ICS 点击此处添加 ICS 号
点击此处添加中国标准文献分类号

DB11

北　京　市　地　方　标　准

DB11/T ××××—××××

数据交易安全评估指南

Guidelines for assessing the security of data transaction

点击此处添加与国际标准一致性程度的标识

（征求意见稿）

××××－××－××发布　　××××－××－××实施

北京市市场监督管理局　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》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。

本文件由北京市经济和信息化局、北京市政务服务和数据管理局提出。

本文件由北京市经济和信息化局、北京市政务服务和数据管理局归口管理。

本文件起草单位：

本文件主要起草人：

数据交易安全评估指南

1 范围

本文件给出了数据交易双方、数据交易场所在数据交易过程中进行安全评估的内容。

本文件适用于数据交易双方、数据交易场所进行数据交易安全自评估，数据交易场所对数据交易供方、需方进行评估，或委托第三方专业机构进行评估，亦可为相关监管部门、行业主管部门用于评估数据交易参与方的安全情况提供参考。

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 22239 信息安全技术 网络安全等级保护基本要求

GB/T 39204 信息安全技术 关键信息基础设施安全保护要求

DB11/T ××××数据交易通用要求

3 术语和定义

DB11/T ××××界定的术语和定义适用于本文件。

3.1

数据交易安全 security of data transaction

在数据交易过程中，数据交易供方、需方和数据交易场所通过采取必要措施，确保数据交易处于有效保护、合法、安全的状态。

4 评估方法

从基础项和加分项两个维度，围绕数据交易流程为数据交易双方、数据交易场所提供数据交易安全评估参考内容，引导规范数据交易行为，为企业数据交易安全流通提供指引。其中，满足基础项是进行加分项评估的前提，满足全部基础项对数据交易双方及数据交易场所是十分必要的，加分项作为评估可选内容，为提升安全能力提供参考。数据交易安全评估范围如图1所示。

