27 实施

中国计算机行业协会　　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。

本文件由中国计算机行业协会提出。

本文件由中国计算机行业协会归口。

本文件起草单位：中国软件评测中心（工业和信息化部软件与集成电路促进中心）、中国电信股份有限公司安徽分公司、联通数字科技有限公司、联通在线信息科技有限公司、亚信科技（成都）有限公司、北京卓识网安技术股份有限公司、重庆市软件评测中心有限公司、恒安嘉新（北京）科技股份公司、北京明朝万达科技股份有限公司、中科信息安全共性技术国家工程研究中心有限公司、上海斗象信息科技有限公司、北京市京都律师事务所、中核核信信息技术（北京）有限公司 、北京金源动力信息化测评技术有限公司、天津郎言安全技术服务有限公司、北京君云天下科技有限公司、上海胡桃网络科技有限公司、贵州企信科技有限公司、河北翎贺计算机信息技术有限公司。

本文件主要起草人：王文鑫、林海静、王露颖、曹顺超、王翔宇、张嘉欢、仇必青、徐灏、林海、李冰、刘宁、张文、黄亚洲、陈杰、王学清、丁晓明、郑旭飞、刘新鹏、喻波、伊鹏达、王庆贺、谢忱、王菲、张士莹、曹涛、赵亮、张靖、方新、李能言、胡耀军、王一、任寅。

引　言

数据安全评估服务有助于强化我国重要数据和核心数据的保护能力，保障数据持续处于有效保护、合法利用、有序流动的状态，提升各行业各领域数据安全水平，加速数据要素市场培育和价值释放。当前，很多单位正在开展数据安全评估业务，但数据安全评估服务能力参差不齐，不利于数据安全评估服务市场的健康发展和数据安全标准的有效落地。本文件通过强化对数据安全评估机构的基本要求和分类要求，从核心技术能力、持续经营能力、评估管理能力3个维度进行统一分级、判定，意在构建统一规范的数据安全评估服务能力评定体系，制定有效的数据安全评估服务能力评定规范及配套评定方法。

数据安全评估服务能力评定规范

1 范围

本文件给出了数据安全评估服务能力评定的基本要求、指标框架、评定流程及评定方法。

本文件既适用于第三方能力评定机构，对其开展的数据安全评估服务能力评定工作提供指引，也适用于数据安全评估服务提供商开展服务能力自评定，为提升其数据安全评估服务能力提供参考。

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。

GB/T 22080 信息技术 安全技术 信息安全管理体系

GB/T 25069 信息安全技术 术语

GB/T 41479 信息安全技术 网络数据处理安全要求

JGJ/T 67 办公建筑设计标准

YD/T 3956 电信网和互联网数据安全评估规范

T/ZHTEA 001 高新技术企业创新能力评价

3 术语和定义

GB/T 25069、GB/T 41479、T/ZHTEA 001中界定的以及下列术语和定义适用于本文件。为了便于使用，以下重复列出了GB/T 25069、GB/T 41479、T/ZHTEA 001中的某些术语和定义。

