ICS 35.030
CCS L80

团　　体　　标　　准

T/SZBA XXXX—XXXX

数据安全合规评估方法

Assessment method for data security compliance

（工作组讨论稿）

2022-11-15

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

深圳市信息服务业区块链协会　　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。

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。

本文件由深圳市信息服务业区块链协会归口。

本文件起草单位：XXX

本文件主要起草人：XXX

数据安全合规评估方法

1 范围

本文件规定了数据安全合规评估的评估框架、评估过程以及评估内容和要求。

本文件适用于数据处理、运营、交易等相关组织的数据安全合规评估，以及监管部门、第三方机构进行数据安全合规审查和评估。

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 25069 信息安全技术 术语

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GB/T 22240 信息安全技术 网络安全等护保护定级指南

GB/T 37964—2019 信息安全技术 个人信息去标识化指南

GB/T 35273—2020 信息安全技术 个人信息安全规范

GB/T 39335—2020 信息安全技术 个人信息安全影响评估指南

GB/T 41391—2022 信息安全技术 移动互联网应用程序（App）收集个人信息基本要求

GB/T 41479—2022 信息安全技术 网络数据处理安全要求

GB/T 39204—2022 信息安全技术 关键信息基础设施安全保护要求

3 术语和定义

GB/T 25069界定的以及下列术语和定义适用于本文件。

3.1

3.2 **数据 data**

任何以电子或者其他方式对信息的记录。

[GB/T 41479—2022，3.1]

3.3

3.4 **匿名化 anonymization**

个人信息经过处理无法识别特定自然人且不能复原的过程。

注：个人信息经匿名化处理后所得的信息不属于个人信息。

[GB/T 41479—2022，3.13]

3.5

3.6 **个人信息 personal information**

以电子或者其他方式记录的与已识别或者可以识别自然人有关的各种信息。

注1：个人信息包括姓名、出生日期、公民身份证号码、个人生物识别信息、住址、通信通讯联系方式、通信记录和内容、账号密码、财产信息、征信信息、行踪信息、行踪轨迹、住宿信息、健康生理信息、交易信息等。

注2：不包括匿名化处理后的信息。

[GB/T 41479—2022，3.6]

3.7

3.8 重要数据 important data

一旦泄露可能直接影响国家安全、公共安全、经济安全和社会稳定的数据。

注：重要数据包括未公开的政府信息，数量达到一定规模的基因、地理、矿产信息等，原则上不包括个人信息、企业内部经营管理信息等。

[GB/T 41479—2022，3.9]

3.9

3.10 去标识化 de-identification

通过对个人信息的技术处理，使其在不借助额外信息的情况下，无法识别个人信息所标识的自然人的过程。

注：去除标识符与个人信息主体（个人信息所标识的自然人）之间关联性。

[GB/T 37964—2019，3.13，有修改]

3.11

3.12 小程序 mini program

基于应用程序开放接口实现的，用户无需安装即可使用的移动互联网应用程序。

注：应用程序通过公开其应用程序编程接口（API）或函数，使外部的程序可以增加该应用的功能或使用让该应用程序的资源，而不需要更改该应用程序的源代码。

[GB/T 41391—2022，3.3]

3.13

3.14 数据出境 data cross-border transfer

中国境内的数据处理者通过网络及其他方式（如物理携带），将在中国境内运营中收集和产生的个人信息和重要数据，通过直接提供或开展业务、提供服务、产品等方式提供给境外的机构、组织或个人的一次活动或连续性活动。

注1：以下情形属于数据出境：

a） 向本国境内，但不属于本国司法管辖或未在境内注册的主体提供个人信息和重要数据；

b） 数据未转移存储至本国以外的地方，但被境外的机构、组织、个人访问查看的（公开信息除外）。

c） 网络运营者集团内部数据由境内转移至境外，涉及其在境内运营中收集和产生的个人信息和重要数据的。

注2：非在境内运营中收集和产生的个人信息和重要数据经由本国出境，未经任何变动或加工处理的，不属于数据出境。

注3：非在境内运营中收集和产生的个人信息和重要数据在境内存储、加工处理后出境，不涉及境内运营中收集和产生的个人信息和重要数据的，不属于数据出境。

注4：境内自然人因个人或者家庭事务向境外提供个人信息，不属于数据出境。

3.15

3.16 关键信息基础设施 critical information infrastructure

公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域的，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统等。

注：负责关键基础设施安全保护的工作部门根据认定规则负责组织认定本行业、本领域的关键信息基础设施，及时将认定结果通知运营者，并通报国务院公安部门。

4 缩略语

下列缩略语适用于本文件。

API：应用程序编程接口（Application Programming Interface）

SDK：软件开发工具包（Software Development Kit）

CIIO：关键信息基础设施运营者（Critical Information Infrastructure Operator）

5 评估框架

数据安全合规评估以用户数据安全合规评估目标为导向，以数据安全相关的法律法规和国家信息安全技术标准体系为评估依据，对评估对象和范围进行确定，经过准备、审核、分析、评价等评估流程，覆盖评估对象的业务运营模式、数据处理主体、数据处理活动、管理措施及落实、出境安全合规、合规跟踪评估等评估内容。数据安全合规评估框架见图1。