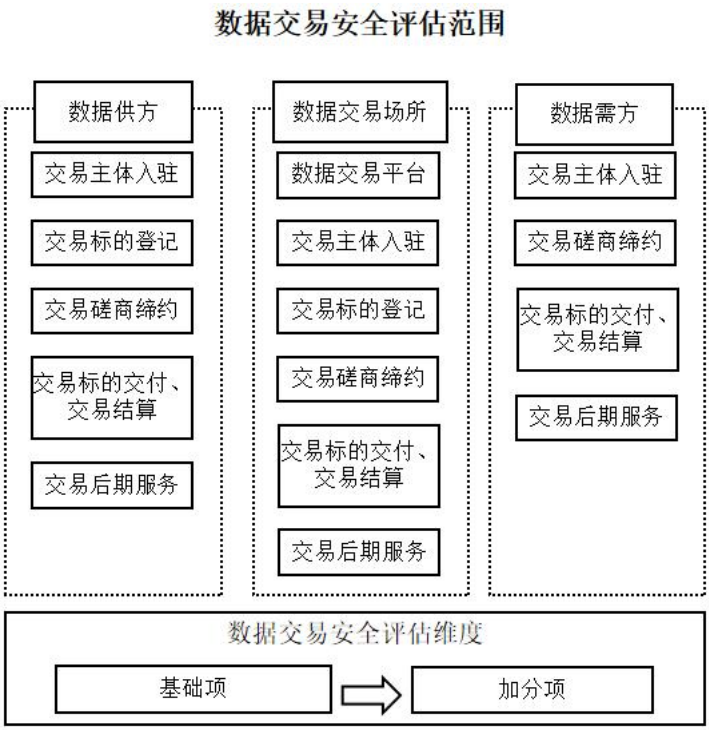

图1 数据交易安全评估范围

5 评估内容及指标体系

5.1 数据供方安全评估

5.1.1 数据供方安全评估指标体系

在数据交易过程中，对数据供方进行安全评估建立可参考的指标体系，具体内容如表1所示。

表1 数据供方安全评估指标体系表

指标维度		评分方法及建议权重范围	评分说明
交易主体入驻	基础项	是/否	基础项评估：对各指标维度进行是否判断，如其中某项指标维度基础项不满足要求，则加分项评估无效，对应指标维度安全要求不达标。加分项评估：指标维度满足基础项要求的情况下，开展指标维度加分项评估。指标维度加分项权重可结合具体行业情况及数据交易应用场景，参考本标准建议权重范围进行评估打分，权重加总为100%，加总后得出评分结果。
	加分项	评分，建议权重范围15%—25%	
交易标的登记	基础项	是/否	
	加分项	评分，建议权重范围20%—30%	
交易磋商缔约	基础项	• 是/否	
	加分项	评分，建议权重范围5%—15%	
交易标的交付、交易结算	基础项	是/否	
	加分项	评分，建议权重范围25%—35%	
交易后期服务	基础项	是/否	
	加分项	评分，建议权重范围10%—20%	

注1：表1中建议权重范围为参考范围，可根据不同行业及应用场景，对指标维度加分项权重范围进行适量调整。

5.1.2 交易主体入驻

5.1.2.1 基础项

基础项包括：

a) 依法成立并有效存续的法人、非法人组织机构，或具备相应民事行为能力的自然人；
b) 近一年内不存在数据类违法违规记录；
c) 在一年内未发生过数据泄露等安全事件，在组织存续期间或自然人具备完全民事行为能力，不存在重大数据违法违规行为；
d) 在五年内未因违反网络安全法律法规受到治安管理处罚和刑事处罚；
e) 场内交易前，按照数据交易场所要求，在数据交易平台完成注册、认证并通过审核。

5.1.2.2 加分项

加分项包括：

a) 具备数据统一鉴别、敏感数据（包括敏感个人信息、重要数据）识别、数据分类分级标识、数据脱敏、数据加密、数据备份和恢复、数据防泄漏、数据共享和公开等技术能力；
b) 具备数据访问权限、数据安全监测与预警、数据分类分级、数据脱敏、数据共享和公开、数据安全监督检查、数据安全责任等安全管理制度；
c) 具备关于主体能力的资质证明类文件，如通过DCMM、DSMM相关认证等；
d) 交易标的为重要数据的，处理数据的信息系统宜符合GB/T 22239中三级及以上网络安全等级保护要求；
e) 交易标的为核心数据的，处理数据的信息系统为关键信息基础设施的，宜符合GB/T 39204中对关键信息基础设施安全保护要求；不涉及关键信息基础设施的，宜符合GB/T 22239中四级网络安全等级保护要求；
f) 交易标的为重要数据、核心数据的，具备对接收方的数据共享、调用情况的监测措施，相关日志留存时间不少于三年，具备满足符合《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》三级网络安全等级保护的安全能力。
g) 交易标的为一般数据的，具备满足符合《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》三级网络安全等级保护的安全能力。

5.1.3 交易标的登记

5.1.3.1 基础项

基础项包括：

a) 涉及重要数据、核心数据的数据交易标的，依法履行登记、审批等相应规定；
b) 交易标的为重要数据、核心数据的，出具上一年度数据安全风险评估报告；
c) 具有明确的概要描述、产品形态、应用场景、使用范围、服务方式和使用期限；
d) 具有数据来源权属合法合规的报告或相关真实有效的证明材料；
e) 个人信息进场交易前需取得有效采集授权，或进行匿名化处理；对于无法满足前述条件的，进行去标识化处理，使其在不借助额外信息的情况下无法识别特定自然人，并进行安全性评估；
f) 真实、准确、完整披露数据交易标的信息，不隐瞒数据来源及涉及的敏感数据（包括敏感个人信息、重要数据）；
g) 场内交易前，根据数据交易场所相关交易规则要求，提供数据交易标的登记上架相关材料以供审核。

