

ICS

CCS 点击此处添加 CCS 号

# T/CCIASC

团体标准

T/CCIASC 050—2025

## 数据安全服务能力评价体系框架

Overview of Data Security Service Capability Evaluation System

(征求意见稿)

2025 - 10 - XX 发布

2025 - 10 - XX 实施

中国计算机行业协会 发布

## 目 次

前 言 .....	II
引 言 .....	III
1 范围 .....	1
2 规范性引用文件 .....	1
3 术语和定义 .....	1
4 数据安全服务体系 .....	2
5 数据安全服务能力评价体系 .....	3
6 评价指标体系 .....	3
7 评定要求 .....	4
7.1 评定基本要求 .....	4
7.2 评定分类要求 .....	4
7.2.1 数据安全评估服务能力的评定规范 .....	4
7.2.2 数据安全建设服务能力的评定规范 .....	5
7.2.3 数据安全运维服务能力的评定规范 .....	5
7.2.4 数据安全咨询服务能力的评定规范 .....	5
7.2.5 数据安全监测预警服务能力的评定规范 .....	5
7.2.6 数据安全应急响应服务能力的评定规范 .....	6
8 评价方法 .....	6
8.1 资料收集法 .....	6
8.2 专家评审法 .....	6
9 评定程序 .....	6
10 评定结果 .....	7
参 考 文 献 .....	9

## 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）、国家电网有限公司、中国电力科学研究院有限公司、国网信息通信中心（大数据中心）、中国电信股份有限公司安徽分公司、中移动信息技术有限公司、北京天融信网络安全技术有限公司、北京中科卓信软件测评技术中心、天津朗言安全技术服务有限公司、远光软件股份有限公司、上海计算机软件技术开发中心、长沙长钢计算机有限公司。

本文件主要起草人：林海静、王露颖、王文鑫、曹顺超、张嘉欢、王翔宇、陈刚、肖红阳、王迪、徐灏、王鸿元、晋钢、黄鹂、李远金、张靖、向万红、林武星、王倩、胡文奇。

## 引 言

随着《中华人民共和国数据安全法》正式实施，以及《工业和信息化部等十六部门关于促进数据安全产业发展的指导意见》等政策文件的相继出台，数据安全服务的规范化和标准化需求日益迫切。作为数字时代信息资产安全的核心支撑，数据安全服务旨在提升数据安全服务提供商的数据安全保护能力，确保数据信息在全生命周期内得到有效防护、合法利用和有序流动，从而提升行业领域的数据安全治理效能，促进数据要素的市场培育与价值释放。然而，当前数据安全服务提供商的服务能力参差不齐，严重制约市场的规范化、标准化发展。因此，构建统一的数据安全服务能力评价体系，提高数据市场安全服务供给质量，成为推动行业高质量发展的关键。本文件旨在通过对数据安全服务能力相关标准展开梳理，构建一套规范化、标准化、系统化的数据安全服务能力评定体系，明确数据安全服务提供商的核心能力要求，为行业的持续健康发展提供有力支撑。

# 数据安全服务能力评价体系框架

## 1 范围

本文件给出了数据安全服务能力评价体系整体框架。

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

## 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 22080-2025 网络安全技术 信息安全管理体系要求

GB/T 25069-2022 信息安全技术 术语

GB/T 41479-2022 信息安全技术 网络数据处理安全要求

T/ZHTEA 001-2023 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：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：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：GB/T 25069—2022，定义3.184

### 3.4 I类知识产权 Class I 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 数据安全服务体系

数据安全服务是一个综合性概念，其主要涵盖数据安全评估、数据安全建设、数据安全运维、数据安全咨询、数据安全监测预警以及数据安全应急响应等六方面。这六方面服务相互支撑、协同合作，通过提供规范化和标准化数据安全服务，强化各行业的数据安全保护能力（如图1）。

