ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T XXXXX—XXXX

信息安全技术 数据安全评估机构能力要求

Information security technology —Capability requirements for assessment organization of data security

(点击此处添加与国际标准一致性程度的标识)

（征求意见稿）

（本草案完成时间：2023 年 4 月 19 日）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

国家市场监督管理总局
国家标准化管理委员会　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。

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专利的责任。

本文件由全国信息安全标准化技术委员会（SAC/TC 260）提出并归口。

本文件起草单位：国家信息技术安全研究中心、中国电子技术标准化研究院、国家计算机网络应急技术处理协调中心、中国网络安全审查技术与认证中心、中国信息安全测评中心、中国网络空间研究院、公安部第三研究所、中国信息通信研究院、中国软件测评中心、国家工业信息安全发展研究中心、中国电子科技集团公司第十五研究所、中国科学技术大学、中国科学院软件研究所、工业和信息化部电子第五研究所、中国电子信息产业集团有限公司第六研究所、国家广播电视总局监管中心、中国民用航空局信息中心、教育部教育管理信息中心、北京银联金卡科技有限公司、北京时代新威信息技术有限公司等。

本文件主要起草人：俞克群、杨韬、陈琳、胡影、张宇光、林星辰、王晖、左晓栋、刘曦泽、刘楠等。

信息安全技术 数据安全评估机构能力要求

1 范围

本文件规定了数据安全评估机构的能力要求。

本文件适用于数据安全评估机构自身能力建设，也适用于主管监管部门对数据安全评估机构开展的评定活动，还可为数据处理者选择数据安全评估机构提供参考。

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 19001—2016 质量管理体系 要求

GB/T 25069—2022 信息安全技术 术语

GB/T 39335—2020 信息安全技术 个人信息安全影响评估指南

GB/T 41479—2022 信息安全技术 网络数据处理安全要求

GB/T 32914-XXXX 信息安全技术 网络安全服务能力要求

GB/T AAAA-XXXX 信息安全技术 数据安全风险评估方法

3 术语和定义

GB/T 25069—2022和GB/T 41479—2022中界定的以及下列术语和定义适用于本文件。

3.1

数据处理活动 data processing activities

数据收集、存储、使用、加工、传输、提供、公开、删除等活动。

3.2

数据安全评估 data security assessment

对数据处理活动存在的安全问题、面临的安全风险、采取的安全措施等开展的技术检测、评价等活动。

注：包括不限于数据安全风险评估、个人信息保护影响评估、数据出境安全评估等。

3.3

数据安全风险 data security risk

由于开展数据处理活动不合理、缺少有效的数据安全措施等，导致数据安全事件的发生及其对国家安全、公共利益或者组织、个人合法权益造成的可能性和影响程度。

3.4

数据安全风险评估 data security risk assessment

对数据和数据处理活动安全进行风险识别、风险分析和风险评价的整个过程。

3.5

数据安全评估机构 assessment organization of data security

从事数据安全评估活动的机构。

3.6

数据处理者 data processor

在数据处理活动中自主决定处理目的和处理方式的个人和组织。

3.7

安全措施 security measure

保护数据和数据处理活动、抵御数据安全风险而实施的各种安全管理和技术实践、规程和机制。

3.8

风险源 risk source

可能导致数据和数据处理活动的保密性、完整性、可用性和合理性受到危害的原因、条件、情形或行为。

注：风险源，既包括安全威胁利用脆弱性可能导致数据安全事件的风险源（简称为“数据安全风险源”），也包括数据处理活动不合理操作可能造成违法违规处理事件的风险源（简称为“不合理数据处理风险源”）。

3.9

合理性 rationality

开展数据处理活动遵守法律、法规，尊重社会公德和伦理，遵守商业道德和职业道德，诚实守信，不危害国家安全、公共利益，不损害个人、组织的合法权益。

4 概述

数据安全评估机构能力要求由机构基本要求、评估管理能力、评估技术能力、评估人员能力、评估资源要求5部分组成，框架见图1。表1给出了数据安全评估类型与能力要求对应关系，附录A给出了数据安全评估机构能力证明方法。

