ICS 33.040
M

YD

中 华 人 民 共 和 国 通 信 行 业 标 准

YD/T 0219—2019

电信网和互联网数据安全评估规范

（报批稿）

The Specification of Telecommunication Networks and Internet Data Security

××××-××-××发布　　××××-××-××实施

中华人民共和国工业和信息化部 发布

目　　录

前　　言

本标准是“电信网和互联网数据安全”系列标准之一。该系列标准预计结构及名称如下：

1、 《电信网和互联网数据安全通用要求》

2、 《电信网和互联网数据安全评估规范》（本标准）

3、 《电信网和互联网数据安全评估技术实施指南》

本标准按照GB/T 1.1-2009给出的规则起草。

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。

本标准由中国通信标准化协会提出并归口。

本标准起草单位：中国信息通信研究院、中国移动通信集团有限公司、中国联合网络通信集团有限公司、中国电信集团有限公司、数据通信科学技术研究所、北京天融信网络安全技术有限公司。

本标准主要起草人：郭建南、尚铁力、魏薇、张媛媛、庞妹、姜宇泽、张峰、江为强、孙艺、于文良、国强、王渭清、韩冬、汪志、冯程、刘晓、侯文浩、范亚辉、符加龙、王媛媛。

1 范围

本标准是电信网和互联网数据安全评估系列标准的子标准，配套YD/T 3802-2020使用，相关术语、定义、范围参照该标准。

本标准规定了电信服务和互联网信息服务提供商开展数据安全评估实施流程和数据安全相关管理及技术措施的评估要点。

本标准适用于电信网和互联网服务提供商组织开展的网络数据安全评估工作，也适用于第三方机构对电信网和互联网服务提供商数据安全保障能力进行审查和评估。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

GB/T 35273-2020 《信息安全技术 个人信息安全规范》

YD/T 3802-2020 《电信网和互联网数据安全通用要求》

YD/T XXXX-XXXX 《基础电信企业数据分类分级方法》

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本文件。

3.1.1

网络数据

通过网络收集、存储、传输、处理和产生的各种电子数据。

[中华人民共和国网络安全法，定义第七十六条第四款]

3.1.2

数据安全

通过管理和技术措施,确保数据有效保护和合规使用的状态。

[GB/T 37988—2019 定义3.1]

3.1.3

数据资产

以电子形式记录的组织机构所拥有和控制的数据。

[电信网和互联网数据安全通用要求，定义3.1.7]

3.1.4

保密性

使信息不泄漏给未授权的个人、实体、进程,或不被其利用的特性。

[GB/T 25069—2010，定义2.1.1]

3.1.5

完整性

准确和完备的特性。

[GB/T 29246—2017，定义2.40]

3.1.6

可用性

已授权实体一旦需要就可访问和使用的数据和资源的特性。

[GB/T 25069—2017，定义2.1.20]

3.1.7

合规

对数据安全所适用的法律法规的符合程度。

[GB/T 37988-2019,定义3.16]

3.1.8

数据处理

对原始数据进行抽取、转换、加载的过程。

[GB/T 37988-2019,定义3.13]

3.1.9

规程

对执行一个给定任务所采取动作历程的书面描述。

[GB/T 25069—2010，定义2.1.7]

3.1.10

个人信息

以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息。

注：关于个人信息的范围和类型依据GB/T35273-2020附录A中要求。

[GB/T 35273-2020，定义3.1]

3.1.11

个人敏感信息

一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息。

注：关于个人敏感信息的范围和类型依据GB/T35273-2020附录B中要求。

[GB/T 35273-2020，定义3.2]

3.1.12

个人信息主体

个人信息所标识或关联到的自然人。

[GB/T 35273-2020，定义3.3]

3.1.13

个人信息控制者

有能力决定个人信息处理目的、方式等的组织或个人。

[GB/T 35273-2020，定义3.4]

3.1.14

明示同意

个人信息主体通过书面、口头等方式主动作出纸质或电子形式的声明，或者自主作出肯定性动作，对其个人信息进行特定处理作出明确授权的行为。

注：肯定性动作包括个人信息主体主动勾选、主动点击“同意”、“注册”、“发送”、“拨打”、主动填写或提供等。

[GB/T 35273-2020，定义3.6]

3.1.15

收集

获得对个人信息的控制权的行为。

注1：包括由个人信息主体主动提供、通过与个人信息主体交互或记录个人信息主体行为等自动采集行为，以及通过共享、转让、搜集公开信息等间接获取个人信息等行为。

注2：如果产品或服务的提供者提供工具供个人信息主体使用，提供者不对个人信息进行访问的，则不属于本标准所称的收集行为。例如，离线导航软件在终端获取用户位置信息后，如不回传至软件提供者，则不属于个人信息收集行为。

[GB/T 35273-2020，定义3.5]

3.1.16

开放共享

电信业务经营者、互联网信息服务提供者进行全部或部分数据复制、分享等行为。

[电信网和互联网数据安全通用要求，定义3.1.9]

3.1.17

合作方

受托代理市场销售和提供业务合作、技术支撑、数据服务等可能接触到组织机构数据的外部机构。其中，业务合作主要包括数据业务合作推广、渠道接入等形式；技术支撑主要包括系统开发集成、系统维护、技术支撑等形式；数据服务主要包括数据建模、数据挖掘、数据分析等数据服务能力提供形式。

[电信网和互联网数据安全通用要求，定义3.1.10]

3.1.18

删除

在实现日常业务功能所涉及的系统中去除个人信息的行为，使其保持不可被检索、访问的状态。

[GB/T 35273-2020，定义3.10]

3.1.19

销毁

通过清除、消磁、粉碎等技术手段使电子信息载体中存储的信息不可再用，且不可恢复的过程。[TD/T 2692-2014，术语和定义2.6]

3.1.20

去标识化

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，无法识别或者关联个人信息主体的过程。

注：去标识化建立在个体基础之上，保留了个体颗粒度，采用假名、加密、哈希函数等技术手段替代对个人信息的标识。

[GB/T 35273-2020，定义3.15]

3.1.21

数据脱敏

对某些敏感信息通过一定规则进行数据的变形，实现敏感隐私数据的可靠保护。

[电信网和互联网数据安全通用要求，定义3.1.14]

3.2

缩略语

下列缩略语适用于本文件。

MAC	网络设备物理地址	Media Access Control
IP	网际互连协议	Internet Protocol
TLS/SSL	传输层安全协议	Transport Layer Security/Socket Secure Layer

4 概述

4.1 评估总体原则

4.1.1 总体框架

电信网和互联网数据安全评估主要利用文件查验、系统演示及测评验证等多种方法评估企业在各类数据处理活动及数据承载系统平台的保障措施合规情况，从通用性管理与全生命周期管理两方面出发，针对各个指标项明确评估涉及的重要管理措施、重点技术措施及判断标准，明确被评估事项合规性保障基线，以提升企业数据安全管理及相关技术保障措施能力水平，评估框架如图1所示。