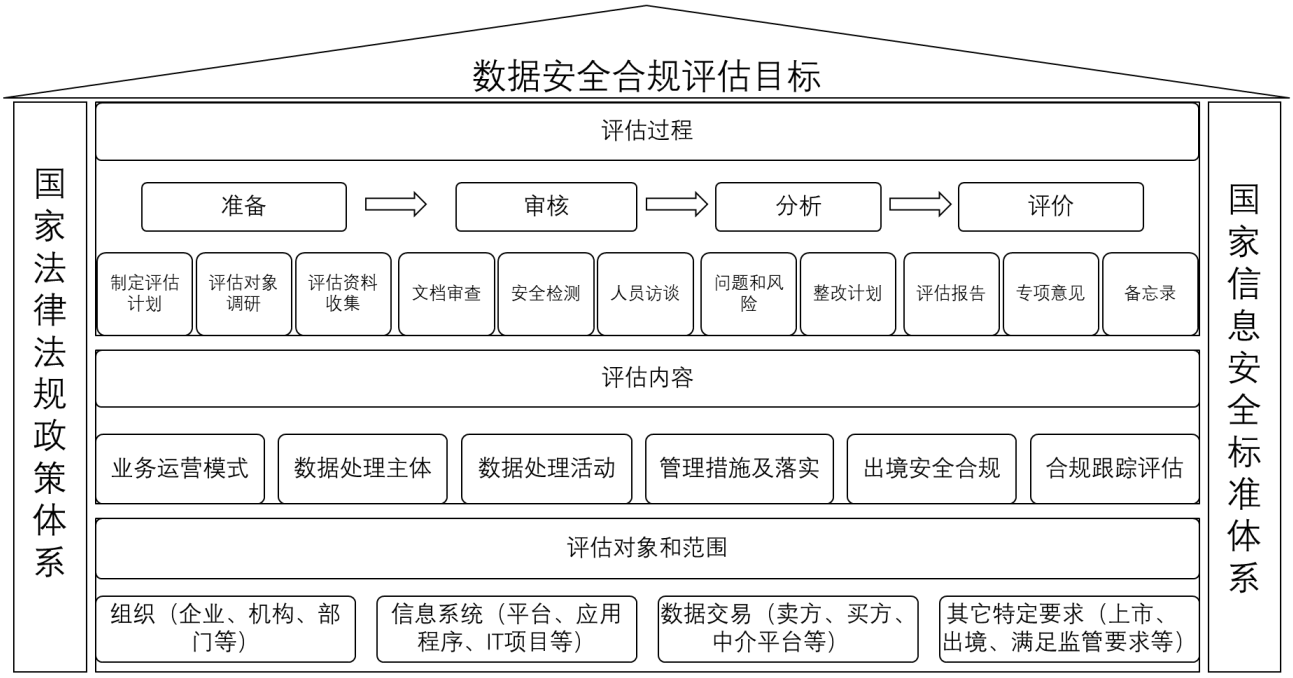

图1数据安全合规评估框架

6 评估过程

6.1 准备

6.1.1 评估方案制定

评估准备阶段应首先制订评估方案，评估方案的制订是一个不断确认的过程，至少应完成以下工作内容的确认：

a） 评估团队

应完成评估团队的组建，包括评估实施机构与被评估机构的人员数量、专业组成以及沟通机制的确认。评估组相关各方成员应具备可支撑评估开展的法律、技术、安全管理、业务规则等方面的相关专业知识和技能，可承担相关的评估和配合工作。

b） 评估范围

应根据评估目的和评估对象来确定评估范围的边界，例如，委托方为达到境外上市或投资收购等目的而进行的数据安全合规评估活动。在某些情况下，评估对象可能不是一个特定的组织机构，而是某个项目、某个业务、某笔交易或是某个信息系统等。可根据实际情况对评估内容进行裁剪辑或补充。

c） 评估依据

应根据评估目的确定评估依据。包括适用的国家相关法律法规、监管规定、行业准则和国际条约、规则，以及相关国际、国家及行业标准等。

d) 评估工具

应明确评估过程中使用的工具。包括安全检查工具、漏洞扫描工具、渗透测试工具等。

e) 评估进度

应对评估进度进行预期规划。以便参与各方预留时间和资源参与评估工作，保障评估活动的实施效率。

f) 评估风险

应对评估活动可能引入的风险及其影响进行分析，如审查活动对信息泄密的风险、测试扫描活动对业务运行和数据正确性的影响、评估工作自身的局限性及约束等，应采用最小影响原则并给出应对措施。

以上内容应与评估活动管理单位充分沟通，制定成文档化的评估方案并获得批准和实施授权。

6.1.2 评估对象调研

应对被评估的对象进行充分的调研，作为后续评估工作的基础。调研应包括如下内容：

a) 业务运营模式

评估对象涉及的业务范围、内容、模式以及与外部组织机构合作的情况。

b) 数据处理活动

评估对象处理数据的类型、流程、规模以及在处理过程中所处的角色和地位，评估数据收集、收集、存储、使用、加工、传输、提供、公开、删除等全生命周期处理活动的情况。

c) 安全管理制度及落实

评估对象的数据安全管理组织架构、管理制度、技术措施、网络安全等级保护、培训教育等情况。

d) 处罚及整改

评估对象及其所在组织涉及的数据合规的投诉、行政处罚、诉讼、仲裁，以及以往信息安全相关测评和数据安全合规评估的整改和纠正措施情况。

宜通过发放调查单的形式来对评估对象进行调研。

6.1.3 评估资料收集

应根据评估目的进行对评估对象相关的数据安全合规资料收集，包括但不仅限于如下内容：

a) 业务介绍、分子机构及股权架构、所在组织的营业执照以及相关行业的经营许可。
b) 与数据供应商和第三方公司签订的协议、合同和文件范本和实例以及对供应商的审查文件。
c) 现有的网络安全、数据安全、数据分级分类、个人信息保护等事项的管理文件。包括制度、规范、程序文件、行业准则和承诺、指引文件、培训考核和监督要求以及近三年执行相关活动形成的技术和质量记录等。
d) 近三年的与信息安全或数据安全相关的诉讼、仲裁和被执法机关调查和处罚的相关文件，包括约谈、调查通知、处罚通知、判决书等。
e) 近三年涉及的网络安全审查报告、等级保护的备案证明以及相关信息系统的等级保护测评报告、网络信息安全及数据安全风险评估报告等。
f) 已发生过的网络安全攻击、系统中断、信息泄露等事件的情况分析及应急响应报告。
g) 评估人员可通过对公开信息进行查询的方式获取评估对象的相关信息，以对收到的资料进行印证和补充。查询渠道可包括：

1) 国家企业信用信息公示系统、信息产业主管部门网站、各地行业主管部门网站、国家及地方网信部门网站以及执行和裁判信息公开网站等。
2) 可利用公共或专用网络搜索引擎对被评估对象散布在互联网或专用网络上的相关信息进行查阅整理。

必要时，可根据实际评估情况，要求被评估方补充资料。

6.2 审核

6.2.1 文档审查

评估人员应对在收集资料过程中收到的相关文件进行逐一审查，以评估相关制度、文件及落实情况是否符合评估依据的相关要求。

6.2.2 安全检测

评估人员可对相关实际运行的网络、信息系统和数据信息实施安全检测，通过查看、分析被测系统的响应和输出结果，评估被测系统的安全技术保障措施是否有效。执行此项工作时，应注意测试数据和评估工具可能对系统运行产生的影响，并尽可能减小这些影响。

6.2.3 人员访谈

必要时，作为文档审查和安全检测结果的补充，可对被评估对象涉及的相关人员进行访谈，以核实评估对象数据安全合规的实际情况。访谈可以采取交流、讨论、询问等形式，访谈对象可视情况包含如下人员：

a) 信息系统相关的研发人员、产品经理和业务设计人员。
b) 组织内部的业务负责人、技术负责人、数据安全负责人以及法律合规负责人。
c) 网络、应用和数据运维人员以及信息安全管理人员。

6.3 分析

6.3.1 问题和风险

在审核过程的执行中，如果发现问题，须及时对发现的问题进行记录，并对问题可能产生的风险进行分析。问题记录应包括如下内容：

a) 问题事实的描述，包括所在业务、违规事实和发生场景等。
b) 违反的内部制度名称及条款。
c) 违反的评估依据的名称及条款。
d) 问题可能引起的风险或处罚后果。
e) 必要时，问题的严重性级别。