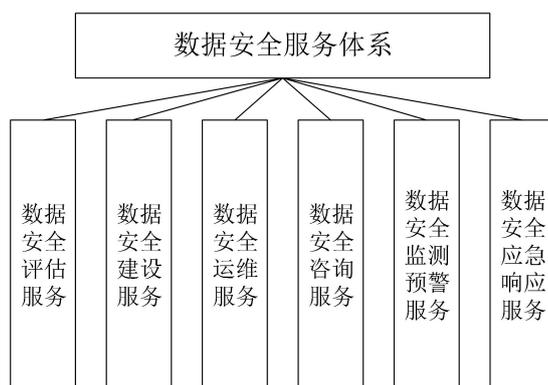


图1 数据安全服务体系框架

数据安全评估服务是指数据安全服务提供商为客户的数据和相关系统提供评估分析，研判客户所面临的威胁及其存在的脆弱性，评估数据安全事件一旦发生可能造成的危害程度，并提出有针对性的抵御威胁的防护对策和安全措施，防范和化解数据及相关系统安全风险，将风险控制在可接受的水平。

数据安全建设服务是指数据安全服务提供商为客户的数据全生命周期过程的安全提供框架设计，形成数据安全建设规划，并对计划实施的数据安全策略细化，在数据安全解决方案的基础上，实施数据安全产品集成部署、数据安全软件定制开发、数据安全加固与整改或其它的数据安全技术和咨询服务。

数据安全运维服务是指数据安全服务提供商为客户的数据资产提供全面的保护和管理，在确保数据的机密性、完整性和可用性的基础上，提高数据质量、防止数据被非法获取及滥用，保障业务的连续性和稳定性。

数据安全咨询服务是指数据安全服务提供商为客户提供关于数据安全的专业建议、解决方案和战略规划。

数据安全监测预警服务是指数据安全服务提供商为客户的数据处理活动提供持续地、实时地观察和分析，以发现潜在的安全风险或已经发生的安全事件，并及时发出预警信息。

数据安全应急响应服务是指数据安全服务提供商为客户提供系统化的预防机制、处置流程等，在事件发生前、发生时及发生后所采取的一系列专业化应对措施。

同时，各项服务间具有紧密的逻辑关联：数据安全评估服务对数据安全体系进行定期评估和验证，识别潜在风险和薄弱环节，为信息系统的持续改进提供理论依据；数据安全建设服务将理论转化为实践，负责数据安全体系的具体落地实施，包括技术部署、系统集成和架构搭建等，确保数据资产在合规的前提下能够合理开发利用；数据安全运维服务确保数据安全服务提供商系信息系统的日常稳定运行，包括系统维护、配置管理、故障处理等内容，保障安全防护措施的持续有效；数据安全咨询服务为数据安全服务提供商提供数据安全战略规划、政策制定和体系建设指导，提高有关人员数据安全相关工作落地效率和保障意识；数据安全监测预警服务通过实时监控，及时发现潜在威胁和安全事件，为应急响应提供预警信息，实时保障信息系统安全；数据安全应急响应服务在安全事件发生时快速响应、有效处置，最大限度降低损失，并总结经验教训反馈至其他环节。

## 5 数据安全服务能力评价体系

数据安全服务能力评价体系由六个方面的数据安全服务能力规范组成,包含数据安全评估服务能力评定规范、数据安全建设服务能力评定规范、数据安全运维服务能力评定规范、数据安全咨询服务能力评定规范、数据安全监测预警服务能力评定规范、数据安全应急响应服务能力评定规范(如图2)。