5.1.3.2 加分项

加分项包括：

a) 提供数据质量、数据合规、数据安全等第三方专业机构出具的报告；
b) 根据数据交易需方要求，提供数据交易标的样本数据。

5.1.4 交易磋商缔约

5.1.4.1 基础项

基础项包括：

a) 不以欺诈、诱骗、误导、胁迫、贿赂等方式交易数据；
b) 明确数据交易标的质量、数量、价格、使用期限等；
c) 如存在数据交易标的使用场景限制，在合同或订单中明确数据交易标的使用或流通的目的、方式和范围，法律法规另有规定的除外；
d) 如提供测试数据，支持数据需方进行数据交易前验证，提供安全可控测试环境，保证测试数据真实、有效；
e) 如涉及数据加工服务的，在合同或订单中明确加工后的数据交易标的相关权属。

5.1.4.2 加分项

根据数据需方需求，给出数据需方关注的产品解答并进行一定的产品优化适配。

5.1.5 交易标的交付、交易结算

5.1.5.1 基础项

基础项包括：

a) 根据合同或订单约定，按时、保质提供数据交易标的，供数据需方进行数据使用；
b) 采取必要措施，确保所交付的数据交易标的安全、合法、有效，并持续履行所交付数据交易标的相关法定义务；
c) 配合监管部门和数据交易场所开展数据交易标的交付和交易结算过程中的履约监管和交易结算核验；
d) 根据合同、订单约定或数据交易场所要求，完成交易结算相关工作。

5.1.5.2 加分项

加分项包括：

a) 在实施过程保障数据需方的使用顺畅，能够提供多种运行环境，满足数据需方的差异化使用需求；
b) 针对数据需方在使用过程中出现的问题提供咨询服务，给予解答及帮助；
c) 保证数据交易标的供给的稳定性和连续性，中途遇到不稳定、中断等情形，及时进行解决。

5.1.6 交易后期服务

5.1.6.1 基础项

基础项包括：

a) 根据合同或订单约定，结束数据交易标的供给；
b) 配合监管部门和数据交易场所开展交易后的追溯和审计工作。

5.1.6.2 加分项

具备完善的交易售后服务体系和台账式管理。

5.2 数据需方安全评估

5.2.1 数据需方安全评估指标体系

在数据交易过程中，对数据需方进行安全评估建立可参考的指标体系，具体内容如表2所示。

表2 数据需方安全评估指标体系

指标维度		评分方法及建议权重范围	评分说明
交易主体入驻	基础项	是/否	基础项评估：对各指标维度进行是否判断，如其中某项指标维度基础项不满足要求，则加分项评估无效，对应指标维度安全要求不达标。 加分项评估：指标维度满足基础项要求的情况下，开展指标维度加分项评估。指标维度加分项权重可结合具体行业情况及数据交易应用场景，参考本标准建议权重范围进行评估打分，权重加总为100%，加总后得出评分结果。
	加分项	评分，建议权重范围15%—25%	
交易标的登记	基础项	是/否	
	加分项	评分，建议权重范围15%—25%	
交易磋商缔约	基础项	是/否	
	加分项	评分，建议权重范围15%—25%	
交易标的交付、交易结算	基础项	是/否	
	加分项	评分，建议权重范围15%—25%	
交易后期服务	基础项	是/否	
	加分项	评分，建议权重范围15%—25%	

注2：表2中建议权重范围为参考范围，可根据不同行业及应用场景，对指标维度加分项权重范围进行适量调整。

5.2.2 交易主体入驻

5.2.2.1 基础项

基础项包括：

a) 依法成立并有效存续的法人、非法人组织机构，或具备相应民事行为能力的自然人；
b) 近一年内不存在数据类违法违规记录；
c) 在一年内未发生过数据泄露等安全事件，在组织存续期间或自然人具备完全民事行为能力，不存在重大数据违法违规行为；
d) 在五年内未因违反网络安全法律法规受到治安管理处罚和刑事处罚；
e) 场内交易前，按照数据交易场所要求，在数据交易平台完成注册、认证并通过审核；
f) 交易标的为重要数据的，处理数据的信息系统符合三级及以上《GB/T 22239-2019信息安全技术 网络安全等级保护基本要求》中网络安全等级保护要求；
g) 交易标的为核心数据的，处理数据的信息系统为关键信息基础设施的，满足《GB/T 39204-2022信息安全技术 关键信息基础设施安全保护要求》中对关键信息基础设施安全保护要求；不涉及关键信息基础设施的，满足《GB/T 22239-2019信息安全技术 网络安全等级保护基本要求》中四级网络安全等级保护要求；
h) 交易标的为重要数据、核心数据的，具备对接收方的数据共享、调用情况的监测措施，相关日志留存时间不少于三年。