3.1

数据安全 data security

通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

注：引自GB/T 41479—2022，定义3.4

3.2

风险管理 risk management

指导和控制组织相关风险的协调活动。

注：引自GB/T 25069—2022，定义3.168

3.3

服务工具 service tools

为达成服务目标或提高服务质量和效率所需要的设备、软件、模板、知识库等。

注：引自GB/T 25069—2022，定义3.184

3.4 **丨类知识产权 Class 丨 Intellectual Property**

发明专利（含国防专利）、植物新品种、国家级农作物品种、国家新药、国家一级中药保护品种、集成电路布图设计专有权等。

注：T/ZHTEA 001—2023，定义3.1

3.5 Ⅱ类知识产权 Class Ⅱ Intellectual Property

实用新型专利、外观设计专利、软件著作权等。

注：T/ZHTEA 001—2023，定义3.2

4 评定原则

a）公正性：评定工作以数据安全评估服务商实际情况为基础，通过系统、深入的分析得出客观、公正的评定结论；

b）透明性：评定过程公开透明，评定结论向社会公开。

5 评定基本要求

数据安全评估服务提供商应具备的基本要求包括：

a) 在中华人民共和国境内注册成立，由中国公民、法人投资或者国家投资的企事业单位；
b) 产权关系明晰，注册资金500万元以上，独立经营核算，无违法记录；
c) 法定代表人、技术负责人、质量负责人、主要技术人员应为中华人民共和国境内的中国公民，且无犯罪记录；
d) 未被列入失信被执行人、重大税收违法案件当事人名单和政府采购严重违法失信行为记录名单等，以及其他可能影响数据安全评估服务提供商能力和信誉的负面清单；
e) 应建立工作保密制度及相应组织监管体系，从事涉密的数据安全服务应满足国家保密机关相关要求；
f) 应具备固定办公地点，且满足JGJ/T 67-2019相关要求；
g) 电信和互联网数据安全评估服务的实施应满足YD/T 3956-2021的第4-6章相关要求。

6 评定指标框架

从核心技术能力、持续经营能力、评估管理能力3个维度分别对数据安全评估服务提出了2级能力要求，由高到低依次是二级、一级能力。其中，核心技术能力的评定指标包括人才基础、知识产权情况、技术转化能力、评估工具水平等；持续经营能力包括管理者能力、单位资质奖励、市场占有能力、盈利能力等；评估管理能力包括人员管理、方案管理、质量管理、风险管理、评估工具使用管理、成果物管理等。

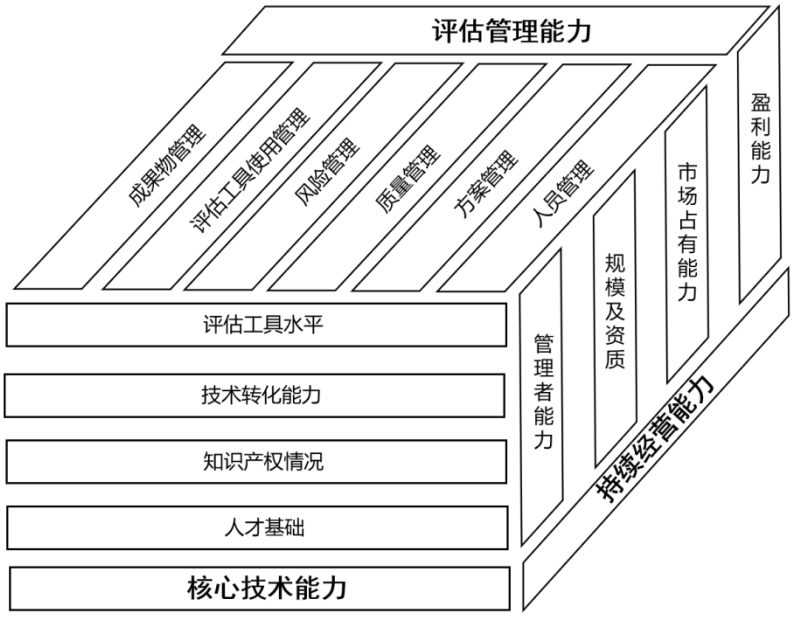

图 1　数据安全评估服务能力评定指标框架图

持续经营能力、核心技术能力、评估管理能力分别从技术、经营、服务过程维度分析企业数据安全评估服务能力。持续经营能力保障了数据安全评估高技术、人才的引进和吸收，促进了核心能力的提升；核心技术能力的提升助力企业提升硬实力，保障企业在高技术产品、服务竞争中占得优势，促进财务资源获得，增强持续经营能力；持续经营能力和核心技术能力提升了服务过程的效能，带动评估管理能力提升；评估管理能力保障市场资源获得、指引研发和生产的方向，促进持续经营能力和核心技术能力提升。

