数据安全风险评估服务认证自评价表

自评价方名称	
服务类型	数据安全风险评估服务
自评价时间	

1 服务管理审核 GB/T 45389-2025《数据安全技术--数据安全评估机构能力要求》第 5 章

序号	标准条款				评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
1	5 能力要求	5.1 基础条件	5.1.1 基本条件	数据安全评估机构具备的基本条件如下： a）在中华人民共和国境内注册；	1、是否在中国境内注册成立？	描述对应评价项的要求，相关的自评价过程、方法和证据，例如：在全国统一社会信用代码查询平台查验了申请单位的资质证明，《XXXX》No.xxxxxx，其场所地址为 XXXXX，有效期为 XXXX-XXXX。	描述自评价结论，例如：符合（不符合或不适用，在备注中说明情况）	
2				b)法定代表人、主要负责人为中华人民共和国境内的中国公民，且无犯罪记录；	1、法定代表人、主要负责人是否具有中国国籍？			
3					2、每年是否对法定代表人、主要负责人开展无犯罪记录调			

序号	标准条款	评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
		查？			
4	c)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；	1、高层管理人员是否被列入中国执行信息公开网--失信执行人名单？			
5		2、是否被国家税务总局列入重大税收违法失信案件信息公布栏名单？			
6		3、是否被列入中国政府采购网--政府采购严重违法失信行为记录名单？			
7		4、是否被国家商务部列入不可靠实体清单？			
8		5、是否被列入信用中国--严重失信主体名单？			
9	d)应具有中国合格评定国家认可委员会颁发的实验室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、网络安全、数据安全等检验检测相关内容；	1、是否具有中国合格评定国家认可委员会颁发的实验室认可证书或检验机构认可证书，证书是否处于有效状态？			
10		2、提供的 CNAS 证书附件中的能力范围是否包含信息安全、网络安全、数据安全等检验检测相关内容？			

序号	标准条款				评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
11				e）应满足GB/T 32914—2023第5章相关要求；	1、对评估过程中所获取数据的保护措施是否满足GB/T 32914-2023第5章5.9中的相关要求，包括： a）评估前是否与被评估方约定评估过程中数据（包括个人信息、业务数据、系统数据、安全数据）及相关材料的保护要求及保护措施，是否明确数据的使用目的和周期、最小处理范围、最小特权访问、事后处置等保护措施？ 注1：约定数据安全保护的条款的方式包括在服务协议中专门体现或签署单独的数据安全保护协议。 注2：现场提供网络安全服务的，明确项目相关资料是否能被外带的要求。 注3：涉及纸质资料的，明确是否可被电子化。 b）是否未曾将评估过程中获取的数据用于其他目的、向第三方提供或公开，服务协议中明确授权或经服务需求方同意的			

序号	标准条款	评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
		除外？ c）是否采取加密、签名、备份等必要的安全措施保证评估过程中获取的数据的保密性、完整性、可用性和真实性，是否未经服务需求方同意情况下更改、删除和销毁原始数据？ d）确因服务需要向境外提供和传输评估过程中获取的数据，是否遵守数据出境管理相关法律法规的要求，是否在事前向被评估方告知出境目的、数据种类、数量、周期和接收方等情况，并取得被评估方书面同意？ e）评估完成后，是否按被评估方和协议的要求进行数据的脱敏、移交、清理或销毁等处理，是否在被评估方提出对数据处理情况进行核验、审计时予以充分配合？ 注：包括服务工具中残留数据的处置。			

序号	标准条款				评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
12					2、是否具备 GB/T 32914-2023 第 5 章 5.11 中要求的检测评估服务能力，包括： a）是否具备基本的检测评估相关服务工具研发能力或二次开发能力？ b）是否按照 GB/T 20984 的规定对风险进行识别、定性或定量分析和评价？ c）需开展漏洞扫描和渗透测试等可能会对被评估方系统、业务和数据等造成影响的，是否向被评估方单独告知影响、风险及应对措施，是否在被评估方同意后采取影响最小的方式实施？ d）在测试环境中开展风险评估的，是否预先分析测试环境与真实环境的区别，是否向被评估方告知评估结果的适用范围？ e）是否对评估所发现的安全问题和风险等提出安全整改建议，是否在服务需求方完成整			

序号	标准条款				评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
					改后验证整改效果（服务需求方无相关需求的除外）？ f）是否妥善留存评估报告等服务交付成果，留存时间不少于6年（有关法律法规和行业管理另有规定的除外）？			
13				f）宜具备数据安全相关检查、检测、评估的服务项目或任务实施经验。	1、是否支撑有关部门开展过数据安全检查工作或具有数据安全检测、评估、咨询服务项目案例？			
14			5.1.2 评估工作公正性与独立性要求	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；	1、是否制定了机构行为规范，规范内容是否至少包含：评估过程严格执行有关法律法规、标准规范，遵守客观公正原则，对评估过程和结果的公正性负责，不向评估对象推荐、指定产品或服务。			
					2、是否正式声明按照行为规范要求开展评估活动？			
				b）对其评估活动的公正性负责，不受可能来自商业、财务或其他方面的压力而影响公正	1、评估活动是否不受来自商业、财务或其他方面的压力而影响公正性？			

序号	标准条款				评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
				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，由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；	1、除国家机关授权或评估机构内部独立开展的数据处理活动外，是否从事过面向公众、被评估对象开展的网络数据处理活动？			
				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；	1、除自用评估工具外，评估机构是否涉及数据安全产品开发、销售、集成、运营等活动？是否从事信息技术产品开发、销售和信息系统集成实施等活动？			
				e）不向评估对象推荐、指定产品或服务。	1、是否存在向评估对象推荐、指定产品或服务的行为？			
15		5.2 管理能力	5.2.1 制度措施	数据安全评估机构应建立、执行数据安全评估制度和措施，包括但不限于以下方面： a）评估项目实施前组	1、是否建立与数据安全风险评估相关的管理制度，明确评估项目实施前组建评估团队、编制评估计划或方案的机制和流程？			

序号	标准条款				评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
16				建评估团队、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。	2、编制的评估计划或方案中是否包含评估目标、范围、评估方式、投入资源（人力、设备等）、时间进度等内容，是否得到被评估方的认可？			
17				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，重点审核评估方案是否明确被评估对象的数据处理活动范围，以及拟投入的相关资源、评估实施周期等内容是否适当等。	1、是否建立评估方案审核管理制度，并对方案的制定开展评审或审核，评审或审核内容包括但不限于被评估对象范围是否明确、拟投入审计资源（人力、设备等）是否满足、实施时间安排是否适当等？			
18				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。	1、是否建立与数据安全风险评估相关的管理制度，包括管理责任部门、管理责任范围、责任人、工作流程、安全管控措施及内部各部门间协作机制？			
19					2、是否建立措施保障每年开展数据安全风险评估业务保密宣传教育、风险排查、自检自查等工作？			

序号	标准条款				评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
20				d）结合 GB/T 19001—2016 中相关要求，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等。	1、是否建立评估实施日常监督制度，记录并监督评估现场工作情况，包括但不限于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等？			
21				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。	1、是否建立评估报告审核管理制度，报告审核人员能否针对报告内容的科学、完整性作出评审？			
22					2、是否建立评估报告审核管理制度，报告审核人员能否针对合规审计过程证明材料的充分性、真实性作出评审？			
23					3、是否建立评估报告审核管理制度，报告审核人员能否针对审计结论的客观、准确性作出评审？			

序号	标准条款				评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
24				f）采取管理措施，限定数据安全评估活动仅在本机构内部开展，原则上不准许委托本机构外其他机构实施。	1、是否制定机构行为规范或管理措施，限制评估活动不得转委托其他机构实施，是否建立措施确保评估活动仅在机构内部开展？			
25				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：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。	1、是否建立评估工作定期自查机制，明确自查内容至少包括：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？			
26					2、是否至少每年一次按照自查机制开展了评估自查工作，是否根据自查结果对发现的必要问题隐患进行整改或说明？			

序号	标准条款	评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
27	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，进行针对性的改进、补救或恢复。	1、是否建立评估变更管理制度，明确需进行变更审批的事项及变更事操作流程？			
28		2、是否建立机制使得评估变更前得到被评估对象的意见，变更实施采用受控方式？			
29		3、变更后造成评估目标、质量和效率、被评估对象信息系统和业务影响的，能否具有进行补救或恢复的处理机制？			
30	i）建立项目沟通与应急处置机制。	1、是否建立了项目沟通与应急处理机制，明确数据安全事件的处置流程？			
31	j）建立报告制度，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	1、是否能在评估过程或评估机构内部管理中监测到可能发生的网络安全事件、数据安全事件、安全漏洞等？			
32		2、发现安全事件或漏洞时，是否能按合同或协议要求及时向被评估对象报告，并记录事件相关内容，并根据相关国家规			

序号	标准条款				评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
				准要求进行报告和协助处置。	定、标准要求进行报告和协助处置？			
33			5.2.2 人员管理与安全保密	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） 评估人员为与数据安全评估机构签订正式合同的员工。	1、是否与评估人员签订了正式合同？			
34				b）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6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；	1、是否建立评估人员管理制度，明确人员档案管理要求、培训要求、材料管理要求等？			
35					2、是否建立并保存评估人员的人员档案，档案保存时间是否不少于 6 年？			
36					3、是否与评估人员单独签订安全保密协议？			
37					4、是否定期对评估人员开展岗位心理测试、普法宣传、警示教育、安全保密教育培训、职			

序号	标准条款	评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
	2）定期对评估人员开展岗位心理测试、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；	业技能培训？			
38	3）评估人员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。	5、是否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？			
39	c）评估任务开始前，给出面向被评估方的保密承诺条款。	1、评估任务开始前，是否给出面向被评估方的保密承诺条款？			
40	d）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，其他任何部门、个人不应留存评估报告和数据安全评估有关原始材料。	1、是否建立数据安全评估报告管理机制，其中是否明确指定统一归档部门，是否规定其他任何部门、个人不应留存评估报告和数据安全评估有关原始材料？			
41	e）统一归档评估报告和过程材料，过程材料	1、是否对评估报告和过程材料进行统一归档，过程材料包括			

序号	标准条款				评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
				包括接收数据、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。	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？			
42					2、是否建立加密、访问控制、审计相关机制和技术措施，对评估活动归档材料的调取进行全流程管控？			
43				f）评估任务结束后，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，予以充分配合。	1、评估任务结束后，是否按被评估方或合同、协议等的要求，进行数据的脱敏、移交、清理、销毁等处置？			
44					2、被评估方对处理情况提出核验或审计的，是否予以充分配合？			
45				g）不应自行公开评估报告及评估过程材料，不应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。	1、是否未曾自行公开评估报告及评估过程材料，国家法律法规规定的除外，是否未曾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？			