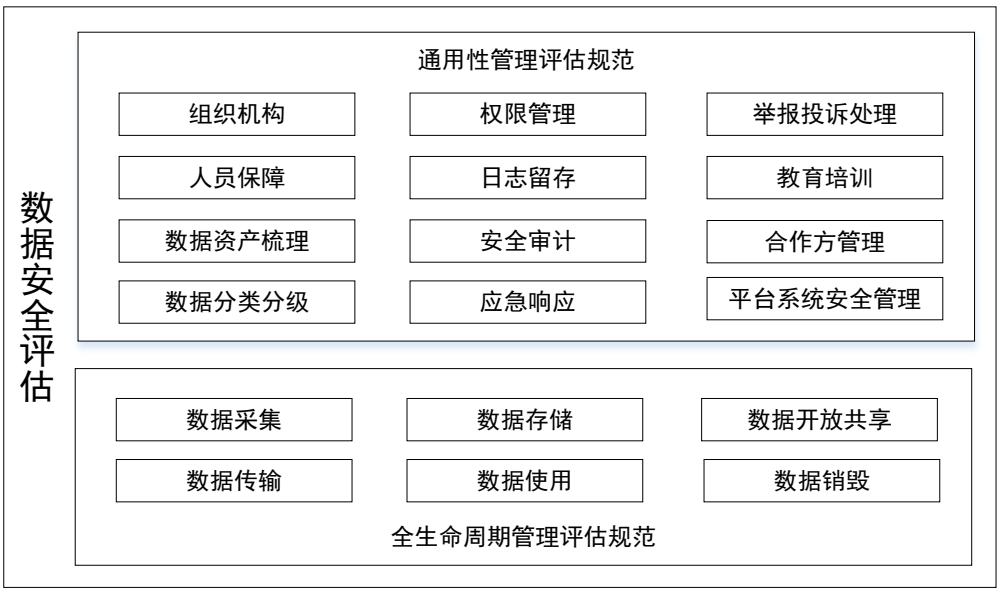

图1 总体框架

4.1.2 评估原则

标准性原则：指遵循电信网和互联网行业相关标准开展数据安全评估工作。

客观公正原则：指评估人员在评估活动中应充分收集证据，对评估对象实施的安全措施的有效性和可靠性做出客观公正的判断。

可重复和可再现原则：指在相同的环境下，对同一评估对象，不同的评估人员依照同样的要求，使用同样的方法，对每个评估实施过程的重复执行都应得到同样的评估结果。

可控性原则：在评估过程中，应保障参与评估的人员、使用的技术和工具、评估过程都是可控的。

完备性原则：严格按照被评估对象所涉及的评估范围进行全面的评估。

最小影响原则：从相关管理层面和工具技术层面，将评估工作对数据和承载数据的应用、系统、网络正常运行的可能影响降低到最低限度，不会对被评估对象涉及的应用、系统、网络运行产生显著影响。

保密原则：指评估人员开展数据安全评估工作前，需要与被评估单位就数据安全保密责任义务进行认定与划分，包括不限于保密协议签署等，应对评估中获取的相关信息、评估过程文档等严格保密，以保障被评估方的数据安全。

4.2 评估启动条件

满足下列情形之一的，应及时启动数据安全评估：

a) 业务运营阶段，在数据承载环境发生较大变化时开展评估：如数据采集渠道变更、数据存储系统升级改造、数据处理技术变更等；

b) 企业应在开展数据重要操作（如开放数据对外接口、数据共享、数据转移、数据加工、数据出境等）前对涉及到的数据相关管理措施、技术措施开展评估；

c) 行业主管部门要求企业进行数据安全评估的；

d) 满足国家法律法规有关情形时，应开展数据安全评估。

4.3 评估流程

4.3.1 评估准备阶段

a) 组建评估团队

应组建适当的数据安全评估团队，包括评估管理单位、责任单位和开发运营单位，评估人员需具备数据安全评估相关能力，以支撑整个评估过程的推进及有效开展。当被评估组织委托安全服务机构开展数据安全评估时，应与被委托单位共同组建评估团队。

b) 确定评估范围

应根据数据评估对象进行评估范围界定，确定数据涉及的生命周期阶段，以及各阶段所涉及的应用、系统、平台范围。

数据评估对象可以为具有收集、使用用户个人信息功能的业务，涉及存储用户个人信息和核心网络数据的业务支撑系统等，例如，评估范围可界定为行业热点业务、业务支撑网运营管理系统、大数据分析系统等。

c) 评估对象调研

数据安全评估团队应对被评估企业的数据安全相关工作进行充分调研，调研内容包括被评估企业数据安全管理相关制度和流程、数据安全设备部署情况等，从而为后续数据安全评估实施奠定基础。

4.3.2 评估实施阶段

评估组织实施阶段，对标数据安全基线要求，采用包括文档查验、人员访谈、系统演示、测评验证等方式对管理措施和技术措施进行评估，对不合规项逐项提出针对性整改建议。数据安全评估团队评估实践过程中，应当对评估佐证材料进行收集、整理，做好评估过程记录。

评估实践过程通常可包括数据安全初评实践、数据安全复评实践两部分：

a) 数据安全初评实践：指数据安全评估团队在完成评估准备阶段后，对评估对象的初步评估。数据安全评估团队应根据初步评估结果，结合评估对象实际情况，对评估不合规项逐项提出针对性整改建议，给出评估对象初评结论。

b) 数据安全整改复核：指数据安全评估团队在评估对象完成整改或达到整改期限后，对评估对象的整改复核评估。数据安全评估团队应根据初步评估结果及整改建议，检查评估对象整改措施有效性、合规性，确定评估对象是否完成整改，给出评估对象复评结论。

具体评估方法包括但不限于以下方法：

a） 文档查验

文档查验是指评估人员查阅数据安全相关文件资料，如企业数据安全管理制度、业务技术资料和其他相关文件，用以评估数据安全管理相关制度文件是否符合标准要求的一种方法。通常在评估准备阶段以及数据安全管理类基线评估部分使用该方法，企业需要事先完整准备上述文档以供评估人员查阅。

b） 人员访谈

人员访谈是指评估人员通过与被评估企业相关人员进行交流、讨论、询问等活动，以评估数据安全保障措施是否有效的一种方法。通常在评估过程中深入企业实地调研时使用，企业需要安排熟悉数据流转过程，以及承载数据的应用、系统、网络情况的人员参加访谈。

c） 系统演示

系统演示是指企业相关人员演示、评估人员查看承载数据的应用、系统、网络，包括数据采集界面、数据展示界面、数据存储界面、数据操作日志记录等，以评估数据安全保障措施是否有效的一种方法。通常在评估过程中深入企业现场调研时使用，企业需要安排相关人员进行现场演示，评估人员根据系统演示情况进行查验。