5.2.2.2 加分项

加分项包括：

a) 具备数据源统一鉴别、敏感数据（包括敏感个人信息、重要数据）识别、数据分类分级标识、数据脱敏、数据加密、数据备份和恢复、数据防泄漏、数据共享和开放等技术能力；
b) 具备数据访问权限、数据安全监测与预警、数据分类分级、数据脱敏、数据共享和开放、数据安全监督检查、数据安全责任等安全管理制度；
c) 具备关于主体能力的资质证明类文件，如通过DCMM、DSMM相关认证等；
d) 交易标的为一般数据的数据需方，宜符合GB/T 22239中三级及以上网络安全等级保护要求。

5.2.3 交易磋商缔约

5.2.3.1 基础项

基础项包括：

a) 不以欺诈、诱骗、误导、胁迫、贿赂等方式交易数据；
b) 遵守数据使用范围限制要求，确保加工的过程和结果数据不超出数据供方要求的使用范围。

5.2.3.2 加分项

国家对数据交易使用应用场景有相关要求的，满足其要求。如，使用人类生物样本、个人信息数据开展涉及数据和算法的科技活动的，按照《科技伦理审查办法（试行）》的规定，通过伦理审查。

5.2.4 交易标的交付、交易结算

5.2.4.1 基础项

基础项包括：

a) 按照数据交易双方约定使用数据，授权使用范围不超出交易约定要求的流通范围；
b) 不绕过或破坏交易数据的安全保护措施，不对去标识化的个人信息进行重新识别；
c) 配合监管部门和数据交易场所开展标的交付和交易结算中的监察和核验；
d) 采取合理、必要的措施，对供方提供的数据交易标的的安全性、合规性进行审核；
e) 根据合同或订单约定或数据交易场所要求，完成交易结算相关工作。

5.2.4.2 加分项

加分项包括：

a) 对数据交付平台业务安全性、稳定性、连续性进行评估和反馈；
b) 对数据交易标的的符合性、有效性进行验证反馈。

5.2.5 交易后期服务

5.2.5.1 基础项

基础项包括：

a) 配合监管部门和数据交易场所开展交易后的追溯和审计工作；接收重要数据、核心数据的，留存交付时间、内容、方式、规模等日志记录时间不少于3年；
b) 按合同或订单约定，保证数据交易标的数据安全、防止数据泄露；
c) 在交易结束后，按合同或订单约定清除相关数据的缓存，并对清除记录及数据清除措施的有效性进行检查。

5.3 数据交易场所安全评估

5.3.1 数据需方安全评估指标体系

在数据交易过程中，对数据交易场所进行安全评估建立可参考的指标体系，具体内容如表3所示。

表3 数据交易场所安全评估指标维度、评估方法及建议权重范围

	指标维度		评分方法及建议权重范围	评分说明
数据交易场所	-	基础项	是/否	基础项评估：对各指标维度进行是否判断，如其中某项指标维度基础项不满足要求，则加分项评估无效，对应指标维度安全要求不达标。 加分项评估：指标维度满足基础项要求的情况下，开展指标维度加分项评估。指标维度加分项权重可结合具体行业情况及数据交易应用场景，参考本标准建议权重范围进行评估打分，权重加总为100%，加总后得出评分结果。
		加分项	评分，建议权重范围15%—25%	
数据交易平台	-	基础项	是/否	
		加分项	评分，建议权重范围15%—25%	
交易环节	交易主体确认	基础项	是/否	
		加分项	评分，建议权重范围5%—15%	
	交易标的确认	基础项	是/否	
		加分项	评分，建议权重范围5%—15%	
	交易磋商缔约	基础项	是/否	
		加分项	评分，建议权重范围5%—15%	
	交易标的交付、交易结算	基础项	是/否	
		加分项	评分，建议权重范围15%—25%	
	交易后期服务	基础项	是/否	
		加分项	评分，建议权重范围5%—15%	