序号	标准条款					评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
46				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。		1、是否建立并执行其他防范评估过程数据泄露的安全管理制度。			
47						2、是否建立并执行其他防范评估过程数据泄露的技术措施，如加密传输、加密存储等？			
48			5.2.3 评估过程与行为管理	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)告知开展评估的依据；	1、是否制定评估过程规范制度或流程，对评估前告知评估依据、留存评估过程相关证明材料、评估结论的可追溯性等进行明确要求？			
49						2、在开展评估活动前，是否明确告知被评估方评估活动的依据（包括但不限于依据标准、参考标准等内容）？			
50					b)确保评估结论可追溯、过程可复现；	1、是否完整留存评估活动的输入信息（包括但不限于系统架构图、系统拓扑图、数据资产清单、数据流向图、访谈记录、调查结果等），评估过程记录，评估工具过程记录等相关证明材料，相关证明材料与最终评估结论是否一致？			

序号	标准条款					评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
51					c)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6年以上，用于复核验证。	1、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的留存时间是否能够确保在6年以上？			
52				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，不应从事的活动内容包括但不限于：	1、是否制定了评估活动行为准则，是否采取措施确保所有数据安全风险评估人员均知晓评估活动行为准则？			
53					a)影响被评估对象正常运行，危害被评估对象安全；	1、制定的评估活动行为准则中是否涵盖以下内容： （a）不应从事影响被评估对象正常运行，危害被评估对象安全的活动；			
					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	（b）评估工作开展前，应当与被评估方针对评估工作期间的保密工作进行充分协商，避免造成泄露知悉的被评估对象及被评估对象的国家秘密、工作			

序号	标准条款	评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
	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、工作秘密、商业秘密、个人隐私等；	秘密、商业秘密、个人隐私等数据；			
	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；	（c）不得故意隐瞒评估过程中发现的安全问题，不得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；	（d）不得非授权占有、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	e）不得限定被评估对象购买、使用其指定的相关产品或服务；			

序号	标准条款					评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
					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；	（f）对系统或数据的操作不能超出合同、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。	（g）不得开展其他危害国家安全、社会秩序、公共利益以及损害个人、组织合法权益的活动。			
54			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	1、是否建立数据安全评估风险控制机制，明确评估活动流程中的风险点及管控要求，并能以适当方式对评估对象予以提示？			
55						2、是否能在协议等有效力的文件中明确约定或提示评估机构因不可抗力问题导致的任务逾期风险及应对措施？			

序号	标准条款					评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
56					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；	3、是否能在协议等有效力的文件中明确提示因被评估方提供的材料不全导致评估结果不准确性风险及补救措施？			
57					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；	1、是否能在协议等有效力的文件中明确评估活动对被评估方业务运行可能造成的影响及应对措施？			
58						2、是否建立相应机制能在评估活动中明确提示设备或工具接入对被评估方系统正常运行可能造成的影响及应对措施？			
59						3、无论被评估对象是否同意接受接入设备或工具带来潜在风			

序号	标准条款					评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
						险的，评估机构能否得到其明确意见？			
60					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。	1、是否在协议中约定因技术措施无法实现对数据处理活动产生的风险及应对措施？			
61						2、是否在协议中约定因评估人员操作不当导致被评估方面临的风险及应对措施？			
62						3、是否在协议中约定对评估范围内数据处理活动涉及的被评估主体造成的损害风险及责任承担？			
63				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）管理措施包括安全操作和意识培训、完善和宣贯安全操作规程等；	1、是否在相关制度中明确应急预案的管理要求及触发条件？			
64						2、是否具有评估活动应急预案，并明确不可抗力导致逾期情形下的替代方案？			
65						3、是否规定应急管理规程相关文件的修订完善要求，并将最新版本文件进行发布或宣贯？			

序号	标准条款					评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
66					b)技术措施包括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。	1、配备的评估活动工具是否具有安全可靠的证明？			
67						2、是否能采用人员权限访问控制、加密传输、加密存储、过程留痕等技术措施将评估实施风险尽可能降低？			
68			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，培训内容应包括政策法规及标准规范、实践经验、评估案例、工具使用等，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	1、是否制定了数据安全评估人员培训计划，培训内容是否包括政策法规、标准规范、实操教学、案例分析等？			
69						2、是否留存培训记录，数据安全风险评估人员每年培训时长不低于 20 个学时？			

序号	标准条款					评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
					时。				
70				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。	1、是否制定了申诉、投诉及争议处置管理制度？是否留存相应的记录。			
71						2、是否保障申投诉渠道畅通？			
72				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	1、是否在相关管理制度中明确数据安全评估业务相关的政策标准跟踪、持续改进目标、改进措施和计划等？			
73						2、是否针对数据安全评估活动开展过程中发现的问题形成指导性文件，如作业指导书、技术手册等，并定期评审更新？			

序号	标准条款					评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
					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。				
74		5.3 技术能力	5.3.1 数据安全风险评估的技术能力	5.3.1.1 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）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；	1、是否收集和整理所在行业或地区数据安全相关法律法规及标准规范，是否做好内部相关人员培训与考试，是否能够按照法规识别违规行为？			
75						2、是否能保障人员知晓行业或地区数据安全相关法律法规及标准规范的制定和施行情况？			

序号	标准条款					评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
76					b）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；	1、是否制定了数据安全保护风险识别指南等指导文件用于帮助明确风险评估对象、风险评估范围和边界，以及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？			
77					c）数据资产识别，根据数据处理者提供的数据分类分级规则和数据目录，识别数据分类分级情况、数据资产、数据属性，数	1、是否能够识别数据资产的数据分类分级情况、数据资产、数据属性等要素，数据属性是否涵盖数据类别和级别、数据范围、数据规模、数据形态、元数据内容等？			

序号	标准条款	评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
	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；				
78	d)识别或绘制数据处理活动数据流图，数据流图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等；	1、是否能识别或绘制数据处理活动数据流图？			
79		2、数据流程图是否能涵盖数据流转各环节的相关方、信息系统、数据类型？			
80	e)数据处理活动各环节识别，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、	1、是否能针对业务场景识别发现数据流转处理活动各项环节及处理目的？			
81		2、是否能识别数据处理活动目的、数据处理各环节活动，涵盖的数据类型和系统范围？			

序号	标准条款	评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
	公开、删除活动环节的方式、范围等；				
82	f）数据处理活动相关方识别，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个人、数据处理委托方、数据接收方等；	1、是否在指导文件中明确数据处理活动相关方的类型及概念？			
83		2、是否能准确识别数据处理活动相关方的关联关系、合同或授权效力等？			
84	g）数据处理活动保护措施识别，识别已采用的网络安全	1、是否具有数据处理活动保护措施的识别能力，能够有效识别已采用的网络安全、数据安全、技术保护措施等？			

序号	标准条款					评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
85					防护措施，以及数据安全管理、技术方面相关保护措施等。	2、是否能对技术保护措施进行检测及验证其有效性？			
86				5.3.1.2 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，风险源包括未	1、是否具有参照有关标准规范合法、正当、必要识别数据处理活动中存在的合理性方面风险问题的能力？			
87						2、是否具有识别数据处理活动中存在的合理性方面风险问题的能力，风险源包括未严格执行相关法律法规和标准规范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，以及数据脱敏、去标识化或匿名化不充分等？			

序号	标准条款					评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
					严格执行相关法律法规和标准规范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，以及数据脱敏、去标识化或匿名化不充分等；				

序号	标准条款	评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
88	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验证数据保护措施不适当可能导致的风险问题，风险源包括存在安全漏洞、利用漏洞攻击防御手段不足、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或存在恶意软件、信息系统配置错误、传输方式不安全、审计监控措施不适当	1、是否具有依据数据及信息系统保密性、完整性、可用性进行风险源判断的能力？			
89		2、是否具有识别因信息系统脆弱性以及验证数据保护措施不适当可能导致的风险问题的能力，风险源包括存在安全漏洞、利用漏洞攻击防御手段不足、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或存在恶意软件、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？			

序号	标准条款					评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
					等。				
90				5.3.1.3 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	1、是否具有准确判断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的能力？			
91						2、是否具有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的能力？			

序号	标准条款					评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
					造成的危害程度级别；				
92					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；	1、是否能够结合数据处理活动分析数据处理活动安全措施有效性、完备性准确判断安全措施在控制风险问题中发挥的作用？			
93						2、是否能够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？			
94					c）风险综合评价，综合数据安全风险危害程度和数据安	1、是否具有综合数据安全风险危害程度和数据安全风险可能性，评价数据安全风险所处的风险区间的能力？			

序号	标准条款					评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
					全风险可能性，评价数据安全风险所处的风险区间。				
95				5.3.1.4 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控制措施建议能力，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控制建议，包括停止收集、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；	1、是否能根据评估过程中发现的数据安全风险提出相应风险控制建议，包括停止收集、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？			
96					b)结合法律法规要求和数据	1、提出的风险控制措施建议是否符合法律法规要求，是否充			

序号	标准条款					评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
					处理活动实际情况，充分考	分考虑应用条件、应用场景、实施难易程度等因素？			
97					虑 5.2.4 中风险控制措施的应用条件、应用场景、实施难易程度等因素，支撑风险控制措施建议的针对性、可操作性；	2、风险控制措施建议是否具有针对性、可操作性？			
98					c）对风险控制措施预期效果分析，判断风险控制措施发挥的作用，预估采取风险控制措施后的残余风险水平；	1、是否能判断风险控制措施发挥的作用，是否能预估采取风险控制措施后的残余风险水平？			
99					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	1、是否能对评估对象可能存在的法律法规风险进行提示？			
100						2、是否能对评估对象遵守国内相关法律法规，优化、完善内			

序号	标准条款					评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
					国内相关法律法规，优化、完善内部管理措施提供建议。	部管理措施提供建议？			
101			5.3.2 个人信息保护影响评估的技术能力	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以下方面： a）个人信息处理活动涉及的敏感个人信息识别。		1、是否能准确识别个人信息处理活动涉及的敏感个人信息？			
102				b）个人信息保护政策分析。		1、是否能根据个人信息保护政策进行个人信息保护影响评估分析？			
103				c）个人信息收集处理告知同意原则的分析判断，包括处理目的是否涉及强制要求或误导用户、是否由个人在		1、是否能准确分析判断个人信息收集处理的目的?			
104						2、是否能分析判断个人信息收集处理的目的是否涉及强制要求或误导用户？			

序号	标准条款	评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
105	充分知情的前提下自愿作出同意等。	3、是否能分析判断个人信息收集处理是否基于告知同意的原则？			
106	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，分析实际收集个人信息的种类、方式、上传情况等，包括是否存在超出最小必要范围或个人授权范围收集个人信息的情况；分析实际向第三方提供个人信息情况，包括是否存在超出最小必要范围或个人授权范围向第三方提供个人信息的情况。	1、是否能准确判断个人信息收集是否遵循有关法律法规？是否结合个人信息处理活动的核心业务功能？			
107		2、是否能准确分析实际收集个人信息的种类、方式、上传情况等，包括是否存在超出最小必要范围或个人授权范围收集个人信息的情况？			
108		3、是否能准确分析实际向第三方提供个人信息情况，包括是否存在超出最小必要范围或个人授权范围向第三方提供个人信息的情况？			
109	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。	1、是否能判断可能存在的自动化决策情况？			
110		2、是否能对可能存在的自动化决策情况进行必要性分析、算法分析？			