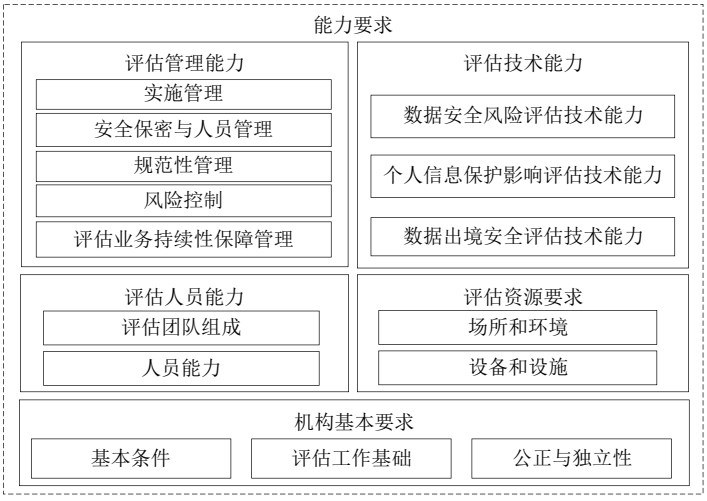

图1 数据安全评估机构能力要求框架图

表1　数据安全评估类型与能力要求对应关系

序号	数据安全评估活动类型	评估活动应满足的能力要求	
1	数据安全风险评估	5.1 机构基本要求	5.1.1 基本条件、5.1.2 评估工作基础、5.1.3 公正与独立性章节全部条款内容。
		5.2 评估管理能力	5.2.1 实施管理、5.2.2 安全保密与人员管理、5.2.3 规范性管理、5.2.4 风险控制、5.2.5 评估业务持续性保障管理章节全部条款内容。
		5.4 评估人员能力	5.4.1 评估团队组成、5.4.2 人员能力章节全部条款内容。
		5.5 评估资源要求	5.5.1 场所和环境、5.5.2 设备和设施章节全部条款内容。
		5.3.2 数据安全风险评估技术能力章节全部条款内容。	
2	个人信息保护影响评估	5.1 机构基本要求	5.1.1 基本条件、5.1.2 评估工作基础、5.1.3 公正与独立性章节全部条款内容。
		5.2 评估管理能力	5.2.1 实施管理、5.2.2 安全保密与人员管理、5.2.3 规范性管理、5.2.4 风险控制、5.2.5 评估业务持续性保障管理章节全部条款内容。
		5.4 评估人员能力	5.4.1 评估团队组成、5.4.2 人员能力章节全部条款内容。
		5.5 评估资源要求	5.5.1 场所和环境、5.5.2 设备和设施章节全部条款内容。
		5.3.3 个人信息保护影响评估技术能力章节全部条款内容。	
3	数据出境安全评估	5.1 机构基本要求	5.1.1 基本条件、5.1.2 评估工作基础、5.1.3 公正与独立性章节全部条款内容。
		5.2 评估管理能力	5.2.1 实施管理、5.2.2 安全保密与人员管理、5.2.3 规范性管理、5.2.4 风险控制、5.2.5 评估业务持续性保障管理章节全部条款内容。
		5.4 评估人员能力	5.4.1 评估团队组成、5.4.2 人员能力章节全部条款内容。
		5.5 评估资源要求	5.5.1 场所和环境、5.5.2 设备和设施章节全部条款内容。
		5.3.2 数据安全风险评估技术能力章节全部条款内容。	
		5.3.4 数据出境安全评估技术能力章节全部条款内容。	
		涉及个人信息出境的安全评估场景，还应满足 5.3.3 个人信息保护影响评估技术能力章节全部条款内容。	
4	其他	5.1 机构基本要求	5.1.1 基本条件、5.1.2 评估工作基础、5.1.3 公正与独立性章节全部条款内容。
		5.2 评估管理能力	5.2.1 实施管理、5.2.2 安全保密与人员管理、5.2.3 规范性管理、5.2.4 风险控制、5.2.5 评估业务持续性保障管理章节全部条款内容。
		5.4 评估人员能力	5.4.1 评估团队组成、5.4.2 人员能力章节全部条款内容。
		5.5 评估资源要求	5.5.1 场所和环境、5.5.2 设备和设施章节全部条款内容。
		法律法规规定或主管监管部门要求的其他有关能力。	