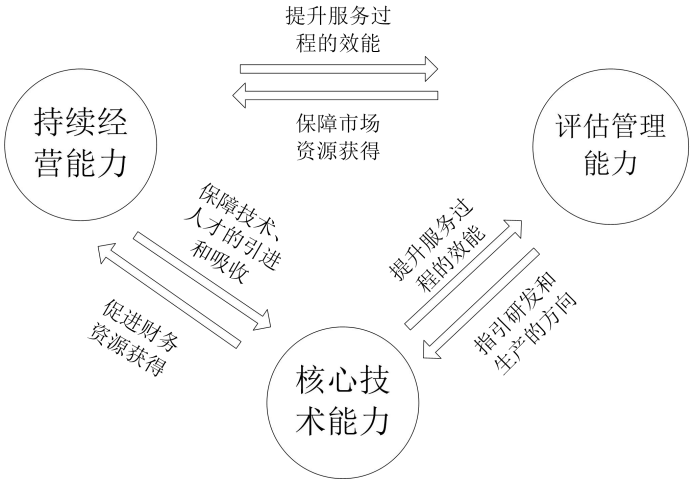

图 2　数据安全评估服务分项能力间的关系图

7　评定分类要求

7.1　核心技术能力

7.1.1 人才基础

7.1.1.1 一级要求

a) 正式受聘人员应不少于15人，直接从事数据安全评估服务的人员不低于8人；
b) 直接从事数据安全评估服务的技术人员大学本科以上学历不少于80%；
c) 至少2名正式受聘技术人员接受过数据安全防护技术和准则的系统培训，或参与起草数据安全防护系列标准；
d) 至少2名正式受聘技术人员具有国家和相关机构认可的数据安全评估专业资质；
e) 制定技术人员岗前培训计划，相关人员经考核评定合格后方可上岗；
f) 正式受聘技术人员应具备数据安全相关基础知识，熟悉数据安全相关法律法规、政策和标准；
g) 正式受聘技术人员应具备良好的沟通与协调能力,能理解服务需求方的业务流程和数据安全目标；
h) 正式受聘技术人员应具备强有力的执行能力，能够落实数据安全相关制度、策略。

7.1.1.2 二级要求

应满足本文件7.1.1.1节一级要求的所有条款，并在以下方面增强或者增加要求：
a) 正式受聘人员应不少于75人，直接从事数据安全评估服务的人员不低于20人；
b) 至少10名正式受聘技术人员具备3年以上的数据安全服务项目经验，且具有成功的项目案例；
c) 至少4名正式受聘技术人员接受过数据安全防护技术和准则的系统培训，或参与起草数据安全防护系列标准；
d) 至少4名正式受聘技术人员具有国家和相关机构认可的数据安全评估师资质，或其他数据安全评估相关专业资质；
e) 正式受聘技术人员应具备敏感数据发现、重要数据和核心数据分类分级评估、数据安全风险评估等能力，能对被测资产提出整改建议；
f) 正式受聘技术人员应具备密码技术与应用等数据安全专业知识,熟悉数据安全产品开发、测试。

7.1.2 知识产权情况

7.1.2.1 一级要求

a) 具备跟踪研究数据安全评估新技术新产品新服务的能力；
b) 熟悉知识产权申请流程，了解相关法律法规。

7.1.2.2 二级要求

应满足本文件7.1.2.1节一级要求的所有条款，并在以下方面增强或者增加要求：
a) 拥有数据安全相关知识产权5项及以上（Ⅱ类）或1项及以上（Ⅰ类），相关数据安全技术的先进程度较高，对主要数据安全产品（服务）在技术上发挥核心支持作用；
b) 建立知识产权创造、运用、保护、管理和服务全环节制度体系。

7.1.3 技术转化能力

7.1.3.1 一级要求

a) 了解数据安全相关科技成果转化的主要方式；

b） 了解数据安全评估工具的开发方法。

7.1.3.2 二级要求

应满足本文件7.1.3.1节一级要求的所有条款，并在以下方面增强或者增加要求：

a） 近3年内数据安全相关科技成果转化的年平均数不少于4项；
b） 具备自研或联合开发数据安全评估工具的能力；
c） 具备发现数据安全评估工具安全风险的能力。

7.1.4 评估工具水平

7.1.4.1 一级要求

a） 应具备数据安全评估服务工具（包括设备、平台、软件、模板、知识库等）。

7.1.4.2 二级要求

应满足本文件7.1.4.1节一级要求的所有条款，并在以下方面增强或者增加要求：

a） 具备数据分类分级评估、敏感资产识别发现、数据流动状态分析评估、数据脆弱性评测、数据出境及异常分析评估等数据安全评估服务工具；
b） 数据安全评估服务工具应具有至少3个成功使用的案例。

7.2 持续经营能力

7.2.1 管理者能力

7.2.1.1 一级要求

a） 法人或负责人具备一定的战略能力、组织能力；
b） 明确质量负责人，且具备2年以上的质量管理经验；
c） 明确数据安全技术负责人，且具备2年以上的数据安全项目管理经验。