6.3.2 整改计划

必要时，评估人员可协助评估对象所在组织针对问题进行整改计划的制定。整改计划应包括：

a) 问题的描述或识别信息。
b) 工作建议与整改措施。
c) 责任方或落实方。
d) 整改有效性的验证方。
e) 计划完成期限。

6.4 评价

6.4.1 评估报告

评估工作完成后，应形成数据安全合规评估报告，评估报告应包括如下内容：

a) 评估背景：描述评估的目的。
b) 评估声明：评估结果的适用范围、约束、假设以及免责声明。
c) 评估依据：评估所依赖的法律法规、相关标准或文件。
d) 评估范围：评估对象的组成和评估内容的描述。
e) 评估流程：评估实施活动的过程性描述。
f) 评估结论：在充分审核的基础上，对评估对象的数据安全合规情况进行客观、公正的结论性总结，可包括：
   1) 数据处理业务活动的合规性总结。
   2) 安全管理措施及落实情况的合规性总结。
   3) 技术保障措施及落实情况的合规性总结。
   4) 发现问题及存在风险情况总结。
   5) 适用时，针对之前的网络和数据安全审查、测评、评估、行政调查中发现问题的整改及落实情况的总结。
   6) 必要时，给予评估对象针对的问题整改及后续持续改进的意见和建议。

6.4.2 专项意见

基于特定目的的数据安全评估，可按被评估对象所在组织的要求出具专项分析意见，如：

a) 是否属于关键信息基础设施运营者的专项分析意见；
b) 数据分级分类管理的专项意见；
c) 是否需要进行网络安全审查的专项意见；
d) 关于数据出境的专项意见；
e) 关于上市融资项目的专项意见；

等。

6.4.3 备忘录

基于特定目的的数据安全评估，如发现涉及重大合规性问题，可能对特定目的的达成产生直接影响，可以备忘录的形式进行重大问题说明和风险揭示。以供评估对象所在组织快速了解问题并引起重视，更有针对性的实施整改并提高效率。

7 评估内容

7.1 业务运营模式

7.1.1 处理资质

应对评估对象所在组织的行政许可及相关证照的完备性、运营主体的一致性、授权范围与实际数据处理相关活动的匹配性以及质量管理体系的健全性进行审查。如营业执照、增值电信业务经营许可证、在线数据与交易处理业务许可证、网络文化经营许可证、网络出版服务许可证、信息网络传播视听节目许可证、互联网药品信息服务资格证、质量管理体系认证等及相关的许可和认证范围。

7.1.2 处理模式

应对评估对象或所在组织的业务模式、业务流程进行充分识别，包括：

a) 组织与客户、供应商和其它合作方的模式（提供方、接收方、共同处理等）。

b) 组织在数据处理或是交易链中所处的角色（收集方、使用方、交易中介方等）。

c) 组织是数据处理平台的建设者还是运营者，或两者兼有。

不同的业务模式及角色对于数据安全合规的要求不同，评估方应根据识别的结果来选取后续的评估内容。

7.1.3 系统平台

应对评估对象数据处理所依附的信息系统和网络资产进行识别，形成系统资产清单。包括各类应用系统、网站、移动APP、小程序、云平台等及网络系统，以决定安全检测等评估所覆盖的范围。

7.2 数据处理主体

7.2.1 外部处理

7.2.1.1 委托方

评估对象委托外部机构处理数据时，应对如下内容进行审核：

a) 建立数据安全评估、个人信息安全影响评估以及内外部数据安全检查与评估制度的情况。

b) 对受托方的资格审查的相关记录。包括行政许可、授权范围、质量管理体系等。

c) 与受托方签订的数据处理合同或协议的效力及内容。包括依照评估依据要求和合同约定履行数据安全要求、数据处理目的、处理期限、处理方式、信息种类、保护措施、处理地点、销毁、转委托处理、分享以及双方的权利和义务等。