5 能力要求

5.1 机构基本要求

5.1.1 基本条件

数据安全评估机构应具备以下基本条件：

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 1000 万元以上,独立经营核算，无违法违规记录；
c) 法定代表人、主要负责人、评估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机构能力和信誉的负面清单。

5.1.2 评估工作基础

数据安全评估机构应具备以下工作基础：

a) 从事数据安全评估或相关服务 3 年以上，且无重大服务投诉、处罚事件；
b) 近 3 年完成过数据安全相关检查、检测、评估项目或任务 2 项以上，主要包括：网络或数据安全监管部门、行业主管部门组织的数据安全检查、检测或评估工作；向数据处理者提供的数据安全评估相关服务项目；
c) 具有合格评定国家认可机构实验室颁发的认可证书或检验机构认可证书，且证书处于有效状态，证书认可的能力范围含信息安全或网络安全检验检测相关内容。

5.1.3 公正与独立性

数据安全评估机构应符合从事数据安全评估工作所需要的公正性和独立性等要求，包括但不限于：

a) 严格执行有关法律法规、标准规范，开展客观、公正的评估活动；
b) 对其评估活动的公正性负责，应不受可能来自商业、财务或其他方面的压力影响公正性；
c) 不从事面向公众、被评估对象开展的网络数据处理活动，有国家机关授权或评估机构内部独立开展的数据处理活动除外；
d) 不涉及数据安全产品开发、销售、集成以及运营等活动，不从事信息技术产品开发、销售和信息系统集成实施等活动，自用评估工具除外；
e) 不向评估对象推荐、指定产品或工具；
f) 不介入评估对象之间的市场竞争。

5.2 评估管理能力

5.2.1 实施管理

数据安全评估机构应建立、执行数据安全评估专用实施管理制度和措施，包括但不限于：

a) 评估项目实施前编制评估计划或方案，明确评估目标、范围、评估方式、投入资源、时间进度等，并得到被评估方的认可；
b) 建立并执行评估方案管理制度，采用专家评审或审核方式，重点审核明确被评估对象的数据处理活动范围，及拟投入的相关资源、评估实施周期等内容是否适当等；
c) 建立评估机构管理责任制度，明确责任部门、责任范围、责任人、工作流程、及与其他部门的统筹协调等，做好日常保密、宣传教育、风险排查、自查检查等各项任务；

d） 结合 GB/T 19001-2016 中 7.1.5)有关要求，建立执行评估实施日常监督制度，记录并监督评估现场工作情况，包括进出评估现场的设备使用及材料调阅情况、事前告知情况以及其他评估实施情况；

e） 建立执行评估报告审查制度，采用专家评审或内部审核方式，重点审核评估报告的科学性、完整性，评估过程证明材料的充分性、真实性，以及评估结论的客观性、准确性，通过审核的评估报告才可提供给被评估方；

f） 采取管理措施，限定数据安全评估活动仅于本机构内部开展，原则上不允许委托本机构外其他机构实施，国家监管部门或行业主管部门有规定或要求的除外；

g） 建立执行评估活动定期自查机制，对评估项目、人员、设备场所及安全保密管理等进行自查，自查周期不低于每年一次，发现问题隐患及时整改，并留存相关记录，自查内容包括但不限于：评估项目完成情况、评估报告完成、存放及管理情况、评估人员背景及行为规范情况、评估设备管理和使用情况、评估场所环境安全情况、评估实施安全管理情况等；