如系统存在高度保密性、可用性的要求，评估可通过事后提供日志列表或测试环境等方式进行。

d） 测评验证

测评验证是指评估人员通过实际测试承载数据的应用、系统、网络，查看、分析被测试响应输出结果，以评估数据安全保障措施是否有效的一种方法。通常是评估人员针对数据全生命周期涉及的相关技术指标进行验证时使用，评估人员需要事先进行业务注册、准备验证工具等以完成相关评估指标。

4.3.3 评估总结阶段

评估总结阶段包括召开专家评审会，对评估实施过程及评估意见、评估整改落实情况进行核验，确认评估企业或评估对象是否已经配套数据安全管理措施和数据安全技术措施，满足数据安全基线要求，并撰写形成评估报告。

4.4 报告规范要求

安全评估报告应当包括以下组成部分（见附录A）：

a) 概述，包括被评估企业数据安全管理情况、被评估业务或系统平台具体功能及数据安全情况；

b) 数据安全评估流程，包括评估工作情况概述、评估人员组成、评估实施流程等；

c) 数据安全评估矩阵，根据通用性管理评估规范及全生命周期管理评估规范，梳理总结出合规性评测矩阵表；针对每一项评估指标，综合运用多种评估方法，收集佐证材料；对佐证材料进行研判评估，得出数据安全保障措施合规或完善程度有关结论；

d) 问题分析，根据评估结论梳理评估指标项中不合规项，指出存在问题；

e) 整改建议，依据存在问题逐项提出有针对性整改建议；

f) 整改落实情况，如涉及整改，需体现整改方案及整改措施、结果；

g) 复核结果及签字（建议盖章）。

5 通用性管理评估规范

5.1 组织机构

依据YD/T 3802-2020第7.1节要求开展评估。

评估企业是否已设立数据安全管理责任部门，负责牵头承担企业内部数据安全管理工作，具体包括以下内容：

查验企业文件通报或数据安全管理办法，是否明确数据安全管理责任部门（新设部门或指定某个原部门均可），是否明确部门名称及负责人，相关文件是否已面向组织机构内部发文通报（如OA发文、纸质发文、公司领导办公会决议等），在企业内部进行流转传达。

查验企业文件通报或数据安全管理办法，是否明确数据安全管理责任部门职责，部门职责是否包括但不限于制定数据安全管理整体方针策略，协调建立数据安全技术保障措施，牵头做好数据安全合规性评估、安全审计管理、数据安全事件应急处置、教育培训等工作。

查验企业文件通报或数据安全管理办法，是否明确划分数据安全管理责任部门与各项工作执行落实部门分工界面，工作执行落实部门是否完整包含数据协同管理部门（信息化、客户服务、市场部门等）、数据使用部门（业务部门）、运维支撑部门（网络运维、系统集成等部门）、可能涉及的子公司等。

查验企业数据安全监督检查制度，是否明确由责任部门定期对执行部门数据安全管理制度执行落实情况和落实效果进行监督检查，是否能够通过监督检查及时发现问题并督促整改，是否将数据安全工作执行部门落实情况和效果纳入企业内部绩效考核体系。

5.2 人员保障

依据YD/T 3802-2020第7.2节要求开展评估。

评估企业是否在数据安全管理责任部门和相关部门配备数据安全管理专职人员，是否明确相关人员数据安全工作职责，负责具体承担落实数据安全管理工作。具体包括以下内容：

查验企业数据安全岗位职责说明文件或人员任命书，是否通过正式文件明确企业数据安全管理责任人，是否明确其职责范围，包括但不限于负责牵头制定数据安全管理制度，指导数据安全管理责任部门、协调各相关部门开展数据保护工作，提出数据安全保护的对策建议，监督管理制度和措施的执行落实情况等。

查验企业数据安全岗位人员名单，是否梳理各部门数据安全岗位人员配备情况，包括部门名称、姓名、联系方式和工作职责等，是否在数据安全管理责任部门至少配备一名数据安全专职人员，相关工作执行落实部门至少配备一名数据安全责任人，组织开展部门内数据安全相关工作。相关人员工作职责是否包括但不限于权限管理、安全审计、应急响应、合规性评估、数据安全事件处置和信息报送等。

查验企业数据安全岗位人员工作记录文件，验证企业数据安全管理责任部门和相关部门人员是否按照要求履职。

5.3 数据资产梳理

依据YD/T 3802-2020第7.10节要求开展评估。

评估企业是否建立数据资产梳理制度，是否明确数据资产梳理统一规范要求，是否形成数据资产清单。具体包括以下内容：

查验企业数据资产梳理相关制度文件，是否明确数据资产的安全管理目标和原则，是否明确数据资产的维护和使用责任，是否明确定期系统梳理各数据存储平台系统情况要求，是否明确数据存储系统情况梳理原则和梳理周期。

查验企业数据梳理记录，是否定期梳理各数据存储系统情况，形成平台系统清单，并留存梳理记录；是否覆盖企业系统全范围，从企业收集处理用户个人信息的核心系统扩展到各数据处理活动相关系统，全面掌握企业数据资产规模和情况；是否对企业安全域内外系统或设备接入情况进行全面区分，并留存相关文档记录备查。

注：平台系统清单可参考YD/T 3802-2020附录A中表A.1示例。

查验企业数据资产清单，是否根据规范要求，在完成组织机构平台系统梳理的基础上，针对各系统数据库中存储的数据字段进行关联指向；是否对已形成的数据资产清单进行定期更新，建议更新周期频率不超过一年。

注：数据资产清单可参考YD/T 3802-2020附录A中表A.2示例。

查验企业是否形成数据资产变更记录，对数据资产使用、留存及报废等状态进行登记，并针对已形成的数据资产清单定期更新数据资产变更记录。

5.4 数据分类分级

5.4.1 制度策略

依据YD/T 3802-2020第6.1节、6.2节开展评估。

评估企业是否按照法律法规和相关标准要求，建立企业内部数据分类分级管理制度，具体包括以下内容：

查验企业数据分类分级管理制度，是否明确数据分类分级管理数据范围、管控技术措施、数据分类分级原则、分类分级策略标准变更流程和要求等内容；验证数据分类分级管理原则、定义、方法是否能够真实反应数据本身的属性；验证数据分类分级制度适用范围、管控系统类型是否完整覆盖企业相关数据处理活动涉及的平台系统。

查验企业数据分类分级管理制度，是否按照法律法规和相关标准要求，综合考虑数据的类别属性、使用目的等，明确数据分类策略；是否在数据分类的基础上，对每一类数据类型，结合数据重要及敏感程度、安全保护需求以及一旦泄露、丢失、破坏造成的危害程度等，制定数据分级标准，明确各级数据界限，包括具体类别、子类、范围、对应的数据举例。