序号	标准条款				评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
111				f）对个人信息保护措施是否适当进行分析。	1、是否能对个人信息保护措施进行适当分析？			
112				g）个人信息处理活动对个人权益支持事项的查验分析，包括查询、更正、删除、撤回同意等。	1、是否能对个人信息处理活动中个人权益支持事项进行查验分析，包括查询、更正、删除、撤回同意等？			
113				h）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。	1、是否能依据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？			
114			5.3.3 数据出境安全评估的技术能力	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	1、是否能对数据出境的目的、范围、方式进行合法性、正当性、必要性分析？			

序号	标准条款	评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
	析；				
115	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；	1、是否熟悉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？			
116		2、是否能对出境数据安全的影响进行分析？			
117	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；	1、是否熟悉境外接收方的数据保护水平？			
118		2、是否能对境外接收方的数据保护水平进行分析，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？			
119	d）出境数据的规模、范围、种类、敏感程度识别；	1、是否能对出境数据的规模、范围、种类、敏感程度进行识别？			
120	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；	1、是否能对数据出境中遭到篡改、破坏、泄露、丢失、转移或者非法获取、非法利用等进行风险分析？			
121		2、是否能对数据出境后遭到篡改、破坏、泄露、丢失、转移或者非法获取、非法利用等进			

序号	标准条款				评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
					行风险分析？			
122				f）数据安全是否能够得到充分有效保障的分析判断；	1、是否能对数据安全的保障措施进行分析判断？			
123				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责任分析能力。	1、是否能判断数据处理和境外接收方拟订立的法律文件符合法律法规要求？			
124					2、是否能对数据处理和境外接收方拟订立的法律文件进行分析？			
125		5.4 人力资源能力	5.4.1 评估团队组成	数据安全评估团队构成要求如下： a）评估机构从事数据安全相关检查、检测、评估项目或任务的人员应不少于 10 名；	1、是否具有不少于 10 名数据安全风险评估人员？			
126					2、是否能定期对所有级别人员能力开展自评价，重点评价技术能力和项目经历等？			
127				b）评估团队应不少于 10 人获得数据安全、数据安全评估、信息安全等相关的资质证书，从事特定行业、领域等的评估活动，应具备相应	1、是否具有不少于 10 名数据安全风险评估人员获得数据安全、数据安全评估、信息安全等相关的资质证书？			
128					2、数据安全风险评估人员证书是否均在有效期内？			

序号	标准条款				评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
129				的专业技术能力； c）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，应至少包含项目负责人、技术负责人、评估人员等，职责分工合理，人员稳定。项目负责人、技术负责人具备至少1项数据安全相关检查、检测、评估项目或任务经验。	3、是否能定期对从事特定行业、领域的数据安全风险评估人员进行相应的专业技术能力考核？			
130					1、是否具有数据安全风险评估管理组织架构及职责说明，明确各岗位各级别数据安全风险评估人员管理要求及职责？			
131					2、组建的评估团队是否根据评估领域配备相对应的专业人员？			
132					3、数据安全风险评估团队是否包含项目负责人、技术负责人、评估人员等角色？			
133					4、项目负责人、技术负责人是否具有数据安全相关检查、检测、评估项目或任务经验？			
134			5.4.2 人员能力	数据安全评估人员能力要求如下。 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。	1、是否能定期对数据安全评估人员所掌握的数据安全、个人信息保护相关的法律法规和标准规范的熟悉程度进行考核？			

序号	标准条款	评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
135	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类别、级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、	1、是否能根据数据处理者提供的信息准确识别和验证数据处理活动，以及准确核查数据资产？			
136		2、在实际评估过程中是否能根据法律法规、标准规范准确判断数据的合法利用相关问题？			
137		3、是否能及时发现数据处理活动相关信息系统可能存在的管理和技术问题？			
138		4、是否能定期对数据安全评估人员进行能力考核，涵盖数据类别、级别的规范及对应的可能危害影响？			
139		5、在实际评估过程中是否能及时对数据属性进行判断？			
140		6、数据安全评估人员能力是否了解数据收集、存储、使用、加工、传输、提供、公开、删除等活动的保护措施？			
141		7、在实际评估过程中是否能准确判断对应活动环节保护措施的有效性、适当程度？			

序号	标准条款				评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
142				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。	8、是否能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？			
143				c）应具有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。	1、数据安全评估人员是否具有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？			
144					2、数据安全评估人员是否能够根据评估结果做出专业判断并出具评估报告？			
145				d）应掌握访谈、验证、技术检测等测评方法，对于实施技术查验和测试的人员还应具备	1、是否能定期对数据安全评估人员测评方法掌握情况进行检验，涵盖访谈、验证、技术检测等？			

序号	标准条款				评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
146				熟练使用网络安全测试、数据安全评估等工具的能力。	2、实施技术查验和测试的数据安全评估人员是否能熟练使用网络安全测试、数据安全评估等检测工具？			
147				e）应经过数据安全评估相关培训，并取得相关资质。	1、数据安全评估人员是否经过数据安全评估相关培训？			
148					2、数据安全评估人员是否取得相关资质？			
149		5.5 场所与设备资源能力	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；	1、是否具有固定的办公场所？			
150					2、办公场地是否能保证环境安全，功能布局符合质量管理规定，如材料抗震等级、消防安全证明等？			
151					3、办公环境是否配备了灭火装置，是否在具有防污染措施，以及进出访问控制、视频监控措施？			
152				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；	1、是否能够确保评估实验室的不同评估区域开展项目时应当互不影响？			

序号	标准条款				评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
153				c）对评估方法或评估设备有要求的，确保环境条件满足业务开展，且不对结果有效性产生不利影响。	1、是否能保证评估工具或设备的存放条件满足设备正常运转需要，防止对评估结果的有效性产生不利影响？			
154					2、是否能保证评估工具或设备得到物理防护，禁止未授权的使用，防止对评估结果的有效性产生不利影响？			
155			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。	1、是否具备符合评估活动相关要求的机房？			
156					2、是否针对评估活动中的技术检测需求配备了软/硬件设备资源？			
157					3、软/硬件设备是否能满足技术培训、评估验证和模拟测试的需要？			
158				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 B。	1、是否配备了数量能够满足机构开展数据安全评估工作需要的设备和工具？			
159					2、评估设备和工具的知识库版本是否为最新？			

序号	标准条款				评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
160				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)设备和工具的功能仅限于其声明的功能，不应包含后门、隐蔽通道其他恶意功能，由建设、研制单位出具证明； 2）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，应通过权威机构的检测并提供检测报告。	1、评估设备和工具的功能仅限于其声明的功能，不应包含后门、隐蔽通道其他恶意功能，是否具有建设、研制单位出具的相关有效证明材料？			
161					2、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，是否通过权威机构的检测，是否具有相关检测报告？			
162				d）评估设备和工具在投入使用前需要对其安全性进行验证确认，在使用期间定期核查、持续更新，确保工具的合法版权且授权在有	1、评估人员是否能在评估设备和工具投入使用前进行安全验证确认？			
163					2、评估人员是否在使用前进行评估设备和工具版本更新确认？			

序号	标准条款	评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
164	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。	3、是否保证评估设备和工具具有合法版权且授权在有效期内？			
165		4、是否有专人对评估设备和工具及其组件的安全漏洞进行管理，做到及时更新维护，留存维护记录？			
166	e）在评估活动结束、完成归档后，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。	1、是否能在归档完成后规定时间内进行评估设备和工具的日志、记录清除操作？			
167	f）具有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进行区分，并采取有效措施防止继续使用。	1、是否建立了设备和工具管理制度，明确设备档案、标识管理、故障管理和工具管理等系列要求？			
168		2、是否对评估设备和工具统一登记、统一标识，并能区分故障设备和工具?			
169		3、设备和工具摆放是否合理，对精密度要求高的设备和工具是否配套单独的防护措施？			

序号	标准条款				评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
170				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。	1、是否留有设备维护使用手册等指引文件，是否对设备定期检查维护？			
171					2、是否能将维护规程记录妥善保管，记录完整、规范？			
172				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。	1、评估机构是否根据被评估方的需求，以书面承诺等方式向其说明资源配置、保障情况（包括但不限于人员、工具、时间等）？			

2 服务足迹测评 GB/T 45577-2025《数据安全技术--数据安全风险评估方法》第 6-10 章

序号	标准条款			评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
1.	6 数据安全风险评估准备	6.1 确定评估目标	数据安全风险评估的目标包括但不限于： a）明确数据处理者所涉及的数据种类、规模、分布等基本情况。	1、是否明确了数据处理者所涉及的数据种类、规模、分布等基本情况？	描述对应评价项的要求，抽取组织近一年已完成的、至少两个以上的案例进行评价，描述评价证据，案例记录是否明确了数据处理者所涉及的数据种类、规模、分布等基本情况。	描述自评价结论，例如：符合（不符合或不适用，在备注中说明情况）	
2.			b）明确数据处理者数据处理活动的基本情况。	1、是否明确了数据处理者数据处理活动的基本情况，包括数据处理的目的、数据类型和范围、数据处理活动类型等？			
3.			c）发现可能影响国家安全、公共利益或者个人、组织合法权益的数据安全问题和风险。	1、是否具备发现可能影响国家安全、公共利益或者个人、组织合法权益的数据安全问题和风险的能力？			
4.			d）发现共享、交易、委托处理、向境外提供重要数据等处理活动的数据安全问	1、是否具备发现共享、交易、委托处理、向境外提供重要数据等处理活动的数据安全问			

序号	标准条款			评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
			题和风险。	题和风险的能力？			
5.			e)促进完善数据安全保护措施，提升数据安全保护能力。	1、是否能够促进完善数据安全保护措施，提升数据安全保护能力？			
6.		6.2 确定评估范围	a）全面摸排被评估方的数据安全整体情况，摸清其数据、数据处理活动、数据分类分级等情况；	1、是否能够全面识别被评估方的数据资产，是否掌握被评估方的数据保护目录。			
7.				2、是否能够明确被评估方涉及的数据处理活动？			
8.				3、是否能够明确被评估方数据分类分级管理程序？			
9.			b）结合数据分类分级选择重点评估对象，将涉及个人信息、重要数据、核心数据的所有数据处理活动，以及抽样选择的其他典型一般数据的处理活动作为重点评估对象开	1、是否能够依据被评估方的数据分类分级管理程序或业务、信息系统的重要性和敏感性，确定重点评估对象？			

序号	标准条款			评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
			展评估。如果组织未开展数据分类分级工作，也可结合业务、信息系统的重要性和敏感性，选择核心业务或重要信息系统的数据和数据处理活动作为重点评估对象开展评估。				
10.		**6.3 组建评估团队**	数据处理者开展数据安全风险评估时，可组织业务、安全、法务、合规、运维、研发等相关部门参与实施，评估组长由数据安全负责人或授权代表担任。	1、是否能够得到被评估方的充分配合，例如由被评估方的业务、安全、法务、合规、运维、研发等相关部门参与？			