h） 建立变更管理制度，变更前与被评估方就具体事项主动沟通，经被评估方同意后，确保变更以受控的方式得到评估、批准和实施；变更后对评估目标、质量和效率、被评估方信息系统和业务造成影响的，应进行针对性的改进、补救或恢复；

i） 建立项目沟通与应急处置机制，应符合 GB/T 32914-XXXX 中 5.3.3c)中有关要求；

j） 建立上报制度，评估过程或评估机构内部管理中发现网络安全事件、安全漏洞时，应按合同或协议要求及时向被评估方报告，并记录事件相关内容，根据相关国家规定、标准要求进行报告和协助处置。

5.2.2 安全保密与人员管理

数据安全评估机构应充分考虑数据安全评估的特点，结合安全保密要求，建立并执行以下安全管理制度：

a） 评估人员应为与数据安全评估机构签订正式合同的员工；

b） 应建立数据安全评估人员管理制度，包括但不限于：

1） 建立并保存评估人员的人员档案，档案至少保存至评估人员离职后 5 年，有关法律法规、行业管理另有规定的除外，并与评估人员单独签订安全保密协议；

2） 应定期对评估人员开展岗位忠诚度心理测试、普法宣传、警示教育、安全保密教育培训、职业技能培训等，确保人员安全，提高评估人员安全保密意识；

3） 评估人员应在确认评估过程材料已完成归档且评估报告已发布的前提下，清除评估过程材料。

c） 评估任务开始前，应给出面向被评估方的保密承诺条款；

d） 应建立数据安全评估报告管理机制，机构内部指定统一归档部门，其它任何部门、个人不得留存评估报告和数据安全评估有关原始材料；

e） 应统一归档评估报告和过程材料，过程材料包括但不限于接收数据、资料的记录，关键人员沟通访谈的记录，漏洞、安全事件有关的原始数据等，并建立加密、访问控制、审计相关机制和技术措施；

f） 评估任务结束后，应按被评估方或合同、协议等的要求，进行数据的脱敏、移交、清理、销毁等处置；被评估方对处理情况提出核验或审计的，应予以充分配合；

g） 不得自行公开评估报告及评估过程材料，不得向评估授权方以外的任何组织和个人提供评估报告及评估过程材料，国家法律法规规定的除外；

注： 一般情况下，评估授权方指被评估的数据处理者；主管监管部门组织的数据安全评估，评估授权方指主管监管部门。

h) 其他用于防范评估过程数据泄露的安全管理制度和技术措施。

5.2.3 规范性管理

5.2.3.1 评估过程

数据安全评估机构应确保评估过程的规范性，包括但不限于：

a) 应能对评估依据的法律法规、标准规范进行公示；
b) 应确保评估结论可追溯、复现；
c) 应留存评估结论相关证明材料以及对应的数据处理活动状态和时间记录 5 年以上，用于复核验证。

5.2.3.2 评估机构行为

数据安全评估机构应制定评估活动行为准则，不得从事的活动内容包括但不限于：

a) 影响被评估对象正常运行，存在危害信息安全、数据安全等的行为，危害被评估对象安全；
b) 未与被评估对象对评估工作期间的保密工作进行充分协商，未制定切实方案，造成泄露知悉的被评估对象及被评估对象的国家秘密、商业秘密、工作秘密；
c) 故意隐瞒评估过程中发现的安全问题，或者在评估过程中弄虚作假，未如实出具数据安全评估报告；
d) 非授权占有、使用数据安全评估相关资料及数据文件；
e) 限定被评估对象购买、使用其指定的相关产品或服务；
f) 对系统或数据的操作超出合同、协议及被评估方等约定的范围；
g) 其他危害国家安全、社会秩序、公共利益以及损害个人、组织合法权益的活动。