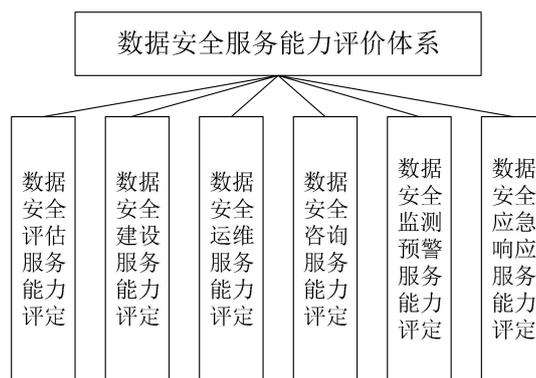


图2 数据安全服务能力评价体系框架

数据安全评估服务能力评定规范旨在对数据安全评估服务提供商的评估工具支撑能力、评估人员能力、合规与风险管理能力等方面进行客观评价。

数据安全建设服务能力评定规范旨在对数据安全建设服务提供商的集成部署能力、技术创新能力、服务交付能力等方面进行客观评价。

数据安全运维服务能力评定规范旨在对数据安全运维服务提供商的核心技术能力、持续经营能力、人员管理等方面进行客观评价。

数据安全咨询服务能力评定规范旨在对数据安全咨询服务提供商的需求分析与方案设计能力、服务能力、质量保证能力等进行客观评价。

数据安全监测预警服务能力评定规范旨在对数据安全监测预警服务提供商的安全防护能力、监测检测能力、预警分析能力等方面进行客观评价。

数据安全应急响应服务能力评定规范旨在对数据安全应急响应服务提供商的技术专业性、响应速度、处置流程等方面进行客观评价。

## 6 评价指标体系

数据安全服务能力评价体系分为评定基本要求及评定分类要求。

评定分类要求从核心技术能力、持续经营能力、项目管理能力3个维度分别对数据安全服务提出了2级能力要求,由高到低依次是二级、一级能力。

持续经营能力、核心技术能力、项目管理能力分别从技术、经营、服务过程维度分析数据安全服务提供商数据安全服务能力。持续经营能力保障了数据安全技术、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数据安全服务提供商提升硬实力,保障数据安全服务提供商在高技术产品、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，带动项目管理能力提升；项目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。

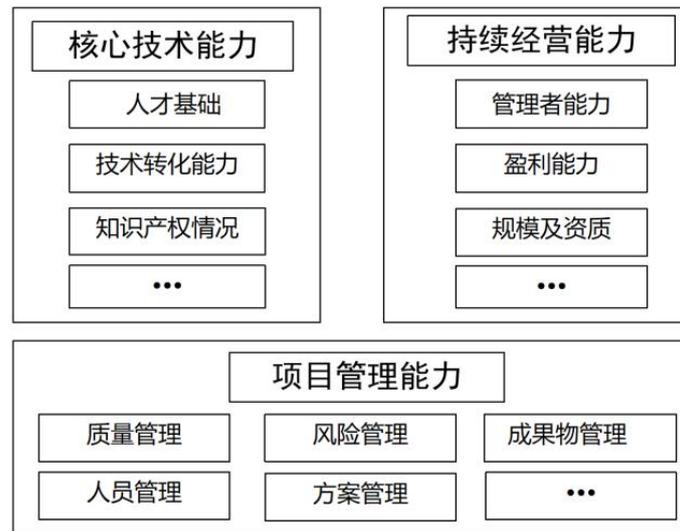


图3 数据安全服务能力评价体系评定分项结构图

## 7 评定要求

### 7.1 评定基本要求

数据安全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或非独立法人的集团公司的省分公司/子公司；
- b) 产权关系明晰，独立经营核算，无违法记录；
- c) 法定代表人、主要负责人、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运维单位或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；
- f) 从事涉密的数据安全服务应满足国家保密机关相关要求；
- g) 应具备固定办公地点。

### 7.2 评定分类要求

#### 7.2.1 数据安全评估服务能力的评定规范

- a) 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，要求评估人员需具备国家和相关机构认可的数据安全评估专业资质，要求数据安全评估服务提供商应具备数据安全评估服务工具；

- b) 持续经营能力的评定指标包括管理者能力、规模及资质、市场占有能力、盈利能力等，要求数据安全评估服务提供商需承担过数据安全评估服务项目，并达到合同金额和评估报告通过验收等条件；
- c) 评估管理能力的评定指标包括人员管理、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，要求数据安全评估服务提供商应具备数据安全评估工具或软件使用管理机制，要求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。