d) 对受托方数据处理过程的监督记录。包括履行数据安全保护义务情况、处理方式及处理地点的正确性、是否进行超出目的处理、处理后数据的删除和销毁情况等。

e) 涉及处理个人信息的，委托前进行个人信息影响评估的实施记录并保存情况，个人信息影响评估活动应依据 GB/T 39335—2020 开展。

7.2.1.2 受托方

评估对象为数据处理的受托方时，应对如下内容进行审核：

a) 必要时，对委托方的资格审查的相关记录。包括行政许可、授权范围、质量管理体系等。

b) 委托合同或协议中委托方确保数据来源合法的承诺和违约赔偿责任。

c) 受托方依照评估依据要求和合同约定履行数据安全保护义务，不超出约定范围处理方式和处理目的承诺。

d) 相关情况下（如合同无效、中止、处理完成后等）数据的返还、删除、销毁的相关实施和确认记录。

7.2.2 共同处理

评估对象为数据的共同处理方时，应对如下内容进行审核：

a) 自主决定数据处理目的及处理方式的主体资格。

b) 共同处理数据各方的权利、义务的约定。

c) 依法承担相关法律责任的约定。

7.2.3 主体变更转移

评估对象在数据处理过程中发生合并、分立、解散、破产等变化导致数据处理的主体发生转移时，应对如下内容进行审核：

a) 通知数据来源数据（可能为组织或个人），处理方发生变化的相关信息（名称/姓名、联系方式等）。

b) 涉及处理个人信息的，若处理目的和方式发生变化，重新取得个人同意的相关证据。

7.3 数据处理活动

7.3.1 分类分级

应对数据分级类情况进行评估，内容包括：

a) 数据分类分级的依据对相关评估依据要求的符合性。如：

1) 从对国家安全、公共利益或个人、组织合法权益的危害程度对数据进行分类分级；

2) 根据个人信息的处理目的、处理方式、个人信息的种类以及对个人权益的影响、可能存在的安全风险等因素，采取个人信息分类管理措施；

3) 结合对个人权益影响分析的结果（宜参照 GB/T 39335—2020 表 D3）对个人信息数据进行分类分级。

b) 对不同分级的数据分别实施不同的管理和技术保护措施的合理性。

注：在大多数情况，对不同分级的数据实施完全一致的管理和技术保护措施是不现实的。

7.3.2 处理过程

7.3.2.1 收集

应对收集数据的情况进行评估，内容包括：

a) 收集信息的合法性基础，相关资质、行政许可、授权等。是否收集与其提供的服务无关的个人信息，是否违反评估依据要求和双方的约定收集、使用个人信息。

b) 收集个人信息的授权同意情况，宜参照 GB/T 41479—2022 5.4、GB/T 41391—2022 6.4 以及评估依据要求开展。

c) 收集信息行为的正当、必要性，宜参照 GB/T 41479—2022 5.2 以及评估依据进行审核。包括：

1) 用户授权（告知—同意）使用的展示时机、形式（显著、醒目、非默认同意）和内容的规范性。

2) 收集内容应当与处理目的直接相关，采取对个人权益影响最小的方式，限于实现处理目的的最小范围，不过度收集个人信息。

3) 应用系统实际收集内容与其宣称的隐私政策、用户协议等内容的一致性。

注：对 APP 的个人信息收集行为进行评估，宜参照 GB/T 41391—2022 开展。

7.3.2.2 存储

应对数据的存储情况进行评估，内容包括：

a) 对数据及其副本存储所采取的安全措施，宜参照 GB/T 41479—2022 5.3 以及评估依据要求进行审核。审核项应包括：

1) 技术保护措施的要求，如加密算法、访问控制、安全审计、个人信息的匿名化等。

2) 存储期限，符合评估依据要求、合同和用户约定的有效期限。

3） 对重要系统和数据库进行容灾备份。

b） 数据及其副本的存储地点满足数据本地化存储和数据跨境的评估依据要求的情况。

7.3.2.3 使用、加工

应对数据的使用和加工情况进行评估，内容包括：

a） 数据的使用和加工获得评估依据要求和相关方授权的文件内容。

b） 数据实际使用、加工的方式和范围符合约定。

注：对于隐蔽的、嵌入式或第三方 SDK 提供的处理过程可采用安全检测的手段予以确认。

c） 未涉及相关规定禁止的数据使用和加工，如未获得用户授权、用户已撤回同意、歧视性的营销策略、违反道德伦理等情况。

注：宜结合 GB/T 41479—2022 5.4-5.5 的要求开展。

7.3.2.4 传输、提供

应对数据的传输和提供情况进行评估，内容包括：

a） 数据提供和接收方的审核，应符合本标准 7.2.1 的要求。

b） 数据传输和提供的安全措施和协议约定，宜参照 GB/T 41479—2022 5.6-5.7 以及法律和相关行业要求进行审核。

c） 涉及第三方 SDK 或 API 的，应对 SDK 组件或 API 接口进行安全检测，评估是否存在已知的安全漏洞以及可能引起数据泄露或未授权的数据跨境的行为。

d） 利用个人信息和个性化推送算法向用户提供信息的，须对推送信息的真实性、准确性以及来源合法性负责，并符合以下要求：

1） 收集个人信息用于个性化推荐时，应取得个人单独同意；

2） 设置易于理解、便于访问和操作的一键关闭个性化推荐选项，允许用户拒绝接受定向推送信息，允许用户重置、修改、调整针对其个人特征的定向推送参数；

3） 允许个人删除定向推送信息服务收集产生的个人信息，法律、行政法规另有规定或者与用户另有约定的除外。

e）向其他个人信息处理者提供其处理的个人信息的，应当向个人告知接收方的名称或者姓名、联系方式、处理目的、处理方式和个人信息的种类，并取得个人的单独同意。

f）从事数据交易中介服务的机构提供服务，应要求数据提供方说明数据来源，审核交易双方的身份，并留存审核、交易记录。

7.3.2.5 公开

应对评估对象的数据公开行为进行评估，包括：

a） 公开前的影响评估情况。如是否对危害国家安全、公共安全、经济安全和社会稳定造成影响。

b） 必要时，数据公开行为和内容是否取得了相关单位的许可和授权。

c） 处理已公开的个人信息，对个人权益有重大影响的，应按评估依据要求取得个人同意。

7.3.2.6 删除、匿名化

应对评估对象删除数据和用户注销后的匿名化处理情况进行评估，内容包括：

a） 对符合 GB/T 41479—2022 5.13、GB/T 35273—2020 8.3、8.5 和评估依据要求的数据进行删除或匿名化处理的处理记录，评估方应从处理的内容、数据量、及时性等方面进行审查。

b） 适用时，APP 提供的用户注销用户的方式，宜参照 GB/T 35273—2020 8.5 的要求进行审核。

c) 处理范围包括数据本身及其全部副本。
d) 处理后的数据无法或不再继续参与数据处理与加工的证明。
e) 适用时，拒绝删除或注销用户给出反馈的情况，应包括：
   1) 通知的告知渠道，如 APP 通知、短信、邮件等。
   2) 拒绝理由，如依据的法律法规、行业监管要求等。
   3) 投诉渠道和途径。

7.4 管理措施及落实

7.4.1 责任人与责任机构

应对评估对象所在组织的数据安全管理责任人和组织架构进行评估，内容包括：

a) 责任人，包括背景审查、工作职责、绩效考核、履行其对应的工作职能的相关工作记录等。可参照 GB/T 41479—2022 6.1、6.2 的要求进行审核。个人信息处理者应公开个人信息保护负责人的联系方式，并将个人信息保护负责人的姓名、联系方式等报送履行个人信息保护职责的部门。
b) 责任机构，包括机构的岗职位设置、运行经费、独立性以及开展相关工作的运行记录等。

7.4.2 数据安全管理措施

应对评估对象所在组织的数据安全管理措施的完整性、一致性、可行性、依从性等方面进行评估，评估内容可包括：

a) 管理体系，包括总体要求、机构设置及职责、基本原则等。
b) 处理流程管理，包括数据收集、使用、传输、提供、存储、删除等管理要求。
c) 数据分类分级管理：
   1) 划分数据类别、级别的原则及对应采取管理和技术措施的要求。
   2) 适用时，个人信息按敏感程度的分类及保护措施。
d) 网络及数据安全风险评估及报送机制，按相关要求定期开展风险评估并报送或公布结果的相并规定。
e) 数据安全风险管理机制，包括开展数据安全风险评估、报告、共享、预警检测等机制。
c) 网络及数据安全应急预案，发现信息安全事件时，启动应急预案、采取补救措施、向主管部门报告、定期实施应急演练等措施。可参照 GB/T 41479—2022 6.3 的要求进行审核。
f) 投诉、举报制度，接受网络信息安全投诉、举报并及时处理、反馈的机制、
a) 数据出境管理，适用时，对数据出境条件、数据出境自评估及程序的要求。
b) 网络安全审查，适用时，制定并落实网络安全审查相关的管理制度和程序。
c) 个人信息管理，包括
   1) 对个人信息访问和操作权的要求；
   2) 定期进行个人信息合规审计的要求；
   3) 适用时，对个人信息影响评估的要求；
   4) 适用时，对未成年人和儿童信息保护的管理要求；
   5) 员工个人信息保护，如对员工的简历、体检信息、生物识别信息的以及雇佣外籍员工的信息保护的规定。

7.4.3 数据安全技术措施

应对评估对象的数据安全保护的技术措施落实情况进行评估，内容可包括：

a) 定期的安全检测，包括网络、主机、应用等层面的安全扫描和安全配置的检测。
b) 采取监测、记录网络运行状态、网络安全事件的技术措施，并按照评估依据要求留存相关的网络日志情况；
c) 防御措施，防范计算机病毒、网络攻击等危害网络安全行为的措施有效性检测。
d) 数据备份，包括备份的内容、范围、形式（全备份、增量备份、差分备份等）、备份地点（本地、异地）、备份及时性以及备份有效性验证等。
e) 加密，包括加密的内容、算法的强度、算法的使用（如必须使用国密算法的场景）、密钥的管理措施等。
f) 去标识化，适用时，对个人信息去标识化的情况，宜参照 GB/T 37964—2019 5、6 部分的要求进行审核。
g) 访问控制，数据访问和操作前对访问者进行鉴别与授权的记录和检测。
h) 监控和预警记录，对网络和应用运行状态、操作的监控和预警记录的完整性和保存期限的检测。

7.4.4 人员管理及安全教育

应对评估对象的人员管理及安全教育落实情况进行评估，内容应包括：

a) 人员签保密协议的情况，如保密内容、保密范围、保密期限、奖惩措施等。
b) 人员上岗前的审查情况，如工作履历、技术能力、人员资质、教育学习等。
c) 人员在岗期间的安全意识、工作技能、管理制度的培训及培训有效性考核情况。
d) 人员离岗后按照相关管理要求进行离岗交接、审计、脱密等措施执行的情况。