5.2.4 风险控制

5.2.4.1 评估活动风险分析

数据安全评估机构应在评估实施前分析评估活动的潜在风险，制定应对措施并确认其有效性，对可能产生的风险、应对措施向被评估方进行风险提示，经其同意后采取影响最小的方式实施，潜在风险包括但不限于：

a) 评估机构因不可抗力导致的任务逾期、被评估方提供的材料不全导致评估结果不准确等方面的风险；
b) 评估活动可能对数据处理活动正常运行造成影响的风险，以及评估设备或工具接入可能对被评估系统正常运行造成影响的风险；
c) 其他可能危害被评估的数据处理者、被评估的数据处理活动相关数据主体的风险。

5.2.4.2 评估活动风险控制

数据安全评估机构应针对评估活动可能存在的风险实施对应的管理和技术措施加以控制：

a) 管理措施包括但不限于安全操作和意识培训、完善和宣贯安全操作规程等；
b) 技术措施包括但不限于对评估报告及有关证据性的访问日志审计、评估报告及有关证据性材料的加密措施等。

5.2.5 评估业务持续性保障管理

5.2.5.1 技术培训

数据安全评估机构应持续开展对评估人员的培训，培训内容应包括但不限于政策法规及标准规范、实践经验、评估案例、工具使用等内容，培训方式可采用内训、外训相结合的方式，数据安全评估人员每年培训时间应不少于20学时。

5.2.5.2 投诉处理

数据安全评估机构应制定投诉及争议处理制度，严格遵守申诉、投诉及争议处理制度，并应记录采取的措施。

5.2.5.3 持续优化

数据安全评估机构应建立持续优化机制，确定改进措施和计划，持续改进管理体系的适宜性、充分性和有效性。持续完善数据安全评估活动有关管理机制、操作手册、技术方法，总结形成技术指导书，持续跟踪国内外数据处理及数据安全评估相关技术发展，持续优化提升评估机构自身管理措施和技术能力。

5.3 评估技术能力

5.3.1 技术能力类型

数据安全评估机构应根据实际需要开展技术能力建设，包括不限于：

a) 数据安全风险评估技术能力；
b) 个人信息保护影响评估技术能力；
c) 数据出境安全评估技术能力；

5.3.2 数据安全风险评估技术能力

5.3.2.1 数据处理活动与数据资产识别分析

数据安全评估机构应具备数据处理活动与数据资产识别分析能力，包括但不限于：

a) 数据处理活动范围识别，在数据处理活动对应的数据处理者支持下，确定数据安全评估的对象、范围和边界，明确评估涉及的数据资产、数据处理活动、业务、信息系统、人员和内外部组织等；
b) 数据资产识别验证，根据数据处理者提供的数据分类分级规则和数据目录，验证数据分类分级情况、数据资产、数据属性，数据属性包括数据类别和级别、数据范围、数据规模、数据形态、元数据内容等；
c) 验证或绘制数据处理活动数据流图，数据流图应包括数据流转各环节经过的相关方、信息系统，以及每一个流动环节涉及的数据类型；
d) 数据处理活动各环节识别分析，识别数据处理活动目的，以及数据收集、存储、使用、加工、传输、提供、公开、删除活动环节的方式、范围等；
e) 数据处理活动相关方识别分析，识别数据处理者与相关方的关系，以及数据处理者与相关方的授权、协议、合同等约定事项，其中数据处理活动相关方包括但不限于个人、数据处理委托方、数据接收方等；
f) 数据处理活动保护措施识别分析和效果验证，识别已采用的网络安全防护措施，以及数据安全管理、技术方面相关保护措施术，包括不限于存储、传输数据的安全保护，并能够对安全保护效果进行验证；
g) 具备数据处理活动及数据处理者对应的行业领域和地区的数据安全相关法律法规及标准规范的基本知识。