序号	标准条款			评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
11.			数据处理者可委托第三方专业技术机构实施，第三方专业技术机构在评估中获取的信息只能用于评估目的，未经授权不应泄露、出售或者非法向他人提供。主管监管部门开展检查评估时，可根据评估范围、涉及的行业特征、专业需求，选择具备相关专业能力的评估人员组成评估队伍。评估队伍应提前完成风险评估文档、检测工具等各项准备工作，并签署保密协议。评估队伍在检查评估中获取的信息，只能用于检查任务目的和实施数据安全保护。被评估方应建立专	1、是否通过签署保密协议等方式确保数据安全风险评估机构未经授权不泄露、出售或者非法向他人提供评估中获取的信息？			

序号	标准条款			评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
			项工作团队，成员一般包括数据安全负责人和安全、法务、合规、运维、研发、业务、数据、风险等部门，或数据处理者内部负责相关事项的其他部门相关人员。专项工作团队应按照要求做好人员、设备、技术保障等工作，配合开展风险评估。				
12.		**6.4 开展前期准备**	开展数据安全风险评估前期准备时，应	1、是否制定了评估工作计划？评估工作计			

序号	标准条款			评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
			根据评估目标、评估范围和调研情况，制订工作计划、确定评估依据、确定评估内容、建立评估文档。 a）制定工作计划。评估工作计划内容一般包括工作目的、工作要求、工作内容、工作流程、调研安排、评估总体进度安排等。开展检查评估时，主管监管部门指导评估团队按照工作要求制定评估工作计划。	划是否涵盖工作目的、工作要求、工作内容、工作流程、调研安排、评估总体进度安排等内容？			
13.			b)确定评估依据。针对评估目标和范围确定评估依据，常见评估依据包括但不限于： 1）《中华人民共和国网络安全法》《中华人民共和国数据	1、是否结合评估目标和范围确定评估依据？ 常见的评估依据包括但不限于： 1）《中华人民共和国网络安全法》《中华人民共和国数据安全法》			

序号	标准条款			评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
			安全法》《中华人民共和国个人信息保护法》等法律，有关行政法规、司法解释； 2）网信部门及主(监)管部门相关数据安全规章、规范性文件； 3）地方数据安全政策规定和监管要求； 4）数据安全相关国家标准、行业标准等； 5）开展自评估时，本单位数据安全制度规范可作为评估依据之一。	《中华人民共和国个人信息保护法》等法律，有关行政法规、司法解释； 2）网信部门及主(监)管部门相关数据安全规章、规范性文件； 3）地方数据安全政策规定和监管要求； 4）数据安全相关国家标准、行业标准等； 5）被评估方数据安全制度规范。			
14.			c）确定评估内容。结合评估目标、范围、依据，针对被评估方的实际情况，确定被评估方每个评估对象适用的评估	1、是否明确了评估内容包括数据处理活动安全、数据安全管理、数据安全技术等方面进行风险评估？			
15.				2、是否明确了评估内			

序号	标准条款			评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
			内容： 1）数据处理者应从数据处理活动安全、数据安全管理、数据安全技术等方面进行风险评估； 2）涉及处理个人信息的，应在1）的基础上，对个人信息保护开展风险评估； 3）开展评估工作过程中，可根据任务要求、评估重点、监管需要、评估依据等，进一步完善评估内容。	容包括个人信息保护相关内容？			
16.				3、是否根据任务要求、评估重点、监管需要、评估依据等进一步完善评估内容？			
17.			d）建立评估文档。针对评估目标、范围、依据和内容，准备风险评估调研表、技术测试工具等。在评估工作开展过程中，应对评估工作相关文件进行统一编	1、是否建立评估文档，包括风险评估调研表、技术测试工具清单等？			
18.				2、是否对评估文档进行统一编号，并按规范进行管理？			

序号	标准条款			评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
			号，并规范管理。				
19.			评估团队编制数据安全风险评估工作方案并获得评估管理方的支持、认可，方案内容包括但不限于如下各方面。 a）评估概述：包括评估目标、评估依据等内容。	1、是否制定了评估工作方案？			
20.				2、是否在评估工作方案中明确评估目标、评估依据等内容？			
21.		**6.5 制定评估方案**	b）评估范围：包括评估对象选择方法、评估对象描述、评估范围等。	1、是否在评估工作方案中明确评估对象选择方法、评估对象描述、评估范围等内容？			
22.			c）评估内容和方法：包括评估内容、评估准则、评估方法等内容。	1、是否在评估工作方案中明确评估内容、评估准则、评估方法等内容？			
23.			d）评估人员：包括评估团队的组织结构、负责人、成员、职责分工等内容。	1、是否在评估工作方案中明确评估团队的组织结构、负责人、成员、职责分工等内容？			
24.			e）实施计划：包括时间进度安排、人员	1、是否在评估工作方案中明确时间进度安			

序号	标准条款			评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
			安排等内容。	排、人员安排等内容？			
25.			f）工作要求：包括评估工作要求、被评估方保障条件等内容，工作要求如严格依照评估内容及标准规范，规范评估行为，按照尽量不影响被评估方正常工作的原则，制定评估工作应急保障和风险规避措施，明确告知被评估方评估可能产生的风险，严守工作纪律和保密要求等。	1、是否在评估工作方案中明确被评估方人力、技术、预算等资源保障条件？			
26.				2、是否制定应急保障措施和风险规避措施？			
27.				3、是否明确告知被评估方评估可能产生的风险？			
28.				4、是否明确评估工作的工作纪律和保密要求等？			
29.			g）测试方案：开展技术测试前应明确测试方案，包括采用的技术工具、测试内容、测试环境、应急措施等，测试方应向被测方明示测试可能涉及的安全风险，	1、是否在开展测试前制定技术测试方案？			
30.				2、技术测试方案是否明确采用的技术工具、测试内容、测试环境、应急措施等？			
31.				3、技术测试方是否向被测方明示测试可能			

序号	标准条款			评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
			双方就测试方案达成共识。检查评估时应提前向有关部门报备。	涉及的安全风险？			
32.				4、技术测试方和被测方是否对测试方案进行认可？			
33.				5、检查评估前是否向有关部门报备？			
34.			评估团队可邀请行业领域相关数据安全、网络安全专家对评估方案进行评议，重点审核方案内容、风险管控、保护措施、可操作性、技术可行性等，进一步修改完善评估方案后，组织实施风险评估工作。	1、是否对评估工作方案进行评审？			
35.				2、是否针对评审意见进一步修改完善评估工作方案？			
36.	**7 信息调研**	**7.1 数据处理者调研**	数据处理者的基本情况的调研内容包括但不限于如下方面。 a）单位名称、法人和其他组织统一社会信用代码、办公地	1、是否调研数据处理者的单位名称、法人和其他组织统一社会信用代码、办公地址、法定代表人信息、人员规模、经营范围、数据安全负责人及其职务、联			

序号	标准条款			评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
			址、法定代表人信息、人员规模、经营范围、数据安全负责人及其职务、联系方式等基本信息。	系方式等基本信息？			
37.			b）单位性质，例如党政机关、事业单位、企业、社会团体等。	1、是否调研数据处理者的单位性质？			
38.			c）是否属于特定类型数据处理者，例如政务数据处理者、大型网络平台运营者、关键信息基础设施运营者等。	1、是否调研数据处理者属于特定类型数据处理者？			
39.			d）所属行业领域。	1、是否调研数据处理者的所属行业领域？			
40.			e）业务运营地区，开展数据处理活动所在国家和地区等。	1、是否调研数据处理者的业务运营地区？			
41.			f）主要业务范围、业务规模等。	1、是否调研数据处理者的主要业务范围、业务规模等？			
42.			g）数据处理相关服	1、是否调研数据处理			

序号	标准条款			评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
			务取得行政许可的情况。	者的数据处理相关服务行政许可获取情况？			
43.			h）被评估单位的资本组成和实际控制人情况。	1、是否调研被评估方的资本组成和实际控制人情况？			
44.			i）是否境外上市或计划赴境外上市及境外资本参与情况，或以可变利益实体（VIE）架构等方式实质性境外上市。	1、是否调研被评估方境外上市或计划赴境外上市及境外资本参与情况，或以可变利益实体（VIE）架构等方式实质性境外上市？			
45.		**7.2 业务和信息系统调研**	业务和信息系统情况包括但不限于如下方面。 网络和信息系统基本情况，包括网络规模、拓扑结构、信息系统等情况和对外连接、运营维护等情况以及是否为关键信息基础设施等情况。 b）业务基本信息，	1、是否调研网络规模、拓扑结构、信息系统等情况和对外连接、运营维护等情况以及是否为关键信息基础设施等情况？			
46.				1、是否调研业务功能、业务类型、服务对象、业务流程、用户规模、覆盖地域、相关部门等基本信息？			

序号	标准条款			评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
			包括业务描述、业务类型、服务对象、业务流程、用户规模、覆盖地域、相关部门等基本信息。				
47.			c）业务涉及个人信息、重要数据或核心数据处理情况。	1、是否调研业务涉及的个人信息、重要数据或核心数据的处理情况？			
48.			d）业务为政务部门或境外用户提供服务情况。	1、是否调研业务为政务部门或境外用户提供服务的情况？			
49.			e）信息系统、App 和小程序情况，包括系统功能、网络安全等级保护备案和测评结论、入口地址、系统连接关系、数据接口、App 及小程序名称和版本等。 f）数据中心和使用云平台情况。	1、是否调研包含的信息系统、App 和小程序的功能、网络安全等级保护备案和测评结论、入口地址、系统连接关系、数据接口、App 及小程序名称和版本等内容？			
50.				1、是否调研信息系统涉及的数据中心、云平台情况？			
51.			g）接入的外部第三	1、是否调研信息系统			

序号	标准条款			评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
			方产品、服务或 SDK 的情况，包括名称、版本、提供方、使用目的、合同协议等。	接入的外部第三方产品、服务或 SDK 的情况？包括名称、版本、提供方、使用目的、合同协议等？			
52.		7.3 数据资产调研	梳理结构化数据（如数据库表等）和非结构化数据（如图表文件等），输出数据资产清单。涉及范围包括但不限于生产环境、测试环境、备份存储环境、云存储环境、个人工作终端、数据采集设备终端等收集和产生的数据。调研内容包括但不限于如下方面。 a）数据资产情况，包括数据资产类型、数据范围、数据规模、数据形态、数据存储分布、元数据等数据。	1、是否制定数据资产清单，包含结构化数据和非结构化数据？			
53.				2、数据资产清单是否包含生产环境、测试环境、备份存储环境、云存储环境、个人工作终端、数据采集设备终端等收集和产生的数据？			
54.				3、是否调研数据资产类型、数据范围、数据规模、数据形态、数据存储分布、元数据等数据资产情况？			