7.2.1.2 二级要求

应满足本文件7.2.1.1节一级要求的所有条款，并在以下方面增强或者增加要求：

a） 数据安全技术负责人具备中级及以上职称；
b） 数据安全技术负责人具备本科及以上学历；
c） 数据安全技术负责人具备5年以上数据安全管理经验。

7.2.2 规模及资质

7.2.2.1 一级要求

a） 应具备1年以上的数据安全行业从业时间；
b） 具有信息安全管理相关的制度规范；
c） 具备至少1项信息安全服务资质，或至少1个信息安全服务项目获奖。

7.2.2.2 二级要求

应满足本文件7.2.2.1节一级要求的所有条款，并在以下方面增强或者增加要求：

a) 应具备5年以上的数据安全行业从业时间；
b) 按照GB/T 22080建立信息安全管理体系；
c) 具备至少3项信息安全服务资质，或至少3个信息安全服务项目获奖。

7.2.3 市场占有能力

7.2.3.1 一级要求

a) 至少承担2个数据安全评估服务项目，单个合同金额不低于20万元人民币，项目合同总金额不低于100万元人民币；
b) 至少终验通过2个数据安全评估服务项目；
c) 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数据安全评估服务项目。

7.2.3.2 二级要求

应满足本文件7.2.3.1节一级要求的所有条款，并在以下方面增强或者增加要求：
a) 至少获得3个数据安全评估服务项目，单个合同金额不低于30万元人民币，项目合同总金额不低于180万元人民币；
b) 至少终验通过4个数据安全评估服务项目。

7.2.4 盈利能力

7.2.4.1 一级要求

a) 近1年净利润、净资产收益均为正；
b) 近1年收入增长率或净利润增长率为正。

7.2.4.2 二级要求

a) 近3年净利润、净资产收益均为正；
b) 近3年收入增长率或净利润增长率为正。

7.3 评估管理能力

7.3.1 人员管理

7.3.1.1 一级要求

a) 设置与数据安全评估服务项目规模相适应人员团队，并建立项目服务人员清单，明确项目服务人员职责；
b) 与项目服务人员签订保密协议，并定期进行保密教育、风险排查、自查检查。

7.3.1.2 二级要求

应满足本文件7.3.1.1节一级要求的所有条款，并在以下方面增强或者增加要求：
a) 建立数据安全评估服务人员档案，包括服务人员的录用、离岗或离职、资质证明、培训/考核记录、从业经历、实际参与项目及分工等信息，档案至少保存至技术人员离职后5年，有关法律法规、行业管理另有规定的除外；

b) 根据项目特点制定数据安全评估服务人员行为规范，包括但不限于遵守需求方管理制度，遵守数据安全服务保密管理制度，规范使用测评专用设备和工具，规范管理成果物等。

7.3.2 方案管理

7.3.2.1 一级要求

a) 编制的方案应获得需求方确认；
b) 编制的方案应具备可操作性，目标应具体、可行，操作计划应详细清晰。

7.3.2.2 二级要求

应满足本文件7.3.2.1节一级要求的所有条款，并在以下方面增强或者增加要求：
a) 编制的方案应明确数据安全评估服务范围、服务目标、评估依据、服务内容、服务成果等；
b) 编制的方案应明确项目服务人员（包括项目负责人、项目实施技术人员的职责等）、服务流程（包括计划或进度等）、服务环境、服务方法、服务工具、服务保障（包括资源保障、质量管理、保密管理、风险控制等）等服务要素，对资金、人员、工具等资源的调配方案具备可操作性。

7.3.3 质量管理

7.3.3.1 一级要求

a) 严格按照相关标准开展评估工作，确保报告内容全面、准确、无缺项；
b) 实施过程符合需求方安全管理相关要求，对服务过程中的关键活动和原始数据进行记录，实施的过程文档记录应准确、完整；
c) 具备客户服务电话热线号码，并提供5×8小时电话热线支持或同等响应级别的客户服务；
d) 建立数据安全评估服务项目管理制度，明确项目管理责任部门、责任范围、责任人、工作流程、及与其他部门的统筹协调等，明确数据安全评估服务项目计划、质量要求及监督检查工作。

7.3.3.2 二级要求

应满足本文件7.3.3.1节一级要求的所有条款，并在以下方面增强或者增加要求：
a) 设置项目质量管理岗位，建立项目服务质量控制机制；
b) 根据方案组织项目实施，定期通过通知、例会、报告（如周、月报）等多种形式与需求方沟通反馈项目质量。