5.3.2.2 数据处理活动风险源识别

数据安全评估机构应具备数据处理活动可能存在的风险源识别发现能力，包括但不限于：

a) 数据处理活动合理性判断，根据法律法规明确的合法、正当、必要等原则，参照有关标准规范，识别数据处理活动中存在的合理性方面风险问题，风险源包括但不限于未严格执行相关法律法规可能引发的法律风险和系统性风险、超范围收集、超限度提供、未与数据接收方约定数据处理方式和范围、非必要的监控画像、未授权个人生物识别信息收集、未取得授权的数据挖掘及衍生数据利用、存储期限不适当、删除不彻底、数据脱敏或去标识化不充分等；

b) 数据及信息系统保密性、完整性、可用性判断，识别因信息系统脆弱性以及数据保护措施不适当可能导致的风险问题，风险源包括但不限于存在安全漏洞、漏洞利用攻击防御手段不足、加密措施不适当、访问控制措施不适当、信息系统残留恶意代码、信息系统配置错误、传输方式不安全、审计监控措施不适当等。

5.3.2.3 数据处理活动风险分析与评价

数据安全评估机构应具备数据处理活动风险的分析与综合评价能力，包括但不限于：

a) 数据安全事件危害程度分析，针对识别出的风险源，结合数据处理活动分析风险源涉及的数据价值，以及事件对个人、组织、公众、国家带来的损害程度，综合分析风险源导致的数据安全事件发生时可能造成的危害程度级别；

b) 数据安全事件发生可能性分析，结合数据处理活动分析数据处理活动安全措施有效性、完备性，判断安全措施在控制风险问题中发挥的作用，结合数据安全事件的发生条件、历史事件等因素，综合分析风险问题导致的数据安全事件发生的可能性；

c) 风险综合评价，按照 GB/T AAAA-XXXX 中第 9 章风险评价有关要求，评价风险问题所处的风险区间。

5.3.2.4 数据处理活动风险控制建议

数据安全评估机构应具备提出风险处置措施建议能力，包括但不限于：

a) 根据评估过程中发现的数据安全风险提出处置建议，包括但不限于停止收集、缩小处理范围、补充签署协议、增加保护措施、完善策略配置、上报有关主管监管部门等；

b) 结合法律法规要求和数据处理活动实际情况，充分考虑 5.3.4-a)中风险处置措施的应用条件、应用场景、实施难易程度等因素，支撑风险处置措施建议的针对性、可操作性；

c) 对风险处置措施预期效果分析，判断风险处置措施发挥的作用，预估采取风险处置措施后的残余风险水平；

d) 对评估对象可能存在的法律法规风险进行提示，并对评估对象遵守国内相关法律法规，优化、完善内部管理措施提供建议。

5.3.3 个人信息保护影响评估技术能力

数据安全评估机构的评估活动涉及个人信息保护影响评估时，数据安全评估机构应具备的技术能力包括但不限于：

a) 个人信息处理活动涉及的敏感个人信息识别；

b) 个人信息保护政策分析；

c) 个人信息收集处理告知同意原则的分析，包括但不限于处理目的是否涉及强制要求或误导用户、是否由个人在充分知情的前提下自愿作出同意等；

d) 遵循有关法律法规，结合个人信息处理活动的核心业务功能，判断分析个人信息处理活动收集使用个人信息最小必要范围；
e) 对可能存在的自动化决策情况进行必要性分析、算法分析；
f) 个人信息处理活动对个人权益支持事项的查验分析，包括但不限于查询、更正、删除、撤回同意等；
g) 按照 GB/T 39335-2020 中 5.4 规定的风险源识别及 GB/T 39335-2020 中 5.5 规定的个人权益影响分析，进行个人信息安全风险分析。

5.3.4 数据出境安全评估技术能力

数据安全评估机构的评估活动涉及数据出境安全评估时，数据安全评估机构还应具备的技术能力包括但不限于：

a) 数据出境的目的、范围、方式等的合法性、正当性、必要性分析；
b) 境外接收方所在国家或者地区的数据安全保护政策和网络环境对出境数据安全的影响分析；
c) 境外接收方的数据保护水平是否达到中华人民共和国法律、行政法规的规定和强制性国家标准的要求分析；
d) 出境数据的规模、范围、种类、敏感程度识别；
e) 数据出境中和出境后遭到篡改、破坏、泄露、丢失、转移或者非法获取、非法利用等风险分析；
f) 数据安全是否能够得到充分有效保障的分析；
g) 数据处理和境外接收方拟订立的法律文件中是否充分约定了数据安全保护保护责任分析能力。