7.4.5 网络安全及关键信息基础设施保护

应对评估对象实施网络安全等级保护情况进行评估，内容应包括：

a) 评估对象的定级和备案情况。须按 GB/T 22240 的要求对定级结果进行复核。
b) 对于确定为二级以上的网络信息系统，须对等级保护备案情况、测评的频率进行确认。
c) 对于确定为三级及以上系统、面向社会服务的政务信息系统以及关键信息基础设施按频率开展密码评估工作的情况进行确认。
d) 处理重要数据的系统原则上应当满足三级以上网络安全等级保护和关键信息基础设施安全保护要求，处理核心数据的系统依照有关评估依据要求从严保护。
e) 必要时，网络信息系统安全保护措施和测评整改符合要求的情况，应按 GB/T 22239 对应级别的相关要求进行审核和检测。
f) 如评估对象有已被认定或可能被认定为关键信息基础设施运营者的情况，还应按 GB/T 39204 的相关要求进行审核和检测。

注：关键信息基础设施的确定参见附录 B。

7.4.6 问题整改和纠正措施

适用时，应对评估对象涉及与数据和网络安全相关的投诉、争议、诉讼、仲裁、行政处罚等情况评估，内容应包括：

a) 投诉、争议、诉讼、仲裁、行政处罚的进展情况。
b) 采取的纠正、纠正措施的适宜性和落实情况。
c) 是否可能产生潜在的被监管部门进一步调查或采取其他措施，导致更为严厉的处罚。

7.5 数据出境安全合规

适用时，应对评估对象数据出境的情况进行评估，评估内容包括：

a) 向个人告知境外接收方的名称或者姓名、联系方式、处理目的、处理方式、个人信息的种类以及个人向境外接收方行使本法规定权利的方式和程序等事项，并取得个人的单独同意。

b) 组织指定个人信息安全影响评估的责任部门或责任人员，自行开展或聘请外部独立第三方进行个人信息保护影响评估，个人信息保护影响评估报告和处理情况记录应当至少保存三年。

注：个人信息影响评估活动应依据 GB/T 39335—2020 开展。

c) 按照国家网信部门制定的标准合同与境外接收方订立合同，约定双方的权利和义务。合同中应当至少约定数据出境的目的及方式、境外数据保存情况、境外数据再转移、不可抗力以及其他违约或侵权事宜及其解决途径与方式。

d) 评估对象的数据出境处理活动是否需向网信部门等管理机构申报数据出境安全评估，如需要申报，应开展数据出境风险自评估，并向网信部门申报数据出境安全评估。

注：自评估内容应当包括处理数据的目的及范围、敏感程度、境外接收方义务及相关责任，审慎评估其出境对国家安全、公共利益等法益带来的风险，以及其他可能影响数据出境安全的事项。

e) 未达到申报数据出境安全评估条件的，是否经专业认证机构进行个人信息保护认证。

f) 关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。

g) 符合境外地区相关规定和要求的情况。

h) 评估依据要求的禁止出境的情况。国家网信部门认定不得出境的数据，是否已停止数据出境，并采取有效措施对已出境数据的安全予以补救。

i) 适用时，使用境外的服务供应商和第三方组件（SDK）可能引起的潜在数据传输链路的数据出境风险情况。

j) 必要时，跨境传输相关的管理记录，包括传输发送方、接收方及所在区域、传输机制、信息类型、处理目的、合同条款、数据主体同意的相关记录。

7.6 安全合规跟踪评估

宜对评估对象数据的安全合规管理的改进和按期执行情况进行持续跟踪监控和评估，包括：

a) 结合评估依据要求，对外部政策、用户服务协议、合同范本等内容进行定期审查和更新的情况。

b) 持续改进和完善内部数据安全管理制度以及流程优化的情况。

c) 定期开展员工数据安全合规培训和考核、开展年度安全风险与安全合规评估以及相关的问题整改落实情况。

附 录 A

附 录 B （资料性）

附 录 C 评估内容和评估重点的影响因素

在数据安全合规评估工作中，应按委托方的评估目的来界定评估范围、确定评估内容并划定评估重点，并结果在评估的过程中发现的相关情况进行动态调整。影响因素包括评估对象的主体、涉及的数据类型、数据处理的规模等，以及这些因素的综合作用。

a) 评估对象主体，如果评估过程中发现评估对象的主体已被评定为相应级别的网络安全等级保护对象或认定为关键信息基础设施运营者（CIIO）或存在后继被认定为关键信息基础设施运营者的可能性。就可将部分评估重点放在评估对象是否符合相关评估依据对相应级别的网络安全等级保护和CIIO的要求上。如涉及个人信息和重要数据出境，则应评估相应的三件条件，即因业务需要、确需向境外提供、经过网信部门组织的安全评估。

b) 涉及的数据类型，国家建立数据分类分级保护制度，从对国家安全、公众利益或个人、组织合法权益的危害程度对数据进行分类分级，可分为一般数据、重要数据、核心数据，采取不同的保护措施。对于关系国家安全、国民经济命脉、重要民生、重大公共利益等的国家核心数据，实行更加严格的管理制度。重要和核心数据主要覆盖的行业涉及信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业、地理、医疗等，评估过程中应对是否涉及重要及核心数据进行判断，如果为肯定，则对相应的数据管理措施进行重点评估，如定期按照规定开展数据安全风险评估并向有关和管部门报送风险评估报告，风险评估报告应包括处理的重要数据的种类、数量、开展数据处理活动的情况，面临的数据安全风险及应对措施等。

c) 数据处理的规模，对于CIIO和个人信息达到国家网信部门规定的数量的个人信息处理者。应对其特别遵守的保护义务进行重点评估，如：

   1) 应当将在境内收集和产生的个人信息存储在境内，确需向境外提供的，应当能过国家网信部门组织的安全评估。
   2) 指定个人信息保护负责人，公开姓名、联系方式。报送履行个人信息保护职责的部门。
   3) 用户数量巨大的互联网服务平台，应建立健全个人信息保护合规体系、由外部独立机构对个人信息保护情况进行监督、定期发布个人信息保护社会责任报告、接受社会监督等。
   4) 掌握超过100万用户个人信息的网络平台运营者赴国外上市，必须向网络安全审查办公室申报网络安全审查，并在上市文件中披露可能产生的经营影响。

附 录 D

附 录 E （资料性）

附 录 F 关键信息基础设施确定指南

一、什么是关键信息基础设施

关键信息基础设施是指面向公众提供网络信息服务或支撑能源、通信、金融、交通、公用事业等重要行业运行的信息系统或工业控制系统，且这些系统一旦发生网络安全事故，会影响重要行业正常运行，对国家政治、经济、科技、社会、文化、国防、环境以及人民生命财产造成严重损失。