7.3.4 风险管理

7.3.4.1 一级要求

a) 在进行数据安全评估服务时，应获得需求方授权，执行过程中发现数据安全事件，及时向需求方报告，并记录事件相关内容；
b) 在进行数据安全评估服务过程中发现产品（含硬件、软件）的安全问题时，及时向需求方报告；
c) 使用服务工具，有可能对服务需求方系统或平台的功能、性能，数据的保密性、完整性、可用性等造成影响的，需向需求方进行风险提示，在采取风险规避措施并得到服务需求方同意后方可使用；

d) 采取必要的监督、审计措施，确保服务人员对系统或数据的操作严格按照服务协议及需求方授权范围进行；
e) 在开展数据安全评估工作前，应与需求方就数据安全保密责任义务进行认定与划分，包括但不限于保密协议签署等，应对评估中获取的相关信息、评估过程文档等严格保密，以保障需求方的数据安全。

7.3.4.2 二级要求

应满足本文件7.3.4.1节一级要求的所有条款，并在以下方面增强或者增加要求：
a) 制定有效的风险应急预案，并确保其可行、易操作，定期开展风险应急预案演练并保存记录；
b) 采取必要措施识别服务范围、服务内容、服务流程、服务环境、服务资源等技术人员实施过程中可能产生的风险，并更新风险应急预案；
c) 建立项目风险沟通与应急处置机制，确定双方接口人，及时处理服务实施过程中产生的投诉、争议、突发事件等项目风险，并形成处置结论或解决方案。

7.3.5 评估工具使用管理

7.3.5.1 一级要求

a) 具备数据安全评估工具或软件使用管理机制；
b) 项目相关人员能熟练使用数据分类分级评估、敏感资产识别发现、数据流动状态分析评估、数据脆弱性评测、数据出境及异常分析评估等工具或软件。

7.3.5.2 二级要求

应满足本文件7.3.5.1节一级要求的所有条款，并在以下方面增强或者增加要求：
a) 根据实际定期更新数据安全评估工具或软件使用管理机制；
b) 建立数据安全评估工具或软件使用培训机制；
c) 数据分类分级、敏感资产识别发现、数据流动状态分析评估、数据脆弱性评测、数据出境及异常分析评估等数据安全评估服务工具的版本较新。

7.3.6 成果物管理

7.3.6.1 一级要求

a) 应建立数据安全评估服务报告编制管理机制；
b) 应具备报告编制能力，掌握数据安全评估报告的相关要求，熟悉报告编制流程。
c) 按服务协议中所规定的关键节点，提交成果物，如项目方案、过程文档和记录、项目报告（包括阶段报告、总结报告、验收报告等），并得到需求方的确认；
d) 保证所有交付成果具备真实性、准确性和完整性；
e) 完成服务交付后，主动清理、交还相关数据、资料、账号、设备工具等，并向需求方提供由项目负责人签字的承诺或确认函。

7.3.6.2 二级要求

应满足本文件7.3.6.1节一级要求的所有条款，并在以下方面增强或者增加要求：
a) 应定期更新报告模板，定期对报告编制、审核等相关项目服务人员进行培训；

b) 建立、维护项目成果（包括但不限于项目方案、过程文档和记录、项目报告等）档案，严格管理项目档案的查询、借阅行为，档案至少保存5年。

8 评定方法

8.1 专家评审法

借助专家意见进行评定。邀请相关领域专家，采用询问、访谈、查阅资料、实地查看、调查统计等方式进行，一般不少于3位。

8.2 资料收集法

通过内部文档或第三方资料收集进行评定。

9 评定程序

数据安全服务提供商申请能力评定等级为一级或二级的，应当将申报材料提交到评审机构，能力评定按下列程序进行：

数据安全服务提供商提交的申请材料应符合本文件第5-7章相关内容，经评审机构初审合格后，由评审机构组织专家对数据安全服务提供商进行现场评定。通过专家现场评定后，数据安全服务提供商将获颁对应等级的证书，并接受评审机构的持续监督。