序号	标准条款			评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
55.			b）分类分级情况，包括数据分类分级规则、数据类别、数据级别、重要数据和核心数据目录情况等。	1、是否调研数据分类分级规则、数据类别、数据级别、重要数据和核心数据目录情况等分类分级情况？			
56.			c）个人信息情况，包括个人信息类别、规模、敏感程度、数据来源、业务流转及与信息系统的对应关系等。	1、是否调研个人信息的类别、规模、敏感程度、数据来源、业务流转及与信息系统的对应关系等个人信息情况？			
57.			d）重要数据情况，包括重要数据种类别、规模、行业领域、数据来源、业务流转及与信息系统的对应关系等。	1、是否调研重要数据的种类别、规模、行业领域、数据来源、业务流转及与信息系统的对应关系等重要数据情况？			
58.			e）核心数据情况，包括核心数据类别、规模、行业领域、数据来源、业务流转及与信息系统的对应关系等。	1、是否调研核心数据的类别、规模、行业领域、数据来源、业务流转及与信息系统的对应关系等核心数据情况？			

序号	标准条款			评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
59.			f）其他一般数据情况。	1、是否调研其他一般数据情况？			
60.		**7.4 数据处理活动调研**	针对评估对象和范围，列出数据处理活动清单，描述数据流转关系，绘制数据流图。数据流图应描述数据流转各环节经过的相关方、信息系统，以及每个流动环节涉及的数据类型等。调研内容包括但不限于如下方面。 a）数据收集情况，如数据收集渠道、收集方式、数据范围、收集目的、收集频率、外部数据源、合同协议、相关系统，以及在被评估方公共场所安装图像采集、个人身份识别设备的情况等。	1、是否制定了数据处理活动清单、数据流图，明确数据流转关系？			
61.				2、数据流图是否明确数据流转各环节经过的相关方、信息系统，以及每个流动环节涉及的数据类型等？			
62.				3、是否调研数据收集渠道、收集方式、数据范围、收集目的、收集频率、外部数据源、合同协议、相关系统等数据收集情况？			
63.				4、是否调研被评估方公共场所安装图像采集、个人身份 设备的情况？			
64.			b）数据存储情况，	1、是否调研数据存储			

序号	标准条款			评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
			如数据存储方式、数据中心、存储系统(如数据库、大数据平台、云存储、网盘、存储介质等)、外部存储机构、存储地点、存储期限、备份冗余策略等。	方式、涉及的数据中心、存储系统(如数据库、大数据平台、云存储、网盘、存储介质等)、外部存储机构、存储地点、存储期限、备份冗余策略等数据存储情况？			
65.			c）数据传输情况，如数据传输途径和方式（如互联网、VPN、物理专线等在线通道情况，采用介质等离线传输情况）、传输协议、内部数据共享、数据接口等。	1、是否调研数据传输途径和方式、传输协议、内部数据共享、数据接口等数据传输情况？			
66.			d）数据使用和加工情况，如数据使用目的、方式、范围、场景、算法规则、相关系统和部门，数据清洗、转换、标注等加工情况，应用算法推荐技术提供互联网	1、是否调研数据使用目的、方式、范围、场景、算法规则、相关系统和部门？			
67.				2、是否调研数据清洗、转换、标注等加工情况？			
68.				3、是否调研应用算法			

序号	标准条款			评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
			信息服务的情况，核心数据、重要数据或个人信息委托处理、共同处理的情况等。	推荐技术提供互联网信息服务的情况？			
69.				4、是否调研核心数据、重要数据或个人信息委托处理、共同处理的情况？			
70.			e）数据提供情况，如数据提供（数据共享、数据交易，因合并、分立、解散、被宣告破产等原因需要转移数据等）的目的、方式、范围、数据接收方、合同协议，对外提供的个人信息和重要数据的种类、数量、范围、感程度、保存期限等。	1、是否调研数据对外提供原因、目的、方式、范围、数据接收方、合同协议等？			
71.				2、是否调研对外提供的个人信息和重要数据的种类、数量、范围、感程度、保存期限等？			
72.			f）数据公开情况，如数据公开的目的、方式、对象范围、数据种类、数据规模等。	1、是否调研数据公开的目的、方式、对象范围、数据种类、数据规模等？			

序号	标准条款			评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
73.			g）数据删除情况，如数据删除情形、删除方式、数据归档、介质销毁等。	1、是否调研数据删除情形、删除方式、数据归档、介质销毁等？			
74.			h）数据出境情况，是否存在个人信息或重要数据出境，如跨境业务、跨境办公、境外上市、使用境外云服务或数据中心、国际交流合作等场景的数据出境情况。	1、是否调研个人信息或重要数据出境情况，包括跨境业务、跨境办公、境外上市、使用境外云服务或数据中心、国际交流合作等场景？			
75.		7.5 安全防护措施调研	调研已有安全措施情况，包括但不限于如下方面。 a）已开展的等级保护测评、商用密码应用安全性评估、安全检测、风险评估、安全认证、合规审计情况，及发现问题的整改情况。	1、是否调研信息系统的等级保护测评、商用密码应用安全性评估、安全检测、风险评估、安全认证、合规审计相关报告，明确已有的安全措施及发现问题的整改情况。			
76.			b）数据安全管理组	1、是否调研数据安全			

序号	标准条款			评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
			织、人员及制度情况。	管理组织、人员及制度情况？			
77.			c）防火墙、入侵检测、入侵防御等网络安全设备及策略情况。	1、是否调研防火墙、入侵检测、入侵防御等网络安全设备及策略情况？			
78.			d）身份鉴别与访问控制情况。	1、是否调研各设备和系统的身份鉴别与访问控制情况？			
79.			e）网络安全漏洞管理及修复情况。	1、是否调研网络安全漏洞管理及修复情况？			
80.			f）VPN 等远程管理软件的用户及管理情况。	1、是否调研 VPN 等远程管理软件的用户及管理情况？			
81.			g）设备、系统及用户的账号口令管理情况。	1、是否调研设备、系统及用户的账号口令管理情况？			
82.			h）加密、脱敏、去标识化等安全技术应用情况。	1、是否调研数据加密、脱敏、去标识化等安全技术应用情况？			
83.			i）3 年内发生的网络和数据安全事件、攻击威胁情况：	1、是否调研 3 年内发生的网络和数据安全事件、攻击威胁情况？			

序号	标准条款			评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
			1）3 年内发生的网络和数据安全事件、攻击威胁情况，包括事件名称、数据类型和数量、发生原因、级别、处置措施、整改措施等，重大事件需提供事件调查评估报告； 2）实际环境中通过检测工具、监测系统、日志审计等发现的威胁； 3）近期公开发布的社会或特定行业威胁事件、威胁预警； 4）其他可能面临的数据泄露、窃取、篡改、破坏/损毁、丢失、滥用、非法获取、非法利用、非法提供等安全威胁。	是否明确事件名称、数据类型和数量、发生原因、级别、处置措施、整改措施等？			
84.				2、是否调研 3 年内发生的重大网络和数据安全事件的事件调查评估报告？			
85.				3、是否调研实际环境中通过检测工具、监测系统、日志审计等发现的威胁？			
86.				4、是否调研近期公开发布的社会或特定行业威胁事件、威胁预警？			
87.				5、是否调研其他可能面临的数据泄露、窃取、篡改、破坏/损毁、丢失、滥用、非法获取、非法利用、非法提供等安全威胁？			
88.	8 风险识别	8.1 通则	从数据安全管理、数据处理活动、数据安	1、在测评工作相关的制度中具备测评结论			

序号	标准条款			评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
			全技术、个人信息保护等方面进行数据安全风险识别，发现可能存在的数据安全风险源。具体实施时可按照以下步骤开展。 a）如果被评估方已开展过相关的测评工作，应先对已开展的测评工作结论进行分析。	分析的要求。			
89.				2、是否对已开展的相关测评工作结论进行分析。			
90.			b）针对被评估对象的特点，选择适用的评估内容进行评估，评估内容选择方法如下: 1）数据处理者均应识别数据安全管理(见8.3)、数据处理活动(见8.4)、数据安全技术(见8.5)等风险情况; 2）个人信息处理者	1、是否分析评估对象的特点，是否根据评估对象的特点选择适用的评估内容。评估内容选择方法如下： 1）数据处理者均应识别数据安全管理(见8.3)、数据处理活动(见8.4)、数据安全技术(见8.5)等风险情况; 2）个人信息处理者还			

序号	标准条款			评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
			还应在 1)的基础上，识别个人信息保护风险情况(见 8.6)，参考 GB/T45574—2025 及本文件提出的数据安全风险评估方法，识别敏感个人信息安全风险； 3) 被评估对象涉及数据出境的，应按照国家相关法规、国家标准要求进行数据出境安全保护工作，若存在未按要求开展相关工作的，直接判定存在安全风险，并结合第 9 章进行风险分析与评价； 4) 梳理各评估项的风险识别结果，形成数据安全风险识别工作记录。	应在 1)的基础上，识别个人信息保护风险情况(见 8.6)，参考 GB/T45574—2025 及本文件提出的数据安全风险评估方法，识别敏感个人信息安全风险； 3) 被评估对象涉及数据出境的，应按照国家相关法规、国家标准要求进行数据出境安全保护工作，若存在未按要求开展相关工作的，直接判定存在安全风险，并结合第 9 章进行风险分析与评价； 4) 梳理各评估项的风险识别结果，形成数据安全风险识别工作记录。			
91.		8.2 已开展测	被评估方应按照法	1、是否在开展风险评			

序号	标准条款			评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
		评情况分析	律、行政法规、部门规章、强制性国家标准等文件要求，通过有关检测评估。在开展风险评估时，应记录被评估方已开展的检测评估工作情况，主要包括： a）数据处理活动涉及应开展检测评估工作名称、要求来源等基本情况。	估时，是否记录被评估方已开展的检测评估工作情况。			
92.				2、是否记录已开展的检测评估工作名称、要求来源等情况。			
93.			b）已开展检测评估工作有效性(指是否由有资质机构，按照正常程序开展)。	3、是否记录已开展的检测评估工作的机构、机构名称、机构资质以及是否按照检测评估流程开展评估工作。			
94.			c）检测评估内容和结果，及检测评估工作开展情况。	4、是否记录已开展的检测评估内容、结果，以及检测评估工作的开展情况。			
95.		8.3 数据安全管理	应从以下方面识别数据安全管理风险。评估项应符合附录	1、数据安全管理的风险评估，评估项是否符合附录 A.1 的规定。			