5.4 评估人员能力

5.4.1 评估团队组成

数据安全评估队伍构成要求如下：

a) 评估机构从事安全检测、评估相关工作人员不少于 15 名；
b) 评估机构从事 5.1.2-b)中数据安全相关检查、检测、评估项目或任务的人员不少于 10 名；
c) 评估团队应不少于 10 人获得数据安全、信息安全相关的资格证书，包括但不限于：信息安全保障人员认证（CISAW）、注册信息安全专业人员（CISP）、计算机技术与软件专业技术资格（水平）高级证书等信息安全相关专业培训或资格认证。从事特定行业、领域等的评估活动，应具备相应的专业技术能力；
d) 单项评估活动组建的评估团队根据评估领域配备专业人员，且职责分工合理；
e) 单项评估活动组建的评估团队应至少包含 1 名项目负责人、1 名技术负责人、以及不少于 3 名评估人员；
f) 单项评估活动应具有稳定的评估团队。

5.4.2 人员能力

数据安全评估人员能力要求包括：

a) 应熟悉数据安全、个人信息保护相关的法律法规和标准规范；
b) 应熟练掌握数据安全风险评估方法，包括但不限于：
   1) 根据数据处理者提供的信息，识别、验证数据处理活动，核查数据资产；
   2) 根据法律法规、标准规范在实际评估过程中判断数据合法利用相关问题，能够发现数据处理活动相关信息系统可能存在的管理和技术方面问题；

3) 熟悉数据分类分级有关标准中关于数据级别、类别的规范及对应的可能危害影响，能够根据实际评估场景中的问题对应的数据属性进行判断；
4) 了解数据收集、存储、使用、加工、传输、提供、公开、删除等活动的保护措施，能够根据实际评估场景判断对应活动环节保护措施的有效性、适当程度；
5) 依据数据安全风险评估方法，从风险发生的危害影响和可能性方面客观判断数据处理活动相关环节的风险区间。

c) 应具有网络数据安全相关标准应用实践经验或具有数据安全相关项目研究或应用经验，能够根据评估结果做出专业判断并出具评估报告；
d) 应掌握访谈、验证、技术检测等测评方法，对于专门实施技术查验和测试的人员还应具备熟练使用网络安全测试、数据安全评估等工具的能力；
e) 应经过数据安全评估相关专门培训，并取得相关资质。

5.5 评估资源要求

5.5.1 场所和环境

数据安全评估机构自身场所和环境应具备以下能力要求：

a) 具有固定的办公场所，评估工作场地环境安全、功能布局等应符合质量管理的相关规定，并配有必要的防污染、防火、控制进入等安全措施；
b) 各评估实验室的不同评估区域开展项目时应当互不影响；
c) 对评估方法或评估设备有要求的，环境条件应满足业务开展，不应对结果有效性产生不利影响。