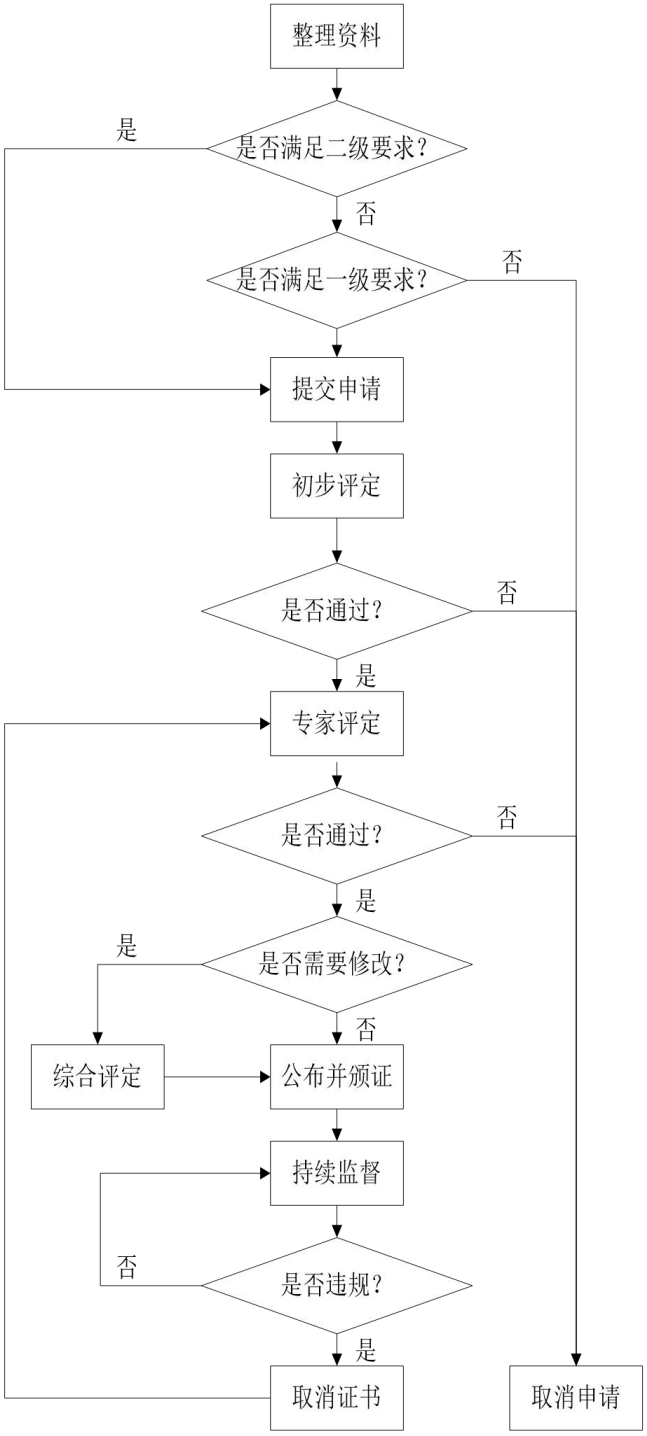

图 3　数据安全评估服务能力评定流程图

10　评定结果

a）评定通过后，数据安全评估服务能力评定结果和监督检查结果应在评定机构的官方网站进行公布，并获颁评定证书；

b）评定证书有效期为三年，获证的数据安全服务提供商应邀请评定机构每年进行一次年检；

c）获证的数据安全服务提供商在证书到期前六个月申请重新评定和换证，复申程序参照本文件第9章评定程序执行。

参 考 文 献

[1] GB/T 22080-2016 信息技术 安全技术 信息安全管理体系
[2] GB/T 25069-2022 信息安全技术 术语
[3] GB/T 30271—2013 信息安全技术 信息安全服务能力评估准则
[4] GB/T 30276—2020 信息安全技术 网络安全漏洞管理规范
[5] GB/T 31168—2023 信息安全技术 云计算服务安全能力要求
[6] GB/T 35273-2020 信息安全技术 个人信息安全规范
[7] GB/T 35274-2017 信息安全技术 大数据服务安全能力要求
[8] GB/T 37973-2019 信息安全技术 大数据安全管理指南
[9] GB/T 37988-2019 信息安全技术 数据安全能力成熟度模型
[10] GB/T 41479-2022 信息安全技术 网络数据处理安全要求
[11] JGJ/T 67-2019 办公建筑设计标准
[12] YD/T 3644-2020 面向互联网的数据安全能力技术框架
[13] YD/T 3802-2020 电信网和互联网数据安全通用要求
[14] YD/T 3956-2021 电信网和互联网数据安全评估规范
[15] T/ZHTEA 001—2023 高新技术企业创新能力评价