注：分类分级方法可参照行业内分级分类标准。

5.4.2 数据标识

依据YD/T 3802-2020第6.3节、6.4节要求开展评估。

评估企业是否形成数据分类分级清单，是否对数据进行分类分级标识（如通过对数据字段或数据库表单打标签等形式），具体包括以下内容：

查验企业数据分类分级清单，是否依据数据分类分级制度策略，结合数据分类分级管控系统对象，完成各数库表字段映射，梳理形成包含数据类别、数据定位、数据范围、对应系统数据等内容的数据分类分级清单，并根据数据分类分级变更情况进行动态更新并留存更新记录。

演示企业业务和业务支撑系统，验证是否根据分类分级制度策略，实现数据资产的分类分级标识（如通过对数据字段或数据库表单打标签等形式）。

注：企业可通过数据的安全分类分级标识工具，基于组织机构的数据资产安全分类分级策略，对数据进行自动的分类分级标识，实现数据标识结果的发布和审核等。

5.4.3 差异化措施

依据YD/T 3802-2020第6.5节要求开展评估。

查验企业数据分类分级管理制度，是否充分考虑业务或系统平台场景需求，在数据采集、传输、存储、使用、共享、销毁等数据全生命周期各个环节中针对不同类别级别的数据明确相应的安全保障措施，包括不限于数据加密、数据脱敏、数据变更、数据销毁、操作权限管理、数据流动记录、人员操作日志记录、数据备份与恢复等技术能力和措施。

5.4.4 策略变更

依据YD/T 3802-2020第6.6节开展评估。

查验企业数据分类分级管理制度，是否明确关于数据分类分级策略制定、变更的流程规范，细化关于策略修订、发布、实施等具体管理要求，并对策略变更情况进行记录。

5.5 权限管理

依据YD/T 3802-2020第7.4节开展评估。

查验企业数据访问权限管理制度，是否明确数据处理活动平台系统账号权限分配、开通、使用、销毁等安全保障原则和审批流程要求；是否明确数据处理账号操作的审批要求和操作流程；是否建立并定期更新企业数据处理活动平台系统权限分配表，是否对能够处理用户个人信息的业务系统账号进行定期梳理，并对岗位角色的权限进行规范。

通过技术验证企业数据处理活动平台系统账号权限分配是否遵循“权限明确、职责分离、知其所需、最小特权”的原则，每个账号是否按照角色或用户组进行授权，是否严格控制超级管理员权限账号数量。

通过演示企业账号生命周期管理流程，验证针对开发运维人员、第三方人员在创建和注销系统账号时，是否严格遵循系统账号创建和注销申请审批流程，并记录审批过程和结果。

a) 通过技术验证企业业务支撑系统是否通过基于IP或MAC地址、账号口令等的方式对所有接入数据处理活动平台系统的用户或业务进行身份认证和权限控制；

b) 通过技术验证企业业务支撑系统是否配置口令复杂度策略，如：口令长度不少于8位，使用大写字母、小写字母、数字及特殊字符中至少三种的组合，且与用户名、字符顺序无相关性；

c) 通过技术验证企业业务支撑系统是否配置账号锁定策略，对系统账号口令输入尝试次数进行限制；

d) 通过技术验证企业业务支撑系统是否对口令遗忘的申请和重置流程实施严格管理，口令重置流程是否存在业务逻辑设计缺陷，是否留存申请和重置记录；

e) 演示企业业务支撑系统是否采取掩码显示、加密传输、加密存储等方式保护账号口令安全；加密密钥保护工作按照5.12.5条进行合规性评估。

注1：若采用哈希加盐的方式进行口令保护，盐值也需安全存储。

注2：加密密钥是指一种用于控制密码变换操作（例如加密、解密、密码校验函数计算、签名生成或签名验证）的符号序列。

[GB/T 25069-2010,定义2.2.2.106]

5.6 日志留存

依据YD/T 3802-2020第7.5节开展评估。

查验企业日志留存相关制度文件，是否明确日志留存要求，包括日志记录范围、记录规范、留存时间以及日志记录访问权限控制等内容，重点关注但不限于数据授权访问、批量复制、开放共享、销毁及数据接口调用等环节日志。

a) 查验企业业务人员操作日志记录信息是否包括执行时间、操作账号、处理方式、授权情况、登录信息等；

b) 查验企业网络运行状态、网络安全事件相关的日志记录保存时间是否满足国家相关法律法规要求，不少于6个月；是否定期对网络日志进行备份，防止数据安全事件导致的日志被删除；

查验企业是否配备日志审计人员，且审计权限与系统管理权限、策略管理权限分立设置；是否对日志操作人员操作进行权限控制，避免非法删除、修改和覆盖。

5.7 安全审计

依据YD/T 3802-2020第7.6节要求开展评估。

评估企业是否制定了数据安全审计制度，是否针对数据全生命周期各阶段（数据采集、数据传输、数据存储、数据使用、数据开放共享、数据销毁）开展安全审计，实现对数据访问和操作的有效监控和审计，防控数据全生命周期各阶段中可能存在的未授权访问、数据滥用、数据泄漏等安全风险，具体包括以下内容：

查验企业数据安全审计制度，是否明确数据安全审计工作牵头部门和相关执行部门；是否明确审计目的、审计对象、审计内容（如明确异常操作的定义）、审计操作规程、审计频度、审计结果规范、审计问题整改跟踪等内容；企业是否定期开展安全审计和整改工作，及时消除安全隐患。

查验企业数据安全审计制度，核查审计对象是否完整覆盖企业相关数据处理活动涉及的平台系统。

查验企业数据安全审计制度，核查数据安全审计的内容是否包括企业内部权限控制（如数据非授权访问）、企业内部数据流向跟踪情况（如批量复制、转移）、数据安全保障措施有效性等，是否能够发现和处置数据非授权访问、批量导出等异常情况。

a) 演示企业是否已建设安全审计平台，并将审计对象全量接入安全审计平台；

b) 演示企业是否为审计人员开通审计平台审计账号，负责对数据全生命周期各阶段的数据访问和操作进行安全监控；

c) 演示企业审计平台，验证是否根据数据安全审计内容和企业账号权限管理机制，定义异常操作的范围，配置相应的审计策略（模型）；

查验企业数据安全审计制度，是否要求至少以季度为单位滚动开展数据安全审计，记录并形成数据安全审计报告。

a) 查验数据安全审计报告是否完整记载安全审计发现的问题，是否在一年内实现数据处理活动涉及的平台系统安全审计工作全覆盖。审计数据记录内容是否至少包括：操作时间、操作主体、操作类型、操作对象、操作结果；

b) 查验企业数据安全审计报告，验证企业数据安全管理责任部门是否针对有关问题协调数据安全相关执行部门提出改进方案，并要求落实解决；是否对审计问题进行跟踪审核，并留存异常情况处置记录。

5.8 应急响应

依据YD/T 3802-2020第7.7节要求开展评估。

评估企业是否制定数据安全事件应急响应制度，明确数据安全事件应急响应牵头部门及相关执行部门的工作职责、数据安全事件发现及报告机制、安全事件等级及相关应急措施、溯源及处置流程、事件总结等要求，具体包括以下内容：