关键信息基础设施包括网站类，如党政机关网站、企事业单位门户网站、新闻网站等；平台类，如即时通信、网上购物、网上支付、搜索引擎、电子邮件、论坛、地图、音视频等网络服务平台；生产业务类，如办公和业务系统、工业控制系统、大型数据中心、云计算平台、电视转播系统等。

二、如何确定关键信息基础设施

关键信息基础设施的确定，通常包括三个步骤，一是确定关键业务，二是确定支撑关键业务的信息系统或工业控制系统，三是根据关键业务对信息系统或工业控制系统的依赖程度或可能造成的损失认定关键信息基础设施。

(一)确定本地区、本部门、本行业的关键业务。

可参考下表，结合本地区、本部门、本行业实际梳理关键业务。

行业		关键业务
能源	电力	电力生产（含火电、水电、核电等）
		电力传输
		电力配送
	石油石化	油气开采
		炼化加工
		油气输送
		油气储存
	煤炭	煤炭开采
		煤化工
金融		银行运营
		证券期货交易
		清算支付
		保险运营
交通	铁路	客运服务
		货运服务
		运输生产
		车站运行
	民航	空运交通管控
		机场运行
		订票、离岗及飞行调度检查安排
		航空公司运营
	公路	公路交通管控
		智能交通系统（一卡通、ETC收费等）

行业		关键业务
	水运	水运公司运营（含客运、货运）
		港口管理运营
		航运交通管控
水利		水利枢纽运行及管控
		长距离输水管控
		城市水源地管控
医疗卫生		医院等卫生机构运行
		疾病控制
		急救中心运行
环境保护		环境监测及预警（水、空气、土壤、核辐射等）
工业制造(原材料、装备、消费品、电子制造)		企业运营管理
		智能制造系统（工业互联网、物联网、智能装备等）
		危化品生产加工和存储管控（化学、核等）
		高风险工业设施运行管控
市政		水、暖、气供应管理
		城市轨道交通
		污水处理
		智慧城市运行及管控
电信与互联网		语音、数据、互联网基础网络及枢纽
		域名解析服务和国家顶级域注册管理
		数据中心/云服务
广播电视		电视播出管控
		广播播出管控
政府部门		信息公开
		面向公众服务
		办公业务系统

（二） 确定关键业务相关的信息系统或工业控制系统。

根据关键业务，逐一梳理出支撑关键业务运行或与关键业务相关的信息系统或工业控制系统，形成候选关键信息基础设施清单。如电力行业火电企业的发电机组控制系统、管理信息系统等；市政供水相关的水厂生产控制系统、供水管网监控系统等。

（三） 认定关键信息基础设施。

对候选关键信息基础设施清单中的信息系统或工业控制系统，根据本地区、本部门、本行业实际，参照以下标准认定关键信息基础设施。

A. 网站类

符合以下条件之一的，可认定为关键信息基础设施：

1. 县级（含）以上党政机关门户网站。
2. 日均访问量超过100万人次的网站。
3. 一旦发生网络安全事故，可能造成以下影响之一的：
   1） 影响超过100万人工作、生活；

2) 影响单个地市级行政区30%以上人口的工作、生活；
3) 造成超过100万人个人信息泄露；
4) 造成大量机构、企业敏感信息泄露；
5) 造成大量地理、人口、资源等国家基础数据泄露；
6) 严重损害政府形象、社会秩序，或危害国家安全。

4. 其他应该认定为关键信息基础设施。

B. 平台类

符合以下条件之一的，可认定为关键信息基础设施：

1. 注册用户数超过1000万，或活跃用户（每日至少登陆一次）数超过100万。
2. 日均成交订单额或交易额超过1000万元。
3. 一旦发生网络安全事故，可能造成以下影响之一的：
   1) 造成1000万元以上的直接经济损失；
   2) 直接影响超过1000万人工作、生活；
   3) 造成超过100万人个人信息泄露；
   4) 造成大量机构、企业敏感信息泄露；
   5) 造成大量地理、人口、资源等国家基础数据泄露；
   6) 严重损害社会和经济秩序，或危害国家安全。
4. 其他应该认定为关键信息基础设施。

C. 生产业务类

符合以下条件之一的，可认定为关键信息基础设施：

1. 地市级以上政府机关面向公众服务的业务系统，或与医疗、安防、消防、应急指挥、生产调度、交通指挥等相关的城市管理系统。
2. 规模超过3000个标准机架的数据中心。
3. 一旦发生安全事故，可能造成以下影响之一的：
   1) 影响单个地市级行政区30%以上人口的工作、生活；
   2) 影响10万人用水、用电、用气、用油、取暖或交通出行等；
   3) 导致5人以上死亡或50人以上重伤；
   4) 直接造成5000万元以上经济损失；
   5) 造成超过100万人个人信息泄露；
   6) 造成大量机构、企业敏感信息泄露。
   7) 造成大量地理、人口、资源等国家基础数据泄露。
   8) 严重损害社会和经济秩序，或危害国家安全。
4. 其他应该认定为关键信息基础设施。