#### 7.2.2 数据安全建设服务能力的评定规范

- a) 核心技术能力的评定指标包括人才基础、技术创新机制、知识产权情况、技术转化能力等，要求技术人员具有国家和相关机构认可的数据安全建设专业资质；
- b) 持续经营能力的评定指标包括管理者能力、规模及资质、市场占有能力、盈利能力等，要求数据安全建设服务提供商承担数据安全建设服务项目，并达到合同金额和终验通过等条件；
- c) 项目管理能力的评定指标包括人员管理、方案管理、质量管理、风险管理、成果物管理等，要求数据安全建设服务提供商设置与数据安全建设服务项目规模相适应人员团队，并建立项目人员清单，明确项目人员职责。

#### 7.2.3 数据安全运维服务能力的评定规范

- a) 核心技术能力的评定指标包括人才基础、运维工具水平、技术创新机制、技术转化能力，要求运维人员具有相关机构认可的数据安全运维专业资质，要求数据安全运维服务提供商具备数据安全运维服务工具；
- b) 持续经营能力的评定指标包括管理者能力、规模及资质、市场占有能力、盈利能力，要求数据安全运维服务提供商具有承接数据安全运维服务项目经验，并具有项目合同金额要求；
- c) 项目管理能力的评定指标包括人员管理、方案管理、质量管理、风险管理、成果物管理、供应商管理，要求数据安全运维服务提供商建立供应商管理制度，明确供应商管理责任部门、职责范围、责任人，规范供应商引入、评估、合作及退出的工作流程，以及与其他部门的协作机制。

#### 7.2.4 数据安全咨询服务能力的评定规范

- a) 核心技术能力的评定指标包括人才基础、技术研究能力、知识产权情况、技术转化能力等，要求数据安全服务咨询提供商咨询人员需具备国家和相关机构认可的数据安全咨询专业资质，并拥有丰富的行业经验；
- b) 持续经营能力的评定指标包括管理者能力、单位资质奖励、市场占有能力、盈利能力等，要求数据安全咨询服务提供商承担过数据安全咨询服务项目，并达到合同金额和客户满意度等条件；
- c) 项目管理能力的评定指标包括人员管理、质量管理、风险管理、成果物管理、客户关系管理等，要求数据安全咨询服务提供商具备项目满意度调查，实行客户分层与精准维护，为不同层级的客户提供个性化、定制化的服务，以满足其特定需求。

#### 7.2.5 数据安全监测预警服务能力的评定规范

- a) 核心技术能力的评定指标包括人才基础、技术创新机制、技术转化能力等，要求技术人员具备国家认可的数据安全专业资质和丰富的威胁分析经验，并能将先进监测技术应用于实际业务场景，要求数据安全服务监测预警提供商具备监测预警技术平台或相关技术手段；
- b) 持续经营能力的评定指标包括管理者能力、规模及资质、市场占有率能力、盈利能力等，要求数据安全监测预警服务提供商具备成熟的业务运营体系和持续的服务保障能力；
- c) 项目管理能力的评定指标包括人员管理、方案管理、质量管理、风险管理、成果物管理等，要求数据安全监测预警服务提供商建立完善的监测预警机制，具备快速识别安全威胁和及时预警的能力，并能提供专业可靠的分析报告和处置建议。

#### 7.2.6 数据安全应急响应服务能力的评定规范

- a) 核心技术能力的评定指标包括人才基础、技术创新机制、技术研究情况、技术转化能力等，要求技术人员具备数据安全应急响应资质和丰富的实战处置经验，能够运用先进的威胁检测与溯源技术；
- b) 持续经营能力的评定指标包括管理者能力、规模及资质、市场占有率能力、盈利能力等，要求数据安全应急响应服务提供商在应急响应领域的服务成熟度和可持续发展能力；
- c) 项目管理能力的评定指标包括人员管理、方案管理、质量管理、风险管理、成果物管理等，要求数据安全应急响应服务提供商建立标准化应急响应机制，并能提供专业的应急预案、事件分析报告和整改方案。