序号	标准条款			评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
96.			A 的 A.1 的规定。 a）数据安全管理制度:主要包括数据安全制度体系、数据安全制度落实等,评估项应符合 A.1.1 的规定。	2、数据安全管理的风险评估是否包含数据安全管理制度,主要包括数据安全制度体系、数据安全制度落实等,评估项应符合 A.1.1 的规定。			
97.			b）安全组织机构:主要包括数据安全组织架构、数据安全岗位设置等,评估项应符合 A.1.2 的规定。	3、数据安全管理的风险评估是否包含数据安全组织机构,主要包括数据安全组织架构、数据安全岗位设置等,评估项应符合 A.1.2 的规定。			
98.			c）分类分级管理:主要包括数据资产管理、数据分类分级制度、数据分类分级保护等,评估项应符合 A.1.3 的规定。	4、数据安全管理的风险评估是否包含分类分级管理:主要包括数据资产管理、数据分类分级制度、数据分类分级保护等,评估项应符合 A.1.3 的规定。			
99.			d）人员安全管理:主要包括人员录用、保密协议、转岗离	5、数据安全管理的风险评估是否包含人员安全管理:主要包括人			

序号	标准条款			评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
			岗、数据安全培训等，评估项应符合A.1.4的规定。	员录用、保密协议、转岗离岗、数据安全培训等，评估项应符合A.1.4的规定。			
100.			e）合作外包管理:主要包括合作方管理机制、合作协议约束、外包人员访问权限、第三方接入与数据回收、政务数据委托处理等，评估项应符合A.1.5的规定。	6、数据安全管理的风险评估是否包含合作外包管理:主要包括合作方管理机制、合作协议约束、外包人员访问权限、第三方接入与数据回收、政务数据委托处理等，评估项应符合A.1.5的规定。			
101.			f）安全威胁和应急管理:主要包括安全威胁和事件、安全应急管理等，评估项应符合A.1.6的规定。	7、数据安全管理的风险评估是否包含安全威胁和应急管理:主要包括安全威胁和事件、安全应急管理等，评估项应符合A.1.6的规定。			
102.			g）开发运维管理:主要包括新应用开发审核，对开发代码、测试数据的安全	8、数据安全管理的风险评估是否包含开发运维管理:主要包括新应用开发审核，对开发			

序号	标准条款			评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
			管理等。评估项应符合 A.1.7 的规定。	代码、测试数据的安全管理等。评估项应符合 A.1.7 的规定。			
103.			h） 云数据安全:主要包括被评估对象使用云计算服务、被评估对象是云计算服务提供者两类，评估项应符合 A.1.8 的规定。	9、数据安全管理的风险评估是否包含云数据安全:主要包括被评估对象使用云计算服务、被评估对象是云计算服务提供者两类，评估项应符合 A.1.8 的规定。			
104.		8.4 数据处理活动安全	应从以下方面识别数据处理活动安全风险。评估项应符合 A.2 的规定。 a） 数据收集安全:主要包括数据收集合法正当性、通过第三方收集数据安全、数据质量控制、数据收集方式、数据收集设备及环境安全等。评估项应符合 A.2.1 的规定。	1、数据处理活动的风险识别是否包含数据收集安全风险，主要包括数据收集合法正当性、通过第三方收集数据安全、数据质量控制、数据收集方式、数据收集设备及环境安全等。评估项应符合 A.2.1 的规定。			

序号	标准条款			评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
105.			b）数据存储安全：主要包括数据存储适当性、逻辑存储安全、存储介质安全等评估项应符合 A.2.2 的规定。	2、数据处理活动的风险识别是否包含数据存储安全风险，主要包括数据存储适当性、逻辑存储安全、存储介质安全等评估项应符合 A.2.2 的规定。			
106.			c）数据传输安全：主要包括传输链路安全性、传输链路可靠性等。评估项应符合 A.2.3 的规定。	3、数据处理活动的风险识别是否包含数据传输安全风险，主要包括传输链路安全性、传输链路可靠性等。评估项应符合 A.2.3 的规定。			
107.			d）数据使用和加工安全：主要包括数据使用和加工合法性、数据正当使用、数据导入导出、数据处理环境、数据使用和加工安全措施等。评估项应符合 A.2.4 的规定。	4、数据处理活动的风险识别是否包含数据使用和加工安全风险，主要包括数据使用和加工合法性、数据正当使用、数据导入导出、数据处理环境、数据使用和加工安全措施等。评估项应符合 A.2.4 的规定。			

序号	标准条款			评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
108.			e）数据提供安全：主要包括数据提供合法正当必要性、数据提供管理、数据提供技术措施、数据接收方、数据转移安全、数据出境安全等。评估项应符合A.2.5的规定。	5、数据处理活动的风险识别是否包含数据提供安全风险，主要包括数据提供合法正当必要性、数据提供管理、数据提供技术措施、数据接收方、数据转移安全、数据出境安全等。评估项应符合A.2.5的规定。			
109.			f）数据公开安全：主要包括数据公开适当性、数据公开管理等。评估项应符合A.2.6的规定。	6、数据处理活动的风险识别是否包含数据公开安全风险，主要包括数据公开适当性、数据公开管理等。评估项应符合A.2.6的规定。			
110.			g）数据删除安全：主要包括数据删除管理、存储介质销毁等。评估项应符合A.2.7的规定。	7、数据处理活动的风险识别是否包含数据删除安全风险，主要包括数据删除管理、存储介质销毁等。评估项应符合A.2.7的规定。			
111.			h）其他数据处理活动安全：主要针对即	8、数据处理活动的风险识别是否包含其他			

序号	标准条款			评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
			时通信、快递物流、网上购物、网络支付、网络音视频、汽车、网络预约汽车服务等数据处理活动进行风险识别。评估项应符合 A.2.8 的规定。	数据处理活动安全风险，主要针对即时通信、快递物流、网上购物、网络支付、网络音视频、汽车、网络预约汽车服务等数据处理活动进行风险识别。评估项应符合 A.2.8 的规定。			
112.		8.5 数据安全技术	应从以下方面识别数据安全技术风险。评估项应符合 A.3 的规定。 a）网络安全防护:主要包括网络资源管理、网络隔离、边界防护等。评估项应符合 A.3.1 的规定。	1、数据安全技术风险识别是否包含网络安全防护，主要包括网络资源管理、网络隔离、边界防护等。评估项应符合 A.3.1 的规定。			
113.			b）身份鉴别与访问控制:主要包括身份鉴别、访问控制、授权管理等。评估项应符合 A.3.2 的规定。	2、数据安全技术风险识别是否包含身份鉴别与访问控制，主要包括身份鉴别、访问控制、授权管理等。评估项应符合 A.3.2 的规			

序号	标准条款			评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
				定。			
114.			c）监测预警:主要包括安全监测预警和信息报告机制的建设落实、异常行为监测指标建设等。评估项应符合 A.3.3 的规定。	3、数据安全技术风险识别是否包含监测预警，主要包括安全监测预警和信息报告机制的建设落实、异常行为监测指标建设等。评估项应符合 A.3.3 的规定。			
115.			d）数据脱敏:主要包括数据脱敏规则、脱敏方法和脱敏数据的使用限制等。评估项应符合 A.3.4 的规定。	4、数据安全技术风险识别是否包含数据脱敏，主要包括数据脱敏规则、脱敏方法和脱敏数据的使用限制等。评估项应符合 A.3.4 的规定。			
116.			e）数据防泄露:主要包括数据防泄露技术手段部署、数据防泄露技术措施有效性等。评估项应符合 A.3.5 的规定。	5、数据安全技术风险识别是否包含数据防泄露，主要包括数据防泄露技术手段部署、数据防泄露技术措施有效性等。评估项应符合 A.3.5 的规定。			
117.			f）数据接口安全:	6、数据安全技术风险			

序号	标准条款			评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
			主要包括对外接口安全、接口安全控制等。评估项应符合A.3.6的规定。	识别是否包含数据接口安全，主要包括对外接口安全、接口安全控制等。评估项应符合A.3.6的规定。			
118.			g）数据备份恢复:主要包括数据备份恢复策略和操作规程的建设落实情况、数据灾备、数据备份恢复等。评估项应符合A.3.7的规定。	7、数据安全技术风险识别是否包含数据备份恢复，主要包括数据备份恢复策略和操作规程的建设落实情况、数据灾备、数据备份恢复等。评估项应符合A.3.7的规定。			
119.			h）安全审计:主要包括审计执行、日志留存记、行为审计等。评估项应符合A.3.8的规定。	8、数据安全技术风险识别是否包含安全审计，主要包括审计执行、日志留存记、行为审计等。评估项应符合A.3.8的规定。			
120.		8.6 个人信息保护	如被评估范围涉及个人信息处理，应从以下方面识别个人信息保护风险，评估项应符合A.4的规	1、个人信息保护风险识别是否包含个人信息处理基本原则，主要包括合法、诚信原则，正当、必要原则等。评			

序号	标准条款			评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
			定。 a）个人信息处理基本原则:主要包括合法、诚信原则,正当、必要原则等。评估项应符合 A.4.1 的规定。	估项应符合 A.4.1 的规定。			
121.			b）个人信息告知:主要包括处理个人信息告知规则等。评估项应符合 A.4.2 的规定。	2、个人信息保护风险识别是否包含个人信息告知,主要包括处理个人信息告知规则等。评估项应符合 A.4.2 的规定。			
122.			c）个人信息同意:主要包括个人信息前取得个人同意、撤回同意等。评估项应符合 A.4.3 的规定。	3、个人信息保护风险识别是否包含个人信息同意,主要包括个人信息前取得个人同意、撤回同意等。评估项应符合 A.4.3 的规定。			
123.			d）个人信息处理:主要包括个人信息保存、个人信息共同处理、个人信息委托处理、个人信息转	4、个人信息保护风险识别是否包含个人信息处理,主要包括个人信息保存、个人信息共同处理、个人信息委托			

序号	标准条款			评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
			移、向他人提供个人信息、自动化决策、个人信息公开等。评估项应符合 A.4.4 的规定。	处理、个人信息转移、向他人提供个人信息、自动化决策、个人信息公开等。评估项应符合 A.4.4 的规定。			
124.			e）敏感个人信息处理:主要包括敏感个人信息处理通用规则、生物特征识别信息安全等。评估项应符合 A.4.5 的规定。	5、个人信息保护风险识别是否包含敏感个人信息处理，主要包括敏感个人信息处理通用规则、生物特征识别信息安全等。评估项应符合 A.4.5 的规定。			
125.			f）个人信息主体权利:主要包括个人信息的查阅、复制、可携带、更正、补充、删除及其他个人信息主体权利保障等。评估项应符合 A.4.6 的规定。	6、个人信息保护风险识别是否包含个人信息主体权利，主要包括个人信息的查阅、复制、可携带、更正、补充、删除及其他个人信息主体权利保障等。评估项应符合 A.4.6 的规定。			
126.			g）个人信息安全义务:主要包括个人信息保护措施、个人信	7、个人信息保护风险识别是否包含个人信息安全义务，主要包括			