注3：表3中建议权重范围为参考范围，可根据不同行业及应用场景，对指标维度加分项权重范围进行适量调整。

5.3.2 数据交易场所主体安全评估

5.3.2.1 基础项

基础项包括：

a) 依法注册的，经政府部门批准成立并有效存续，并具备我国行政主管部门的授权或许可进行组织和管理数据交易活动的组织机构；

b) 近一年内无数据类违法违规记录的合法组织机构；

c) 建立明确的数据交易规则，明确定义包括数据交易标的准入及审核、交易主体准入及审核、交易磋商缔约规范、数据交易标的交付监管规则、交易结算规则、交易后期服务及评价评级规则，对数据交易场所内的数据交易活动进行流程化的约束和管理，定期对数据交易规则进行完善，并按照相应制度规则，对交易主体、数据交易标的进行审核；

d) 制定交易活动的监督监管准则，防止和及时终止不符合交易规则约束的交易活动，并建立信息公示机制；

e) 建立内部数据安全管理制度、信息安全巡检制度、交易所信息报送和披露机制、应用程序研发管理制度、应用程序测试管理制度、数据处理环境操作规范、远程数据访问控制及日志审计制度、应用运维流程规范及巡检制度，定期对制度进行完善并就落实情况进行监督；

f) 如发现违反市场监督管理、网络安全、数据安全等有关规定的数据交易行为，依法采取必要的处置措施，保存有关记录，按照相关法律法规和监管要求向主管部门报告。

5.3.2.2 加分项

加分项包括：

a) 建立数据交易合规巡检机制，定期对交易主体、数据交易标的的安全性、合规性进行检查；
b) 建立数据交易参与方的信用管理机制，对入驻各方服务内容、质量、交易行为等进行评估；
c) 加强数据交易过程的透明度，确保所有交易活动都能够追踪和记录，以便在出现问题时能够快速定位和解决；
d) 完善数据交易异议处理机制，为交易双方提供公正、高效的争议解决途径；
e) 推动建立行业标准和技术规范，引导数据交易市场健康有序发展；
f) 加强对数据交易市场的监管科技应用，利用大数据、区块链等技术手段提升监管效能和精准度。

5.3.3 数据交易平台安全评估

5.3.3.1 基础项

基础项包括：

a) 在经政府批准依法设立的数据交易场所内建设，且部署在中华人民共和国境内；
b) 采用的密码技术符合国家密码管理相关要求；
c) 宜符合GB/T 22239中三级及以上网络安全等级保护要求；
d) 建立安全风险监测机制，及时发现安全缺陷、漏洞等风险，并采取补救措施；
e) 建立隐私保护机制，包括数据匿名化处理、用户同意管理、数据访问和披露控制；
f) 7支持监管部门访问交易日志、数据存证、电子服务合同、订单等审计资料，开展数据交易服务的安全审计工作；
g) 为数据供方、需方提供安全的上传或下载接口，包括基于密码技术的身份认证、访问控制；
h) 提供传输链路加密、传输数据保密性和完整性校验等保护措施；
i) 提供安全稳定的数据交付环境，并采取数据加密、访问控制、数据防泄漏、水印溯源、安全审计等措施，防止交易过程中的数据泄露、篡改、破坏或非法获取、非法交易、非法利用等；
j) 对每笔数据交易操作日志进行记录，生成数据交易日志，保证交易日志、数据存证、数据来源合法性等文件不可篡改和可追溯，保存相关记录至少6个月以供审查；重要数据、核心数据交易日志记录不少于3年；对每笔数据交易操作日志进行记录， 生成数据交易日志， 保证交易日志、 数据存证、 数据来源合法性等文件不可篡改和可追溯， 保存相关记录至少 6 个月以供审查；涉及重要数据、核心数据的，相关记录留存时间不少于3年；
k) 应用加密技术、身份认证、访问控制、网络隔离、数据脱敏、数据备份和灾难恢复技术等，保障交易活动过程产生的数据的安全性。