查验企业数据安全事件应急响应制度，是否明确应急响应目的、依据、范围、原则、事件分级和分类、组织结构及职责、预防和预警机制、应急处置、应急响应保障措施、应急预案的宣贯、培训、演练和维护等内容；数据安全事件等级是否按照《工业和信息化部关于印发<公共互联网网络安全突发事件应急预案>的通知》（工信部网安〔2017〕281号）、GB/T 20986-2007等文件要求，以及数据安全事件对国家安全、经济发展和社会公共利益、企业和个人信息主体合法权益影响程度、数据安全事件的影响范围及持续时间等因素进行划分。

查验企业数据安全事件应急响应方案，是否有效结合了数据安全事件场景和等级划分，是否包括但不限于数据泄露（丢失）、数据滥用、数据被篡改、数据被损毁、数据违规使用等特定场景，是否明确应急响应工作责任分工、实施环节、需配套的应急响应措施，实施环节是否包括事件监测、定位、分级、启动、响应处置、报告、事件评估、结束响应、应急总结、情况跟踪等阶段。

查验企业数据安全应急演练工作记录，验证企业业务是否根据数据安全事件应急响应预案，制定演练计划并定期组织演练，保存演练记录。每类数据安全事件场景是否至少一年开展一次演练。每个核心数据处理活动涉及的平台系统是否至少两年开展一次演练。

查验企业数据安全应急响应处置记录，是否在发生数据安全事件时及时按照应急预案实施应急措施，包括监测预警（预警分级、事件监测、信息报告、预警发布）、应急响应（先期处置、响应、信息发布、应急处置结束）、恢复重建（恢复生产、安全加固、事件总结）。是否视情况将事件情况、应急措施以及可能造成的影响等向电信主管部门报告。当发生的数据安全事件涉及个人信息时，企业是否按照GB/T35273-2020中第10章要求采取以下处置措施：

a) 及时将事件相关情况以邮件、信函、电话、推送通知等方式告知受影响的个人信息主体。难以逐一告知个人信息主体时，采取合理、有效的方式发布与公众有关的警示信息；

b) 企业告知内容包括但不限于：安全事件的内容和影响、已采取或将要采取的处置措施、个人信息主体自主防范或降低风险的建议、针对个人信息主体提供的补救措施、个人信息保护负责人及个人信息保护工作机构的联系方式。

5.9 举报投诉处理

依据YD/T 3802-2020第7.8节要求开展评估。

查验企业举报投诉处理制度，是否按照法律法规和相关标准要求，建立数据安全举报投诉处理制度，明确举报投诉处理的部门和人员、数据安全举报投诉类型和相关处理流程、要求等。

演示企业业务是否面向用户提供数据安全举报投诉渠道和有效的联系方式，至少采用以下一种：电子邮件、电话、传真、在线客服、在线表格等；是否能够受理与用户个人信息保

护相关的举报投诉，例如用户个人信息违规采集、使用、共享等。若通过官方网站设置投诉举报信息提交窗口，是否可提交投诉举报人、问题、建议等内容。

查验企业业务数据安全举报投诉处理记录，是否遵循数据安全投诉处理制度，针对有效举报线索依法依规组织开展处置和记录工作，并自接到投诉之日起十五日内答复投诉人。

5.10 教育培训

依据YD/T 3802-2020第7.9节要求开展评估。

查验企业数据安全教育培训制度，是否按照法律法规和相关标准要求，建立数据安全教育培训机制，明确培训周期、培训人员、培训内容、培训考核等内容。

查验企业数据安全教育培训记录（如培训计划、培训通知、培训议程、培训课件、签到表等相关记录文件），是否每年至少开展一次数据安全管理培训工作。

查验企业数据安全教育培训签到表，企业数据安全教育培训人员是否覆盖企业数据安全岗位人员名单，包括企业数据安全责任人、数据安全管理责任部门全体人员、相关部门配合落实数据安全管理工作人员等，详见YD/T 3802-2020第7.2.2节。

查验企业培训计划，是否针对数据安全管理相关岗位制定相应培训计划，并对培训计划定期审核和更新。

查验企业数据安全教育培训课件，企业数据安全培训内容是否完整覆盖数据安全制度要求和实操规范等内容，包含但不限于数据安全与用户个人信息保护相关法律法规、标准制度、管理方法、合规性评估、技术防护、应急演练和相关知识技能。

查验企业数据安全教育培训考核记录，企业数据安全教育培训结束后是否就培训内容对培训人员进行考核，对培训效果进行评定、记录和归档。

5.11 合作方管理

依据YD/T 3802-2020第14章要求开展评估。

5.11.1 管理制度

查验企业合作方数据安全管理制度，是否明确合作方数据安全管理的监督管理部门和执行配合部门，是否明确针对不同合作类型的数据安全保护方式和责任落实要求。

查验企业合作方数据安全管理制度，是否要求各部门按照“谁运营、谁负责”原则，建立合作方管理清单机制，明确清单梳理周期，全面梳理并定期更新各部门涉及的合作方清单。

查验企业合作方清单，是否包含合作方企业名称、合作业务或系统、合作形式、合作期限、合作方联系人等信息。

查验企业合作方数据安全管理监督检查制度，企业合作方数据安全管理的监督管理部门是否履行监督管理职责，建立合作方数据安全管理监督检查机制，明确合作方数据安全管理要求。

查验企业合作方数据安全管理监督检查制度，检查是否明确合作方资质审核、服务合同、接入管理、权限管理、主体授权、多个合作方管理、安全技术、数据脱敏、行为监测、数据销毁等安全管理要求。

查验企业合作方数据安全管理监督检查制度，是否明确检查周期，定期组织开展针对合作方数据安全管理责任落实情况的监督检查工作，对发现的问题及时督促整改，留存监督检查结果及问题整改情况记录。

5.11.2 资质审核

查验企业合作方资质审核记录文件，企业需求部门是否在业务合作开展前，对合作方的信用情况、是否发生过数据安全事件等进行调研，是否对合作方数据安全保护能力进行合规性评估，确保其具备相应的保密及运营资质。

查验企业合作方评估报告和服务合同，企业在业务合作涉及个人信息时，是否对合作方个人信息保护工作进行合规性评估，是否在评估通过后签订服务合同。

查验企业合作方评估报告，企业业务在合作期限内，需求部门是否定期组织企业相关业务部门对合作方进行动态合规性评估，及时发现存在的安全风险，并督促整改。

5.11.3 服务合同

查验企业与合作方是否签订服务合同、安全保密协议和数据安全协议，并依据 YD/T 3802-2020 第 14.6 节明确相关内容。

5.11.4 接入管理

评估企业是否建立合作方接入管理机制，明确合作方系统接入备案、终端接入控制、定期巡查、接口安全管理要求，开展合作方接入管理工作，具体包括以下内容：

查验企业合作方数据安全管理制度，是否建立合作方系统接入备案管理要求和流程，在合作方系统需接入本企业系统时，是否由需求部门发起到组织机构数据安全管理责任部门申请备案，留存备案记录。