序号	标准条款			评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
			息保护负责人、个人信息保护影响评估、个人信息安全应急等。评估项应符合A.4.7的规定。	个人信息保护措施、个人信息保护负责人、个人信息保护影响评估、个人信息安全应急等。评估项应符合A.4.7的规定。			
127.			h）个人信息投诉举报:主要包括投诉举报渠道建设情况，接受投诉、举报的联系方式公布情况等。13GB/T45577—2025评估项应符合A.4.8的规定。	8、个人信息保护风险识别是否包含个人信息投诉举报，主要包括投诉举报渠道建设情况，接受投诉、举报的联系方式公布情况等。13GB/T45577—2025评估项应符合A.4.8的规定。			
128.			i）大型网络平台个人信息保护:主要包括个人信息保护合规制度体系建设、处理个人信息的规范和保护个人信息的义务等。评估项应符合A.4.9的规定。	9、个人信息保护风险识别是否包含大型网络平台个人信息保护，主要包括个人信息保护合规制度体系建设、处理个人信息的规范和保护个人信息的义务等。评估项应符合A.4.9的规定。			

序号	标准条款			评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
129.	9 风险分析与评价	9.1 通则	在信息调研、风险识别基础上，按照 9.2 和 9.3 进行风险分析和评价，形成数据安全风险清单。其中，所有数据安全风险评估过程均应按照 9.2.1 进行风险归类分析，梳理形成数据安全风险源清单。可结合实际需要，视情开展风险危害程度分析、风险发生可能性分析、风险评价。不进行风险评价时，风险归类分析形成的数据安全风险源清单可作为数据安全风险清单。	1、是否进行数据风险分析和评价，是否形成数据安全风险清单。			
130.				2、是否结合实际需要，视情开展风险危害程度分析、风险发生可能性分析、风险评价。			
131.				3、是否在不进行风险评价时具有风险归类分析形成的数据安全风险源清单，是否将该清单作为数据安全风险清单。			
132.			数据安全风险分析，主要从影响数据保密性、完整性、可用性和数据处理合理性角度分析各项风	1、数据安全风险分析是否从影响数据保密性、完整性、可用性和数据处理合理性角度分析各项风险源可能			

序号	标准条款			评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
			险源可能引发的数据安全风险，及风险危害程度和发生的可能性。可基于实际情况，视情对数据安全风险进行评价。风险评价一般结合评估对象实际情况，基于 9.2.2 和 9.2.3 的分析结果，综合风险危害程度及风险发生可能性对安全风险进行综合评价。	引发的数据安全风险，及风险危害程度和发生的可能性。			
133.				2、是否基于实际情况对数据安全风险进行评价，综合风险危害程度及风险发生可能性对安全风险进行综合评价。			
134.		9.2 数据安全风险分析	9.2.1 风险归类分析 结合信息调研情况和数据安全风险识别工作记录，梳理发现的数据安全风险源，使用一个或多个风险源分析其可能引发的数据安全风险，形成数据安全风险源清单。可参考附	1、是否结合信息调研情况和数据安全风险识别工作记录，梳理发现的数据安全风险源，是否使用一个或多个风险源分析其可能引发的数据安全风险，形成数据安全风险源清单。			
135.				2、数据安全风险清单内容是否全面，具体要			

序号	标准条款			评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
			录 B 所列典型数据安全风险类型进行风险分析。数据安全风险源清单见表 1，表中各字段填写要求如下。 a）序号:填写风险编号，如 1 或 R1 等。 b）风险类型:填写数据安全风险归类分析的结果，如数据泄露风险。 c）风险描述:填写实际数据风险情况，如某项、某几项或某类数据存在数据泄露风险。 d）风险源描述:填写风险源名称，如访问某数据时，某部门某业务或信息系统身份鉴别信息不健全，在某种情形下可能被攻击者或内部	求如下： a）序号:填写风险编号，如 1 或 R1 等。 b）风险类型:填写数据安全风险归类分析的结果，如数据泄露风险。 c）风险描述:填写实际数据风险情况，如某项、某几项或某类数据存在数据泄露风险。 d）风险源描述:填写风险源名称，如访问某数据时，某部门某业务或信息系统身份鉴别信息不健全，在某种情形下可能被攻击者或内部员工访问、下载，可能导致一定量级某类数据泄露。 e）涉及的数据及类型、级别:填写某类风险中一个风险源涉及的数据情况，如涉及			

序号	标准条款			评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
			员工访问、下载，可能导致一定量级某类数据泄露。 e）涉及的数据及类型、级别:填写某类风险中一个风险源涉及的数据情况，如涉及 1000 万银行卡号，属于个人信息，重要数据。 f）涉及的数据处理活动:填写某类风险中一个风险源涉及的数据处理情况，如数据收集、存储、使用和加工，涉及 1000 万个人信息向境外提供的情况。	1000 万银行卡号，属于个人信息，重要数据。 f）涉及的数据处理活动:填写某类风险中一个风险源涉及的数据处理情况，如数据收集、存储、使用和加工，涉及 1000 万个人信息向境外提供的情况。			
136.			9.2.2 风险危害程度分析 风险危害程度分析，主要考虑数据价值、风险源严重程度等因素。将结合数据级	1、风险危害程度分析是否考虑数据价值、风险源严重程度等因素。			
137.				2、是否结合数据级别、规模、种类、处理目的、方式、范围等情况，综			

序号	标准条款			评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
			别、规模、种类、处理目的、方式、范围等情况，综合分析数据安全风险一旦发生，对国家安全、公共利益、组织或者个人合法权益造成的危害程度。	合分析数据安全风险一旦发生，对国家安全、公共利益、组织或者个人合法权益造成的危害程度。			
138.			共利益、组织或者个人合法权益造成的危害程度。风险危害程度分析遵循就高从严、整体分析原则，如果该风险涉及多项数据，应进行累加判断，将涉及数据的风险按照最高危害等级判断。分析方法如下。 a）数据价值主要从数据分级、经济效益、业务效益、投入成本计量等方面分析。数据级别、经济效益、业务效益等越高代表数据价值越高。其中，数据安全	3、风险危害程度分析是否遵循就高从严、整体分析原则，是否对涉及多项数据的风险，进行累加判断，将涉及数据的风险按照最高危害等级判断。			

序号	标准条款			评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
			级别按照GB/T43697—2024确定。个人信息规模和数据敏感程度可作为数据价值判断的衡量因素。 b）风险源严重程度，主要考虑风险源对数据处理者带来的危害程度。数据安全风险危害程度的判断标准见表2，风险危害程度从低到高可分为低、中、较高、高、很高5个级别。附录C的C.1给出各类数据安全风险危害程度等级参考。如需进行定量分析，见附录D的D.1。				
139.			9.2.3 风险发生可能性分析 风险发生可能性分	1、风险发生可能性分析是否考虑风险源发生频率、安全措施有效			

序号	标准条款			评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
			析，主要考虑风险源发生频率、安全措施有效性和完备性、风险源关联性等因素。分析方法如下。 a）风险源发生频率，可从被评估对象发生相关数据安全事件的次数及频率、同行业或业务模式相似的单位发生相关数据安全事件的次数及频率、相似数据安全事件发生次数及频率、轻微安全问题累计发生次数等方面，综合分析同类风险源发生可能性。一般风险源或安全事件发生频率越高，风险发生可能性越高。 b）安全措施有效性、完备性，主要通	性和完备性、风险源关联性等因素。分析方法如下。		
140.				2、风险发生可能性分析是否考虑风险源发生频率，是否从被评估对象发生相关数据安全事件的次数及频率、同行业或业务模式相似的单位发生相关数据安全事件的次数及频率、相似数据安全事件发生次数及频率、轻微安全问题累计发生次数等方面，综合分析同类风险源发生可能性。			
141.				3、风险发生可能性分析是否考虑安全措施有效性、完备性，是否通过识别数据安全措施应对风险源的有效性、全面性等。核心数据、重要数据及相关数			

序号	标准条款			评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
			过识别数据安全措施应对风险源的有效性、全面性等。核心数据、重要数据及相关数据处理活动，需采取更严格的安全防护措施才能降低风险发生可能性。c）风险源关联性，主要通过风险源清单关联分析，发现多个风险源组合后可能引发的数据安全风险，综合判断风险发生可能性。在综合分析风险源发生频率、安全措施有效性和完备性、风险源关联性的基础上，将数据安全风险 发生的可能性从低到高分为低、中、高 3 个级别，如表 3 所示。等级越高代表措	据处理活动，需采取更严格的安全防护措施才能降低风险发生可能性。		
142.				4、风险发生可能性分析是否考虑风险源关联性，是否通过风险源清单关联分析，发现多个风险源组合后可能引发的数据安全风险，综合判断风险发生可能性。			
143.				5、在综合分析风险源发生频率、安全措施有效性和完备性、风险源关联性的基础上，是否将数据安全风险发生的可能性从低到高分为低、中、高 3 个级别。			

序号	标准条款			评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
			施完备性、有效性越低，风险越可能发生。C.2 给出各类数据安全风险发生可能性等级参考。如需进行定量分析，可参考 D.2。				
144.		9.3 数据安全风险评价	使用风险危害程度和可能性进行数据安全风险评价，评价结果包括如下方面。 a）重大安全风险：一般指可能直接影响国家安全的数据安全风险。 b）高安全风险：一般指可能直接影响经济运行、社会稳定、公共健康安全，以及较为广泛的公众权益，或对国家安全造成间接影响的数据安全风险。 c）中安全风险：一	1、是否使用风险危害程度和可能性进行数据安全风险评价，评价结果是否包括如下方面。 a）重大安全风险：一般指可能直接影响国家安全的数据安全风险。 b）高安全风险：一般指可能直接影响经济运行、社会稳定、公共健康安全，以及较为广泛的公众权益，或对国家安全造成间接影响的数据安全风险。 c）中安全风险：一般			

序号	标准条款			评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
			般指可能直接对企业合法权益造成较为严重的影响，或直接对自然人的人格尊严受到严重侵害或者人身、财产安全受到严重危害，或对经济运行、社会稳定、公众利益造成较为严重间接影响的数据安全风险。 d）低安全风险：一般指可能直接对企业合法权益造成一般影响，或直接对自然人的人格尊严受到侵害或者人身、财产安全受到危害，或对社会、公众权益有一定或较小影响的数据安全风险。 e）轻微安全风险：一般指可能直接对企业合法权益造成	指可能直接对企业合法权益造成较为严重的影响，或直接对自然人的人格尊严受到严重侵害或者人身、财产安全受到严重危害，或对经济运行、社会稳定、公众利益造成较为严重间接影响的数据安全风险。 d）低安全风险：一般指可能直接对企业合法权益造成一般影响，或直接对自然人的人格尊严受到侵害或者人身、财产安全受到危害，或对社会、公众权益有一定或较小影响的数据安全风险。 e）轻微安全风险：一般指可能直接对企业合法权益造成一般或较小影响，或对自然人人格尊严、人身安全、			

序号	标准条款			评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
			一般或较小影响，或对自然人人格尊严、人身安全、财产安全不造成侵害或仅产生较轻微的危害，或对小范围的组织或公民个体权益造成影响的数据安全风险。数据处理者可根据自身情况，将仅影响组织权益、个人权益等的风险自行定为或调整为“重大”“高”等级别，及时进行风险处置。本文件提出了定性和定量评价风险的方法，表 4 提供了一种风险等级定性评价方法，如需获得风险定量评价结果，可参考 D.3 进行风险评价。	财产安全不造成侵害或仅产生较轻微的危害，或对小范围的组织或公民个体权益造成影响的数据安全风险。			
145.		9.4 形成数据安全风险清单	针对各项数据安全风险完成风险评价	1、针对各项数据安全风险完成风险评价后，			