5.3.3.2 加分项

加分项包括：

a) 具备在数据交付过程中提供安全隔离环境，支撑数据交易标的物的数据计算加工、算法模型的运行，并具备隔离环境和过程数据的销毁机制，以保障数据交付的可靠性。其中所涉算法模型的提供者落实主体责任，对算法、模型文件具备内容审查、审核机制，以保障算法安全性、合规性；
b) 具备恶意代码防护能力，能够对交易数据含有的恶意代码进行检测；
c) 对数据交易的参与方、数据交易标的、交易环节设置人工干预功能，人工干预内容宜包括交易参与方审核、交易数据和需求审核、交易暂停、交易撤销、交易恢复；
d) 授予数据交易各参与方所需的最小必要权限，实现各参与方的权限分离；
e) 实施分离存储、加密存储等安全措施，保障交易活动过程产生的数据的机密性和完整性，并具备防灾备部署架构、多副本一致性检测等措施，保障数据的可用性；

f） 提供两个及以上不同运营商的互联网链路出口；
g） 进行数据的计算、交付和验证，并根据合约的执行履约情况对数据交易的过程进行管控；
h） 支持签订电子服务合同或订单，采取数字签名等技术措施保证合约不被篡改；
i） 采取相应技术手段，对安全审计的结果进行保护；
j） 建立应急响应机制，规范应急处置措施，规范应急操作流程，加强技术储备，定期进行预案演练。

5.3.4 交易过程安全评估

5.3.4.1 交易主体入驻

5.3.4.1.1 基础项

基础项包括：
a) 提供账户注册、修改、注销等功能；
b) 按照相关制度要求审核数据交易参与方相应资质；
c) 对已注册账户进行信息和权限管理。

5.3.4.1.2 加分项

加分项包括：
a) 通过资料审核、身份鉴别等方式验证第三方评估结论，对第三方提供报告的真实性和有效性进行审核；
b) 根据数据供需双方提供的材料，审核数据安全能力。

5.3.4.2 交易标的登记

5.3.4.2.1 基础项

基础项包括：
a) 审核申请上架的数据交易标的相关材料，包括但不限于数据来源、数据授权、数据质量、数据使用目的、数据使用范围及相关证明材料；
b) 对于包含敏感数据（包括敏感个人信息、重要数据）的数据交易标的，提供相应的安全保障措施；
c) 具备数据交易标的上架、下架、展示、信息修改等功能；
d) 根据我国相关法律法规制定禁止交易数据目录。

5.3.4.2.2 加分项

加分项包括：
a) 对上架数据交易标的进行识别，并生成唯一的标识；
b) 依据数据交易标的分类分级、应用场景等进行权限管理和访问控制。

5.3.4.3 交易磋商缔约

5.3.4.3.1 基础项

审查交易需方的需求，确保数据使用目的合法、正当和必要。

5.3.4.3.2 加分项

加分项包括：

a) 提供在线交易磋商环境；
b) 具备交易磋商的暂停、撤销、恢复能力；
c) 具备交易磋商争议的投诉和处理能力；
d) 辅助供需双方对数据交易标的类型、质量、用途、使用范围、交付方式、使用期限、交易价格和保密条款等内容进行协商和约定；
e) 对磋商结果进行登记，包括数据交易参与方、数据交易标的描述、合约有效期、交易价格、交付质量、交付方式、加工算法逻辑、使用范围、使用对象和使用期限等内容。

5.3.4.4 交易标的交付、交易结算

5.3.4.4.1 基础项

基础项包括：

a) 监督数据交易参与方按照合同或订单约定完成交付、结算；
b) 提供安全隔离环境，对数据交付过程中的加工、计算处理提供平台能力支撑；
c) 对数据交易标的交付过程进行记录，保证记录信息不可篡改；
d) 具备交易结算功能，按照合同或订单约定对交易参与方进行相应收益分配。