### 8 评价方法

#### 8.1 资料收集法

通过数据安全服务提供商自身提供内部文档或第三方进行资料收集后，申请评定。

#### 8.2 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。

### 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。

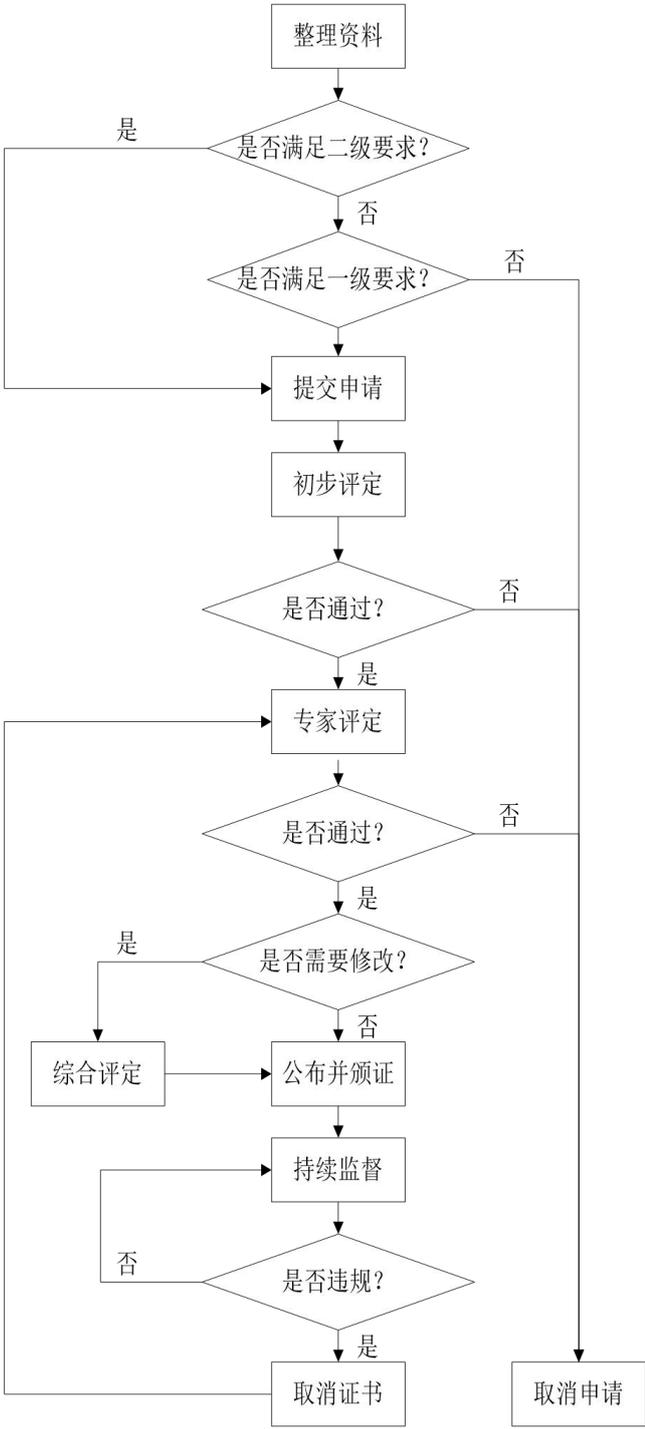


图 4 数据安全服务能力评定流程图

10 评定结果

- a) 评定通过后,数据安全服务能力评定结果和监督检查结果应在数据安全产业公共服务平台官方网站进行公布,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，复审程序参照本文件第9章评定程序执行。

## 参 考 文 献

- [1] GB/T 22080-2025 网络安全技术 信息安全管理体系要求
  - [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] YD/T 3802-2020 电信网和互联网数据安全通用要求
  - [12] YD/T 3956-2021 电信网和互联网数据安全评估规范
-