演示企业合作方接入管理系统，验证是否在合作方终端接入本企业内部网络时，进行严格接入认证，配置安全控制策略。是否限制对网口和无线上网的使用，并统一要求安装防病毒软件，及时更新防病毒软件病毒库，确保防病毒软件有效运行。在发现U盘等外设拷贝设备时是否能及时进行告警。

5.11.5 权限管理

查验企业合作方数据安全管理制度，是否建立合作方账号管理机制，明确合作方账号管理要求，对合作方账号实行严格管理，具体包括以下内容：

a) 是否明确禁止合作方人员掌握系统管理员权限，禁止为合作方人员分配具备创建系统账号或者其他超出工作范围权限的高权限账号；
b) 特殊情况下，合作方人员若需要获得系统管理员权限或涉敏权限，是否进行临时授权并严格监控，留存授权审批记录，工作完成后及时收回权限；
c) 是否建立合作方账号审核制度，明确审核责任部门、审核范围、审核内容、审核周期等内容，按照制度要求定期对全量合作方账号进行严格审核，控制涉敏人员的范围；
d) 是否制定合作方账号管理办法，明确并严格落实对合作方账号申请、回收、授权、有效期等环节的管理要求，是否在合作方人员转岗或离岗前，要求合作方公司提交合作方人员转岗或离岗申请书，由企业主管部门根据相关规定完成合作方人员的账号回收、审核、网络调整等工作，并签署转岗或离岗审批意见后，方可转岗或离岗。

查验企业合作方数据安全管理制度，是否制定并实施严格的物理安全管理制度，严格按照物理安全管理制度进行区域划分，包括但不限于：

a） 是否严格控制落实数据核心安全区进入审批流程；

b） 是否严格控制落实第三方人员进行数据核心安全区的审批流程。

5.11.6 主体授权

查验企业合作方数据安全管理制度，是否明确个人信息主体授权要求，在个人信息主体授权同意的范围内，与合作方开展委托处理等合作，并与合作方签订服务合同，明确合作方数据使用目的、范围，严禁合作方超出合同约定目的和范围使用分析个人信息。

5.11.7 多个合作方管理

查验企业合作方数据安全管理制度，是否明确针对同一业务涉及多个合作方的管理要求。

查验企业合作方数据安全管理制度，是否明确限制每个合作方只获得其工作所需的数据资源。

查验企业合作方数据安全管理制度，是否在与合作方签订的服务合同中明确“未经数据发送方同意，合作方之间不得进行数据交换”。

5.11.8 安全技术

查验企业合作方数据安全管理制度，是否建立定期巡查制度，明确巡查范围、方式和频率等要求；是否针对合作涉及服务器、数据库等系统平台至少每月开展一次巡查工作，巡查方式应包括但不限于与漏洞扫描、基线检查和代码审计等，并对发现的问题及时督促整改，强化合作方数据防篡改、防泄漏以及数据脱敏、数据审计等安全技术措施，留存漏洞扫描、基线检查和代码审计结果和问题整改报告。

查验企业合作方数据安全管理制度，是否明确要求对合作方接口可查询的时限和范围进行严格审核，严禁合作方自行确定查询范围。是否在合作方系统退出服务时，及时关闭相应接口。

5.11.9 数据脱敏

查验企业合作方数据安全管理制度，是否按照法律法规和相关标准要求，建立合作人员使用数据脱敏机制，通过技术验证是否根据实际情况，对合作方人员使用的数据进行脱敏处理，合作方使用的数据是否能直接反映个人信息。

详情可参考第6.4.3节。

5.11.10 行为监测

评估企业是否按照法律法规和相关标准要求，开展合作方行为监测工作，具体包括以下内容：

查验企业合作方数据安全管理制度，是否建立业务合作方安全风险监督管理制度，对合作方数据使用用途进行审计、行为约束和监督管理；是否制定业务合作方数据用途报备机制，明确报备周期，要求合作方定期上报数据使用用途情况，留存相应的工作记录。在机房内合作方操作时，是否要求自有员工在场监督，是否禁止对机房内设备进行接口直连等。

查验企业合作方数据安全管理制度，是否建立合作方考核制度、制定考核细则、明确考核内容、考核周期、考核要求及惩处措施，并依据考核制度要求，对合作方开展考核工作；是否定期检查合作方在数据使用、管理等方面的安全制度和执行情况，对检查过程中发现的问题责成其在规定时限内整改。

查验企业合作方数据安全管理制度，是否建立合作方信用档案，记录合作方数据泄露、滥用等违规行为；是否建立合作方黑名单机制，将存在数据泄露、数据滥用等违规行为的企业纳入黑名单，是否将数据转移共享给存在数据泄露、数据滥用等违规行为的企业。

5.11.11 数据销毁

查验企业合作方数据安全管理制度，是否按照法律法规和相关标准要求，建立合作方数据删除制度，明确合作方数据删除的管理要求，在与合作方签订的服务合同中，明确数据使用期限，并在业务合作结束后，采取有效措施督促合作方按照合同约定及时删除企业提供的原始数据。数据销毁由本企业内部工作人员现场进行有效监督，确保数据删除不可恢复，并留存数据删除记录。脱敏后的数据不在必须删除的范围之内。

详情可参考第6.6节。

5.12 平台系统安全管理

5.12.1 管理制度

查验企业数据处理活动相关平台系统安全管理制度和操作规范，是否按照YD/T 3802-2020第15.1条内容，明确系统软件版本控制、补丁测试和更新、资源管理，以及恶意代码防范、入侵检测管理等安全配置策略要求。

5.12.2 三同步

查验企业是否按照YD/T 3802-2020第15.2条内容，按照工信部关于“三同步”要求，在数据处理活动相关平台系统的设计、建设和运行过程中，做到安全的同步规划、同步建设、同步运行。

5.12.3 接口安全

查验企业是否按照YD/T 3802-2020第15.3-15.4条内容，针对对外数据接口，制定业务平台接口开发规范和协议。

查验业务平台接口技术实现方式是否符合规范和协议内容(含公有和私有协议)，是否对协议与接口进行安全测试。

5.12.4 安全防护

查验企业是否按照YD/T 3802-2020第15.5条内容，定期进行系统级和代码级的安全漏洞扫描，并对发现的安全漏洞进行及时进行安全加固。

演示企业是否按照YD/T 3802-2020第15.6条内容，建立业务平台系统集中漏洞管理功能，实现业务平台系统漏洞和补丁集中式管理，支持业务平台系统漏洞查询、筛选功能，支持补丁获取、分发和回退功能，并留存相关管理记录。