5.3.4.4.2 加分项

加分项包括：

a) 保证数据交易标的交付过程的稳定性、连续性；
b) 根据交付要求，提供机密计算、隐私计算等技术支持；
c) 在数据传输链路上部署交易数据监控工具，具有数据保护机制和数据泄漏检测能力；
d) 应用链路加密、端到端加密、Internet加密等技术对网络数据进行加密，防护针对网络数据机密性的攻击。

5.3.4.5 交易后期服务

5.3.4.5.1 基础项

基础项包括：

a) 数据交易各参与方确认交易结束后，关闭数据访问通道并清除相关缓存；
b) 对数据交易过程中交易记录等证据材料进行管理，提供监督管理和纠纷处理；
c) 定期对数据交易行为进行审计；
d) 未经授权不私自留存及使用数据供方或需方的数据，法律法规另行要求的除外。

5.3.4.5.2 加分项

加分项包括：

a) 对已完成的数据交易进行记录和归档；
b) 提供投诉举报渠道，监督数据交易各环节的数据泄露、滥用等情况；
c) 建立争议解决机制，对服务中的争议进行协调处理；
d) 对数据交易过程中的重要活动、操作，单独生成相应的审计记录。

6 评估流程

6.1 评估准备

开展数据交易安全评估前，宜明确评估目标及评估对象、确定评估范围、组建评估团队、制定工作计划并制定评估方案。

6.2 评估实施

a) 开展评估调研，了解数据交易参与主体、交易标的、交易环节相关安全信息；
b) 根据不同的数据交易安全评估对象，对应不同的安全评估维度和评估内容，开展数据交易安全评估；
c) 结合基础项和加分项评分结果，对数据交易的安全性进行等级划定，得出安全评估结论，等级划定、等级依据及评估建议参考表4：

表4 数据交易安全评估等级

评估等级	等级依据	评估建议
优	基础项评分为满分，加分项评分 85 分以上	基础项指标全部满足要求，加分项评估优秀，评估对象具有较高的数据交易安全能力。
中	基础项评分为满分，加分项评分 60 分以上	基础项指标全部满足要求，加分项评估及格，满足基本的数据交易安全能力，评估对象可根据加分项评估情况进行优化提升。
差	基础项评分不达标	基础项指标存在不满足要求的情况，不满足基本的数据交易安全能力，评估对象需根据评估情况进行安全能力整改及提升。

注4：表4等级依据作为参考，根据行业和应用场景不同，等级依据可进行适量调整。

7 报告编写及结果应用

7.1 报告编写

根据评估情况，可形成数据交易安全评估报告，内容包括但不限于评估概述、评估工作情况、评估对象分析、评估过程、评估结果、问题清单和整改建议等；报告内容宜准确、客观、清晰。

7.2 结果应用

7.2.1 数据交易安全评估报告可作为在数据交易场所开展数据交易的参考依据。

7.2.2 评估对象可根据评估报告制定整改计划，进行安全整改；评估方可视情况开展数据交易安全复评工作。

参 考 文 献

[1] GB/T 22239-2019信息安全技术 网络安全等级保护基本要求
[2] GB/T 31524-2015 电子商务平台运营与技术规范
[3] GB/T 36343-2018 信息技术 数据交易服务平台 交易数据描述
[4] GB/T 37728-2019 信息技术 数据交易服务平台 通用功能要求
[5] GB/T 37932—2019 信息安全技术 数据交易服务安全要求
[6] GB/T 39204-2022 信息安全技术 关键信息基础设施安全保护要求
[7] GB/T 40094.1-2021 电子商务数据交易 第1部分：准则
[8] DB 3708/T 19.1-2023 公共资源交易平台服务规范 第1部分：总则
[9] DB 11/T ××××数据交易服务指南
[10] 国家工业信息安全发展研究中心《2022年数据交易平台发展白皮书》
[11] 《科技伦理审查办法（试行）》
[12] 《北京国际数据交易服务指南》