附 录 G

附 录 H （资料性）

附 录 I 评估模板示例

I.1 数据安全合规调查单示例

数据安全合规调查单

一、业务情况说明

1、 包括业务内容、业务模式和业务流程

2、 业务主体、合作方及合作模式

3、 用户类型与用户协议

二、数据处理活动

1、 收集的类型和内容

2、 收集的场景、来源和方式

3、 从外部供应获取数据的方式和合同

4、 数据的收费和商业运营

5、 是否涉及不满 14 岁的未成年（儿童）信息，以及相关保护措施。

6、 数据使用的场景、目的和用途

7、 如何整理、加工和分析数据

8、 是否对外部提供、转让、传输？以及提供的方式和收费情况

9、 引用第三方 SDK 及审核情况

10、 对本公司和供应商的合规审查情况

11、 数据存储和加工的位置。是否涉及跨境？

12、 数据存储的期限和销毁情况。

三、安全管理制度及落实

1、 负责数据保护的部门和责任人

2、 现有的网络安全、数据安全以及个人信息保护的管理制度

3、 人员管理以及教育培训情况

4、 是否涉及等保、关保，提供相关定级证明和测评报告

5、 保障相关信息和数据安全要求而采取的技术措施以用外部攻击的防范和监控措施。

6、 数据是否分级分类，如何实施分类保护

四、处罚及整改情况

1、 近三年因信息和数据安全相关事宜被投诉、诉讼、仲裁、被执法机关调查和处罚及整改情况。

2、 以往信息安全相关测评和数据安全合规评估的整改和纠正措施情况

I.2 数据安全合规评估报告示例

数据安全合规评估报告

一、评估背景：描述评估的目的。

二、评估声明：评估结果的适用范围、约束、假设以及免责声明。

三、评估依据：评估所依赖的法律法规、相关标准或文件。

四、评估范围：评估对象的组成和评估内容的描述。

五、评估流程：评估实施活动的过程性描述。

六、评估结论：

1、 数据处理业务活动的合规性总结。

2、 安全管理措施及落实情况的合规性总结。

3、 技术保障措施及落实情况的合规性总结。

4、 发现问题及存在风险情况总结。

5、 针对之前的网络和数据安全审查、测评、评估、行政调查中发现问题的整改及落实情况的总结（可选）。

6、 给予评估对象针对的问题整改及后续持续改进的意见和建议（可选）。

附录 1、专项分析意见（可选）

1、 关于是否属于关键信息基础设施运营者（CIIO）的专项分析意见

2、 关于数据分级分类管理的专项分析意见

3、 关于需要进行网络安全审的专项分析意见

4、 关于数据出境的专项分析意见

5、 关于上市融资项目的专项分析意见

。。。。。。

附录 2、重大问题及风险揭示备忘录（可选）

附 录 J

附 录 K （资料性）

附 录 L 数据安全合规相关主要国内法律罚则

法律名称	法律条款	罚 则
《中华人民共和国网络安全法》（2016年11月7日颁布版）	第五十九条	网络运营者不履行本法第二十一条、第二十五条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处一万元以上十万元以下罚款，对直接负责的主管人员处五千元以上五万元以下罚款。关键信息基础设施的运营者不履行本法第三十三条、第三十四条、第三十六条、第三十八条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。
	第六十条	违反本法第二十二条第一款、第二款和第四十八条第一款规定，有下列行为之一的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处五万元以上五十万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款： （一）设置恶意程序的； （二）对其产品、服务存在的安全缺陷、漏洞等风险未立即采取补救措施，或者未按照规定及时告知用户并向有关主管部门报告的； （三）擅自终止为其产品、服务提供安全维护的。
	第六十一条	网络运营者违反本法第二十四条第一款规定，未要求用户提供真实身份信息，或者对不提供真实身份信息的用户提供相关服务的，由有关主管部门责令改正；拒不改正或者情节严重的，处五万元以上五十万元以下罚款，并可以由有关主管部门责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。
	第六十二条	违反本法第二十六条规定，开展网络安全认证、检测、风险评估等活动，或者向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息的，由有关主管部门责令改正，给予警告；拒不改正或者情节严重的，处一万元以上十万元以下罚款，并可以由有关主管部门责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处五千元以上五万元以下罚款。

法律名称	法律条款	罚　　则
	第六十三条	违反本法第二十七条规定，从事危害网络安全的活动，或者提供专门用于从事危害网络安全活动的程序、工具，或者为他人从事危害网络安全的活动提供技术支持、广告推广、支付结算等帮助，尚不构成犯罪的，由公安机关没收违法所得，处五日以下拘留，可以并处五万元以上五十万元以下罚款；情节较重的，处五日以上十五日以下拘留，可以并处十万元以上一百万元以下罚款。 单位有前款行为的，由公安机关没收违法所得，处十万元以上一百万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。 违反本法第二十七条规定，受到治安管理处罚的人员，五年内不得从事网络安全管理和网络运营关键岗位的工作；受到刑事处罚的人员，终身不得从事网络安全管理和网络运营关键岗位的工作。
	第六十四条	网络运营者、网络产品或者服务的提供者违反本法第二十二条第三款、第四十一条至第四十三条规定，侵害个人信息依法得到保护的权利的，由有关主管部门责令改正，可以根据情节单处或者并处警告、没收违法所得、处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款；情节严重的，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照。 违反本法第四十四条规定，窃取或者以其他非法方式获取、非法出售或者非法向他人提供个人信息，尚不构成犯罪的，由公安机关没收违法所得，并处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款。
	第六十五条	关键信息基础设施的运营者违反本法第三十五条规定，使用未经安全审查或者安全审查未通过的网络产品或者服务的，由有关主管部门责令停止使用，处采购金额一倍以上十倍以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。
	第六十六条	关键信息基础设施的运营者违反本法第三十七条规定，在境外存储网络数据，或者向境外提供网络数据的，由有关主管部门责令改正，给予警告，没收违法所得，处五万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

法律名称	法律条款	罚　　则
	第六十七条	违反本法第四十六条规定，设立用于实施违法犯罪活动的网站、通讯群组，或者利用网络发布涉及实施违法犯罪活动的信息，尚不构成犯罪的，由公安机关处五日以下拘留，可以并处一万元以上十万元以下罚款；情节较重的，处五日以上十五日以下拘留，可以并处五万元以上五十万元以下罚款。关闭用于实施违法犯罪活动的网站、通讯群组。 单位有前款行为的，由公安机关处十万元以上五十万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。
	第六十八条	网络运营者违反本法第四十七条规定，对法律、行政法规禁止发布或者传输的信息未停止传输、采取消除等处置措施、保存有关记录的，由有关主管部门责令改正，给予警告，没收违法所得；拒不改正或者情节严重的，处十万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。 电子信息发送服务提供者、应用软件下载服务提供者，不履行本法第四十八条第二款规定的安全管理义务的，依照前款规定处罚。
	第六十九条	网络运营者违反本法规定，有下列行为之一的，由有关主管部门责令改正；拒不改正或者情节严重的，处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员，处一万元以上十万元以下罚款： （一）不按照有关部门的要求对法律、行政法规禁止发布或者传输的信息，采取停止传输、消除等处置措施的； （二）拒绝、阻碍有关部门依法实施的监督检查的； （三）拒不向公安机关、国家安全机关提供技术支持和协助的。
	第七十条	发布或者传输本法第十二条第二款和其他法律、行政法规禁止发布或者传输的信息的，依照有关法律、行政法规的规定处罚。
	第七十一条	有本法规定的违法行为的，依照有关法律、行政法规的规定记入信用档案，并予以公示。
	第七十二条	国家机关政务网络的运营者不履行本法规定的网络安全保护义务的，由其上级机关或者有关机关责令改正；对直接负责的主管人员和其他直接责任人员依法给予处分。

法律名称	法律条款	罚　　则
	第七十三条	网信部门和有关部门违反本法第三十条规定，将在履行网络安全保护职责中获取的信息用于其他用途的，对直接负责的主管人员和其他直接责任人员依法给予处分。 网信部门和有关部门的工作人员玩忽职守、滥用职权、徇私舞弊，尚不构成犯罪的，依法给予处分。
	第七十四条	违反本法规定，给他人造成损害的，依法承担民事责任。 违反本法规定，构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。
	第七十五条	境外的机构、组织、个人从事攻击、侵入、干扰、破坏等危害中华人民共和国的关键信息基础设施的活动，造成严重后果的，依法追究法律责任；国务院公安部门和有关部门并可以决定对该机构、组织、个人采取冻结财产或者其他必要的制裁措施。
《中华人民共和国数据安全法》（2021年06月10日颁布版）	第四十五条	开展数据处理活动的组织、个人不履行本法第二十七条、第二十九条、第三十条规定的数据安全保护义务的，由有关主管部门责令改正，给予警告，可以并处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员可以处一万元以上十万元以下罚款；拒不改正或者造成大量数据泄露等严重后果的，处五十万元以上二百万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处五万元以上二十万元以下罚款。 违反国家核心数据管理制度，危害国家主权、安全和发展利益的，由有关主管部门处二百万元以上一千万元以下罚款，并根据情况责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照；构成犯罪的，依法追究刑事责任。
	第四十六条	违反本法第三十一条规定，向境外提供重要数据的，由有关主管部门责令改正，给予警告，可以并处十万元以上一百万元以下罚款，对直接负责的主管人员和其他直接责任人员可以处一万元以上十万元以下罚款；情节严重的，处一百万元以上一千万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款。
	第四十七条	从事数据交易中介服务的机构未履行本法第三十三条规定的义务的，由有关主管部门责令改正，没收违法所得，处违法所得一倍以上十倍以下罚款，没有违法所得或者违法所得不足十万元的，处十万元以上一百万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照；