演示企业是否按照YD/T 3802-2020第15.7条内容，部署防恶意代码策略，屏蔽危险病毒端口，部署防病毒工具，定期进行平台恶意代码检测和病毒库升级，并对恶意代码监测、病毒库升级留存记录。

查验企业是否按照YD/T 3802-2020第15.8条内容，依据业务安全需求和信任关系规划业务控制边界、应用隔离相关的安全域和安全防护边界，制定边界安全控制策略和管理规则，如身份鉴别、连接管理、网络访问控制、入侵防范等，涉及用户数据的系统是否位于核心安全域。

查验企业是否按照YD/T 3802-2020第15.9条内容，制定边界安全防护设施更新管理规则，是否采用必要手段或管控措施确保规则的实施。

5.12.5 密钥管理

查验企业是否按照YD/T 3802-2020第15.10条内容，在使用密码技术时，制定密码密钥配用和管理要求，对密钥的生成、分发、验证、更新、存储、备份、有效期、销毁进行管理，对密钥的使用实施权限管理、存储隔离和安全审计。是否对密码算法的配用进行规范，并采用公认安全的、标准化公开的加密算法。

查验企业是否按照YD/T 3802-2020第15.11条内容，在使用密码技术作为脱敏的手段时，规范数据的加密和脱敏过程，并保证密钥、相关参数的安全性。

5.12.6 处理安全

演示企业是否按照YD/T 3802-2020第15.12条内容，在系统的数据处理层提供相应的鉴权机制，是否只有合法的用户或应用程序才能发起数据处理请求。

演示企业是否按照YD/T 3802-2020第15.13条内容，使系统的数据处理层支持对敏感数据的识别、过滤、屏蔽、隐藏，使管理员能够灵活控制返回给用户的敏感信息，从而达到敏感数据保护的目的。

演示企业是否按照YD/T 3802-2020第15.14条内容，通过统一的入口控制点对访问数据平台的所有应用提供统一认证，对所有上层应用的访问进行细粒度授权，防止越权访问。

演示企业是否按照YD/T 3802-2020第15.15条内容，使系统支持对某些敏感信息通过脱敏规则进行数据的变形，实现敏感数据的可靠保护，实现在不泄露用户个人信息的前提下保障业务系统的正常运行。

查验企业是否按照YD/T 3802-2020第15.16条内容，针对执行的逻辑代码进行严格的代码安全审查，避免代码执行非期望操作造成用户隐私信息泄漏。

5.12.7 异常检测

演示企业是否按照YD/T 3802-2020第15.17条内容，对系统中防火墙、入侵检测系统等防护手段的工作状态进行监测。

演示企业是否按照YD/T 3802-2020第15.18条内容，配套应用异常行为分析、发现及告警功能，便于及时发现数据平台中可能存在的风险点及攻击行为，强化应用安全管控，保证数据安全。是否能够对应用的以下异常行为进行监测并告警：

a） 应用的非授权访问行为监测与告警（如不具有敏感数据访问权限的应用请求访问敏感数据）。

b） 非合规参数数据访问行为监测与告警。

c） 应用访问执行流异常行为监测与告警。

d） 数据平台流量异常的应用访问行为监测与告警。

6 全生命周期管理评估规范

6.1 数据采集

依据YD/T 3802-2020第8章要求开展评估。

6.1.1 采集规则

查验企业具体业务用户协议或隐私政策文件中业务功能及收集的个人信息，是否明确数据采集的目的、用途和范围，规范数据采集的流程和方法。

查验企业数据采集相关制度文件是否明确数据采集渠道、数据格式、采集流程和采集方式；针对外部数据源，是否明确要求外部数据提供方说明数据来源，并对信息来源的合法性进行确认，确保数据采集渠道的合法性和正当性。

查看隐私政策并注册使用该业务，验证是否按照国内法律法规相关要求，明示采集个人信息的目的、方式和范围，未经被采集者同意，不得采集与其提供的服务无关的个人信息。

查验企业数据采集相关制度文件，是否建立数据采集的风险评估流程，针对采集的数据源、采集频度、采集渠道、采集方式、数据范围和类型进行风险评估；涉及采集个人信息的业务场景是否进一步依据相应的合规要求进行合规风险的评估，并防范采集过程中可能存在的数据泄漏风险。

通过技术验证企业业务是否明确数据采集过程中个人信息的知悉范围和安全控制措施，确保采集过程中的个人信息不被泄露。

查验数据采集合规报告，是否根据规则在业务系统中定期执行数据采集合规性查验。

6.1.2 用户数据采集

查验企业具体业务用户协议或隐私政策文件中业务功能及收集的个人信息，在发生用户信息采集时，企业是否按照公开透明原则，将采集规则以通俗易懂、简单明了的文字向用户明示，并满足YD/T 3802-2020第8.5节相关要求。

查验企业业务用户协议或隐私政策所述的业务功能及收集的个人信息，验证其是否存在单独以改善服务质量、提升用户体验、定向推送信息、研发新产品等为由，以默认授权、功能捆绑等形式强迫、误导用户数据主体同意采集用户数据的行为。

企业如果通过在线方式进行用户个人敏感信息采集，通过技术验证业务是否使用有效加密手段保障用户在线提交信息的安全性。

6.1.3 停止采集

通过隐私政策或用户协议检查企业业务是否按照法律法规和相关标准要求，在停止运营产品或服务、用户终止服务等情况时，停止对用户数据的采集。

通过技术验证企业业务是否为用户提供注销号码或账号的服务，并且在用户注销账号时不得设置过多不合理的注销条件（如需要提交非必要的个人敏感信息）。

6.1.4 其他已明确要求

企业是否遵守GB/T35273-2020第5章的要求。

6.2 数据传输

依据YD/T 3802-2020第9章要求开展评估。

6.2.1 场景划分

查验企业数据传输相关制度文件，是否根据法律法规、业务需求、业务系统可用性、建设成本等要求，明确需要传输加密的业务场景，明确关键网络设施的冗余部署，明确网络安全域划分策略；数据传输安全策略制定是否充分考虑了各数据存储平台系统网络规划设计、部署、维护管理和运营中的安全风险。