序号	标准条款			评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
			后，整理各项风险评估结果，风险源清单基础上形成数据安全风险清单，列出各项风险的风险等级、危害程度、发生可能性等。数据安全风险清单见表 5。表 5 各字段填写要求如下。 a）序号，风险类型，风险描述，风险源描述，涉及的数据及类型、级别，涉及的数据处理活动，按照表 1 填写即可。 b）风险危害程度：按照 9.2.3 获得的风险危害程度分析结果，填写风险危害程度等级，如高。 c）风险发生的可能性：按照 9.2.3 获得的风险发生可能性分析结果，填写风险	是否整理各项风险评估结果。			
146.				2、是否在风险评价后，在风险源清单基础上形成数据安全风险清单，列出各项风险的风险等级、危害程度、发生可能性等。			
147.				3、数据安全风险清单内容是否全面，是否包含以下内容： a）序号，风险类型，风险描述，风险源描述，涉及的数据及类型、级别，涉及的数据处理活动，按照表 1 填写即可。 b）风险危害程度：按照 9.2.3 获得的风险危害程度分析结果，填写风险危害程度等级，如高。 c）风险发生的可能性：按照 9.2.3 获得的			

序号	标准条款			评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
			发生可能性等级，如高。 d）风险等级:按照9.3获得的风险等级评价结果,填写风险等级,如高安全风险。	风险发生可能性分析结果,填写风险发生可能性等级，如高。 d）风险等级:按照9.3获得的风险等级评价结果，填写风险等级，如高安全风险。			
148.	10 评估总结	10.1 编制评估报告	根据评估情况,评估团队编制数据安全风险评估报告(报告模板见附录E）。评估报告应准确、清晰地描述评估活动的主要内容(并附必要的证据或记录)，提出可操作性的整改措施对策建议。风险评估报告的内容包括： a）数据处理者基本信息、数据安全管理机构信息、数据安全负责人姓名和联系	1、是否在评估报告中明确数据处理者基本信息、数据安全管理机构信息、数据安全负责人姓名和联系方式等内容？			

序号	标准条款			评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
			方式等；				
149.			b）评估概述，包括评估目的及依据，评估对象和范围，评估结论等；	1、是否在评估报告的评估概述中明确评估目的及依据，评估对象和范围，评估结论等内容？			
150.			c）评估工作情况，包括评估人员、评估时间安排、评估工具和环境情况等；	1、是否在评估报告的工作情况中明确评估人员、评估时间安排、评估工具和环境情况等内容？			
151.			d）信息调研情况，包括数据处理者、业务和信息系统、数据、数据处理活动、安全措施等情况，形成的数据资产清单、数据处理活动清单，数据流图等文件可视情放在报告正文或附件中；	1、是否在评估报告的信息调研情况中明确数据处理者、业务和信息系统、数据、数据处理活动、安全措施等？			
152.				2、评估报告正文或附件中是否包括数据资产清单、数据处理活动清单、数据流图等？			
153.			e）数据安全风险识别，包括数据安全管理、数据处理活动、	1、是否在评估报告的数据安全风险识别中明确数据安全管理、数			

序号	标准条款			评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
			数据安全技术、个人信息保护等方面识别的风险源情况；	据处理活动、数据安全技术、个人信息保护等方面识别的风险源情况？			
154.			f）风险分析与评价，对数据安全问题可能带来的安全风险进行综合分析，视情对风险进行评价；	1、是否在评估报告的风险分析与评价中对数据安全问题可能带来的安全风险进行综合分析，对风险进行合理评价？			
155.			g）整改建议，针对发现的数据安全问题或风险，提出整改措施或风险处置建议；	1、是否在评估报告的整改建议中针对发现的数据安全问题或风险，提出整改措施或风险处置建议？			
156.			h）数据安全风险源清单，列出完整的数据安全风险源清单，并附上关键记录和证据，若证据无法在附录中完整列出，应列出证据关键信息和序号，在提交评估报告时作为附件提	1、是否在评估报告中列出完整的数据安全风险源清单，并附上关键记录和证据？			
157.				2、若证据无法在附录中完整列出，是否在附录中完整列出证据序号和关键信息，并将证据作为附件一并提			

序号	标准条款			评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
			交；	交？			
158.			i）涉及重要数据、个人信息、核心数据的，应详细列出处理的数据种类、数量（不包括数据内容本身），开展数据处理活动的情况，面临的数据安全风险及其应对措施等；	1、是否在评估报告中详细列出处理的重要数据、个人信息、核心数据的数据种类、数量（不包括数据内容本身），开展数据处理活动的情况，面临的数据安全风险及其应对措施等？			
159.				2、是否在评估报告中详细列出重要数据、个人信息、核心数据的处理活动情况，面临的数据安全风险及其应对措施？			
160.			j）委托第三方机构开展评估或检查评估的，评估报告应由评估组长、审核人签字，并加盖评估机构公章。	1、第三方机构出具的评估报告是否有评估组长、审核人签字，并加盖评估机构公章？			
161.			重要数据的处理者应当每年度向省级	1、重要数据处理者是否每年度向省级以上			

序号	标准条款			评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
			以上有关主管部门报送风险评估报告内容，除上述内容外，还应当包括下列内容。 a）在信息调研情况中，增加处理重要数据的目的、种类、数量、方式、范围、存储期限、存储地点等，开展数据处理活动的情况，不包括数据内容本身。	有关主管部门报送风险评估报告？			
162.				2、重要数据处理者风险评估报告的信息调研情况中是否涵盖重要数据的目的、种类、数量、方式、范围、存储期限、存储地点等，开展数据处理活动的情况？			
163.			b）在信息调研情况中，增加数据安全管理制度及实施情况，加密、备份、标签标识、访问控制、安全认证等技术措施和其他必要措施及其有效性。	1、重要数据处理者风险评估报告的信息调研情况中是否涵盖数据安全管理制度及实施情况？			
164.				2、重要数据处理者的风险评估报告的信息调研情况中是否涵盖数据加密、备份、标签标识、访问控制、安全认证等技术措施和其			

序号	标准条款			评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
				他必要措施及其有效性？			
165.			c）在信息调研情况中，增加发现的网络数据安全风险发生的网络数据安全事件及处置情况。	1、重要数据处理者风险评估报告的信息调研情况中是否涵盖发现的网络数据安全风险发生的网络数据安全事件及处置情况？			
166.			d）在信息调研情况中，提供、委托处理、共同处理重要数据情况。	1、重要数据处理者风险评估报告的信息调研情况中是否涵盖提供、委托处理、共同处理重要数据情况？			
167.			e）在数据安全风险识别中，单独列出提供、委托处理、共同处理重要数据的风险评估情况、网络数据出境情况。	1、重要数据处理者风险评估报告的数据安全风险识别中是否单独列出提供、委托处理、共同处理重要数据的风险评估情况、网络数据出境情况？			
168.			f）处理重要数据的大型网络平台服务提供者报送的风险评估报告，除包括前	1、处理重要数据的大型网络平台服务提供者的风险评估报告中是否补充说明了关键			

序号	标准条款			评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
			款规定的内容外，还应当充分说明关键业务和供应链网络数据安全等情况。	业务和供应链网络数据安全等情况？			
169.			g）有关主管部门规定的其他报告内容。	1、重要数据处理者风险评估报告中是否包含有关主管部门规定的其他报告内容？			
170.		**10.2 风险处置建议**	评估人员结合实际情况，对发现的数据安全风险提出处置建议，酌情指导数据处理者整改。被评估方应制定数据安全风险处置方案，限期完成整改，无法及时完成整改的，应采取临时安全措施，防止数据安全事件发生。	1、评估方是否对被评估方制定数据安全风险处置方案的正确性和合理性进行确认？			
171.				2、无法在限期内完成整改的，评估人员是否确认被评估方已在数据安全风险处置方案中明确采取的临时安全措施，并有效实施？			
172.			重要数据的处理者存在可能危害国家安全的重要数据处理活动的，应当按照省级以上有关主管	1、评估人员是否确认重要数据处理者已立即采取有效措施处置风险，包括但不限于：a）停止收集某些类型			

序号	标准条款			评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
			部门责令整改或者停止处理重要数据等要求，立即采取有效措施处置风险。 常见数据安全风险处置措施包括但不限于以下选项。 a）停止收集某些类型的数据。 b）预处理阶段对某些类型数据进行销毁。 c）缩小处理范围。 d）缩短存储期限。 e）加强对应数据处理活动岗位人员培训。 f）匿名化、去标识化。 g）完善管理制度。 h)补充签署协议(针对数据转移）。 i）修订隐私条款。	的数据。 b）预处理阶段对某些类型数据进行销毁。 c）缩小处理范围。 d）缩短存储期限。 e）加强对应数据处理活动岗位人员培训。 f）匿名化、去标识化。 g）完善管理制度。 h）补充签署协议（针对数据转移）。 i）修订隐私条款。			
173.		**10.3 残余风**	评估人员根据数据	1、评估方是否依据被			

序号	标准条款			评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
		险分析	处理者决定的风险处置措施，结合风险识别和评估方法，预判措施有效性和残余风险，形成记录。被评估方完成整改后，评估方可视情开展数据安全风险复评工作，复评时可重点分析风险处置后的残余风险，以及采取额外控制措施可能导致的次生风险等。	评估方数据安全风险处置方案中的风险处置措施预判措施有效性和残余风险，并形成残余风险分析记录？			
174.				2、评估方是否在被评估方完成整改后，开展数据安全风险复评工作？			
175.				3、评估方是否在复评时重点分析风险处置后的残余风险，以及采取额外控制措施可能导致的次生风险等，并形成相关记录？			

3 服务能力确认 GB/T 45577-2025《数据安全技术--数据安全风险评估方法》第 6-10 章

序号	标准条款	评价指标	自评价描述	自评价结果（符合/不符合/不适用）	备注
1.	《数据安全风险评估服务认证规则》CCRC-DSC-DSRA-001:2026 B/0 5.4.4.1 服务能力确认或验证	1）评估过程按照 GB/T 45577-2025《数据安全技术 数据安全风险评估方法》实施	描述对应评价项的要求，描述《数据安全风险评估服务认证规则》CCRC-DSC-DSRA-001:2026 B/0 5.4.4.1 的对应性评价证据。	描述自评价结论，例如：符合（不符合或不适用，在备注中说明情况）	
2.		2)评估报告内容按照 GB/T 45577-2025《数据安全技术 数据安全风险评估方法》编制			
3.		3)服务提供和交付过程中，评估人员具备开展数据安全风险评估所需资质，客观公正、态度友好			
4.		4)按时出具评估报告			