法律名称	法律条款	罚　　则
		对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。
	第四十八条	违反本法第三十五条规定，拒不配合数据调取的，由有关主管部门责令改正，给予警告，并处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。 违反本法第三十六条规定，未经主管机关批准向外国司法或者执法机构提供数据的，由有关主管部门给予警告，可以并处十万元以上一百万元以下罚款，对直接负责的主管人员和其他直接责任人员可以处一万元以上十万元以下罚款；造成严重后果的，处一百万元以上五百万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处五万元以上五十万元以下罚款。
	第四十九条	国家机关不履行本法规定的数据安全保护义务的，对直接负责的主管人员和其他直接责任人员依法给予处分。
	第五十条	履行数据安全监管职责的国家工作人员玩忽职守、滥用职权、徇私舞弊的，依法给予处分。
	第五十一条	窃取或者以其他非法方式获取数据，开展数据处理活动排除、限制竞争，或者损害个人、组织合法权益的，依照有关法律、行政法规的规定处罚。
	第五十二条	违反本法规定，给他人造成损害的，依法承担民事责任。 违反本法规定，构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。
《中华人民共和国个人信息保护法》（2021年08月20日颁布版）	第六十六条	违反本法规定处理个人信息，或者处理个人信息未履行本法规定的个人信息保护义务的，由履行个人信息保护职责的部门责令改正，给予警告，没收违法所得，对违法处理个人信息的应用程序，责令暂停或者终止提供服务；拒不改正的，并处一百万元以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。 有前款规定的违法行为，情节严重的，由省级以上履行个人信息保护职责的部门责令改正，没收违法所得，并处五千万元以下或者上一年度营业额百分之五以下罚款，并可以责令暂停相关业务或者停业整顿、通报有关主管部门吊销相关业务许可或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款，并可以决定禁止其在一定期限内担任相关企业的董事、监事、高级管理人员和个人信息保护负责人。

法律名称	法律条款	罚　　则
	第六十七条	有本法规定的违法行为的，依照有关法律、行政法规的规定记入信用档案，并予以公示。
	第六十八条	国家机关不履行本法规定的个人信息保护义务的，由其上级机关或者履行个人信息保护职责的部门责令改正；对直接负责的主管人员和其他直接责任人员依法给予处分。
		履行个人信息保护职责的部门的工作人员玩忽职守、滥用职权、徇私舞弊，尚不构成犯罪的，依法给予处分。
	第六十九条	处理个人信息侵害个人信息权益造成损害，个人信息处理者不能证明自己没有过错的，应当承担损害赔偿等侵权责任。 前款规定的损害赔偿责任按照个人因此受到的损失或者个人信息处理者因此获得的利益确定；个人因此受到的损失和个人信息处理者因此获得的利益难以确定的，根据实际情况确定赔偿数额。
	第七十条	个人信息处理者违反本法规定处理个人信息，侵害众多个人的权益的，人民检察院、法律规定的消费者组织和由国家网信部门确定的组织可以依法向人民法院提起诉讼。
	第七十一条	违反本法规定，构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

附 录 M

附 录 N （资料性）

附 录 O 评估内容与主要国内法律规定对应表

评估内容	相关法律规定
处理资质	《中华人民共和国数据安全法》 第三十四条 《中华人民共和国个人信息保护法》 第三十八条，第四十条
外部处理	《中华人民共和国个人信息保护法》 第二十一条，第二十三条，第二十四条，第五十五条， 第五十九条
共同处理	《中华人民共和国个人信息保护法》 第二十条
主体变更转移	《中华人民共和国个人信息保护法》 第二十二条
分类分级	《中华人民共和国网络安全法》 第二十一条第（四）项 《中华人民共和国数据安全法》 第二十一条第一款、第三款， 《中华人民共和国个人信息保护法》 第五十一条第一款第（二）项
处理过程	《中华人民共和国网络安全法》 第二十二条，第四十条 ，第四十一条，第四十二条，第四十三条，第三十七条，第四十七条，第四十八条 《中华人民共和国数据安全法》 第四章（第二十七至三十六条） 《中华人民共和国个人信息保护法》 第四条至第十条，第二章（第十三条至第三十七条），第三章（第三十八至第四十三条），第四章（第四十四至第五十条），第五章（第五十一条至第五十九条）
责任人与责任机构	《中华人民共和国网络安全法》 第二十一条第一款第（一）项，第三十四条第一款第（一）项。 《中华人民共和国数据安全法》 第二十七条第二款。 《中华人民共和国个人信息保护法》 第五十二条。

评估内容	相关法律规定
数据安全管理措施	《中华人民共和国网络安全法》 第二十一条，第四十条，第四十九条。 《中华人民共和国个人信息保护法》 第五十一条第一款第（一）项。
数据安全技术措施	《中华人民共和国网络安全法》 第十条，第二十一条第一款第（二）项、第（三）项， 第二十八条，第三十三条，第四十二条第二款，第五十五条。 《中华人民共和国数据安全法》 第二十七条，第二十八条。 《中华人民共和国个人信息保护法》 第五十一条第一款第（三）项。
人员管理及安全教育	《中华人民共和国网络安全法》 第二十一条第一款第（一）项， 第三十四条第一款第（一）项、第（二）项，第四十五条。 《中华人民共和国数据安全法》 第二十七条第一款。 《中华人民共和国个人信息保护法》 第五十一条第一款第（四）项。
网络安全等级保护	《中华人民共和国网络安全法》 第三十八条。
问题整改和纠正措施	《中华人民共和国网络安全法》 第五十六条。 《中华人民共和国数据安全法》 第四十四条。 《中华人民共和国个人信息保护法》 第六十四条。
数据出境安全合规	《中华人民共和国网络安全法》 第三十七条，第五十条，第六十六条。 《中华人民共和国个人信息保护法》 第三条第二款第（三）项，第三十六条，第三章（第三十八条至第四十三条），第五十三条，第五十五条。
安全合规跟踪评估	《中华人民共和国网络安全法》 第二十一条第一款第（三）项。 《中华人民共和国数据安全法》 第三十条。 《中华人民共和国个人信息保护法》 第三十六条，第三十八条第一款第（一）项，第四十条，第五十五条，第五十六条。

参 考 文 献

[1]《中华人民共和国数据安全法》实施参考（第一版） 中国网络安全产业联盟数据安全工作委员会

[2]《中华人民共和图个人信息保护法》释义 杨合庆 法律出版社

[3] 数据合规实务：尽职调查及解决方案 刘瑛，李晓华 法律出版社