5.5.2 设备和设施

数据安全评估机构开展数据安全评估的设备、设施、工具应具备以下能力要求：

a) 具备符合相关要求的机房以及必要的软、硬件设备，满足技术培训、评估验证和模拟测试的需要；
b) 配备满足数据安全评估工作需要的评估设备和工具，评估设备和工具类型见附录 C；
c) 用于数据安全评估的设备和工具应满足以下基本条件：
   1) 建设、研制单位在中华人民共和国境内具有独立的法人资格，由中国公民、法人投资或者国家投资或者控股的；
   2) 设备和工具的功能应仅限于其声明的功能，不得包含后门、隐蔽通道及其他恶意功能，由建设、研制单位出具证明；
   3) 应配备未被有关部门通报存在问题的，经安全认证合格或安全检测符合要求的设备和工具，设备和工具应通过权威机构的检测并可提供检测报告。
d) 评估设备和工具需要定期核查、持续更新，确保工具的合法版权且授权在有效期内，运行状态良好，关注工具及其组件的安全漏洞公告和相关信息，及时更新维护；
e) 在评估活动结束、完成归档后，应对评估设备和工具产生的数据安全评估活动相关的日志、记录进行清除；
f) 具有完备的设备和工具管理制度。对设备档案和标识管理，以及故障设备和工具管理有明确要求。对评估设备和工具统一登记、统一标识，标识完整、摆放合理，具有配套防护措施，对于有故障的设备和工具应通过加盖明显标识进行区分，并采取有效措施防止继续使用；
g) 设备具有完整的工作维护规程、设备使用说明书、校准或确认报告使用记录、定期维修核查制度和记录，存放地点及保管人等信息规范完整；

h) 对人员、工具等资源进行调配，根据被评估方需要以书面承诺等方式向被评估方说明资源配置、保障情况。

附 录 A
（资料性）
数据安全评估机构能力证明方法

表A.1给出了数据安全评估机构能力证明方法，包括能力类别、能力项、证明或评定方式等内容。

表A.1 能力证明方法

序号	能力类别	能力项	证明或评定方式
1	机构基本条件	基本条件	机构背景方面材料审核
2		评估工作基础	实践案例方面材料审核
3		公正与独立性	机构背景方面材料审核、承诺函
4	评估管理能力	实施管理	管理制度、作业指导书方面材料审核
5		安全保密与人员管理	管理制度、安全保密制度方面材料审核，技术措施现场查验
6		规范性管理	管理制度方面材料审核
7		风险控制	风险管理制度方面材料审核 风险控制技术措施现场查验
8		评估业务持续性保障管理	培训记录、投诉处理制度、更新机制、研究成果等相关材料审核，历史投诉情况审核
7	评估技术能力	数据处理活动与资产识别分析	实践案例证明或模拟案例分析考核
8		数据处理活动风险源识别	
9		数据处理活动风险分析与评价	
10		数据处理活动风险控制建议	
11		个人信息保护影响评估技术能力（如涉及）	
12		数据出境安全评估技术能力（如涉及）	
13	评估人员能力	评估团队组成	人员方面材料审核
14		人员能力	现有相关资质材料审核、技能考核或考试
15	评估资源需求	场所和环境	现场查验
16		设备和设施	设备设施相关材料审核、现场查验

附 录 B
（资料性）
设备和工具类型

数据安全评估设备和工具是数据安全评估的辅助手段，根据数据安全评估过程中任务场景、作用原理的不同，评估设备和工具包括但不限于检测类、监测类、分析类、扫描类、测试类等。表B.1给出了数据安全评估工作中可能需要的评估设备和工具类型示例。

表B.1 设备和工具类型

序号	类型	示例
1	检测类	如APP安全检测分析工具、数据资产识别工具、恶意代码检测工具等。
2	监测类	如API风险监测工具、数据审计工具等。
3	分析类	如符合性分析工具、元数据分析工具、算法评估分析工具、网络协议分析工具、网络流量分析工具等
4	扫描类	如漏洞扫描工具、内存恶意代码残留扫描工具等。
5	测试类	如渗透测试工具等。

参 考 文 献

[1] GB/T 32921—2016 信息安全技术 信息技术产品供应方行为安全准则
[2] GB/T 35280—2017 信息安全技术 信息技术产品安全检测机构条件和行为准则
[3] GB/T 36959—2018 信息安全技术 网络安全等级保护测评机构能力要求和评估规范
[4] GB/T 35273—2020 信息安全技术 个人信息安全规范
[6] RB/T 220—2018 检验检测机构资质认定能力评价 信息安全检验检测机构要求
[7] YD/T 0152—2020 电信网和互联网数据安全评估服务机构能力认定准则