查验企业数据传输相关制度文件，是否在数据分类分级定义的基础上，明确提出相匹配的数据加密传输要求，相关要求中是否包含对数据加密算法要求和密钥的管理要求。

通过技术验证企业是否在安全边界配备数据访问控制措施;查验企业是否建立相应审批流程，对跨组织机构或使用互联网的数据传输事项进行前置审批。

6.2.2 加密传输

通过技术验证企业业务和业务支撑系统是否针对第6.2.1节规定需要数据加密传输要求的业务场景部署相应的加密措施（如采用TLS/SSL方式）。

演示企业业务系统是否提供对数据传输安全策略变更进行审核和监控的能力,是否部署对通道安全配置、密码算法配置、密钥管理等保护措施进行审核及监控的能力。

6.2.3 传输接口

评估企业是否建立数据传输接口管理规范和技术保障措施，具体包括以下内容：

查验企业数据接口管理规范文件，是否建立数据传输接口安全管理工作规范，明确技术管控措施；是否具备系统间接口的设备鉴权和认证能力，通过MAC地址、IP地址或端口号绑定等方式避免违规设备接入，实施数据流程控制、关键操作日志管理，包括接口名称、接口参数、接口安全要求等内容。

a) 查验是否定期对传输接口管理和技术管控措施部署情况进行梳理,形成接口梳理情况清单并定期更新，更新频率应不超过一年；

b) 查验企业传输接口梳理情况清单，是否包括：存在数据传输接口的业务系统、对端单位、对端系统、实现方式、接口类型（如：实时调用接口、文件传输接口等）、对外接口传输数据种类以及目前使用的安全防护措施（如：访问控制、加密、数据脱敏、日志审计等）；

c) 查验企业接口监控处置记录,是否对照接口梳理情况清单及时监控发现低活跃接口或废置接口，并采取相关处理措施；

d) 查验企业传输接口梳理情况清单,是否对涉及个人信息传输的接口进行识别和梳理,通过技术验证企业业务和业务支撑系统是否对接口调用实施控制，包括流控制、流量监控、调用过载保护等措施。

查验企业数据接口管理规范文件，是否严格控制数据传输接口的新增需求。是否根据“安全三同步”要求，对于数据新增、改造接口在规划、设计、建设、运行、改造和维护过程中增加安全评审机制，定期对接口权限控制、传输等相关功能进行安全评估，配备相应传输接口管理和技术管控措施。

演示企业业务和业务支撑系统是否对接口调用行为进行日志记录。

6.2.4 跨境传输

企业存在数据传输出境时，是否按照国家网信部门、国务院等有关部门制定的办法和相关规定要求进行落实。

6.3 数据存储

依据YD/T 3802-2020第10章要求开展评估。

6.3.1 存储规范

查验企业数据存储环节相关制度文件，企业是否结合数据分类分级策略和管理要求明确数据存储安全策略和操作规程，包括数据存储系统差异化的安全存储保护手段（如加密、访问控制、数字水印、数字签名等）、数据存储介质安全策略和管理规定等。

查验企业是否与数据存储系统管理和运维人员签订保密协议，是否在保密协议中明确数据使用范围、操作权限、违约责任等，有效约束相关人员行为，如对企业各类数据进行违规操作。

6.3.2 存储系统部署

查验企业数据存储环节相关制度文件，企业是否制定各类数据存储系统的安全配置规则，明确对存储系统账号权限管理、访问控制、日志管理、加密管理、版本升级等方面的安全要求。

查验企业数据存储环节相关制度文件，是否制定数据存储设备安全管理规范和操作规程，如维护操作流程、应急操作流程等。

通过技术验证企业数据存储系统及数据处理、传输设备是否部署在安全域内，是否限制直接提供公共互联网访问；查验其上线前是否经过安全验收以保证遵循统一的安全配置；对使用的外部数据存储系统是否进行有效的安全配置。

6.3.3 访问控制

通过技术验证企业数据存储系统，是否按照数据访问权限管理制度，配备对用户或业务（应用程序）的访问控制措施，避免非授权访问。

演示企业业务涉及敏感数据存储系统的重大操作（如对数据的批量复制、传输、处理、开放共享和销毁等），是否纳入多人管控模式（如金库模式等）。

6.3.4 存储介质

查验企业数据存储介质安全管理制度，是否明确数据存储介质的获取（购买）、使用、维护、升级、标记和销毁等流程和审批记录要求，是否明确数据存储介质获取渠道、格式化规程、资产标识规程等要求。

查验企业数据存储介质安全管理制度，是否明确数据处理相关平台系统接入移动存储介质的流程规范和管控措施，包括数据存储介质登记、审批、接入等。

演示业务系统是否配套针对将数据下载到本地终端的行为进行审核和日志记录的能力，是否配套对向移动介质输出数据的情况进行二次审核和日志记录的能力。

查验企业数据存储介质安全管理记录，是否配备存储介质使用管理的岗位和人员执行落实企业数据存储介质安全管理要求，相关执行操作是否符合流程规范。

6.3.5 备份恢复

企业是否建立数据存储冗余策略和管理制度，内容覆盖数据服务可靠性、可用性等数据安全保护目标。

查验企业备份恢复相关管理制度，企业是否包括数据备份的规范和操作规程，是否明确规定数据备份的周期、备份方式、备份地点规范，需要对数据恢复性验证机制进行明确说明。

查验企业备份恢复相关管理制度，是否包括数据复制、备份与恢复定期检查等工作程序，工作程序说明是否包括但不限于：数据副本的更新频率、保存期限等。

6.3.6 个人信息存储

演示企业业务用户个人信息存储数据库，通过比对业务用户协议或隐私政策文件，核验企业存储的个人信息是否超出采集使用规则中明确的存储期限；是否对超出保存期限的个人信息进行删除处理。

演示企业业务用户账号注销后的个人信息存储状态，核验企业在不违反法律法规或者国家有关部门留存要求的前提下，用户注销账号后是否及时删除其个人信息或做匿名化处理，经过处理无法关联到特定个人且不能复原的除外。

有关个人信息存储的时间最小化、去标识化处理和个人敏感信息存储，是否参照GB/T35273-2020第6章及企业分级分类要求落实。

6.4 数据使用

依据YD/T 3802-2020第11章要求开展评估。

6.4.1 使用规范

查验企业整体的数据权限管理制度，是否符合网络安全法等国家相关法律法规对数据使用和分析处理的目的和范围的要求，具体包括数据使用审批流程、数据脱敏处理使用规则、数据使用结果发布和使用的安全保护规则，以及相关流程中人员岗位职责。

6.4.2 访问控制

查验企业访问控制相关制度文件，是否明确数据处理活动相关平台系统的访问控制措施（制度和流程建设等），从账号身份管理原则、身份凭证保护、最小授权原则、数据权限默认设置和权限申请和审批等方面提出数据使用安全管控要求，为内部人员分配完成职责所需的最小数据使用权限。

通过技术验证企业业务和业务支撑系统，是否对数据安全管理人员、数据使用人员、安全审计人员的角色进行分离设置；涉及授权特定人员超权限处理数据的，是否由数据安全管理责任部门或数据安全责任人进行审批并记录。

通过技术验证企业业务和业务支撑系统，是否及时清除数据处理活动相关平台系统中无用账号、默认账号，杜绝多人共用同一系统账号的情况。

6.4.3 数据脱敏

查验企业数据脱敏处理管理规范和制度文件，是否明确数据脱敏处理使用应用场景，明确数据脱敏规则、脱敏方法、数据脱敏处理流程、涉及部门及人员的职责分工等。

查验企业数据脱敏处理管理规范和制度，企业业务和业务支撑系统在数据权限和资源的申请阶段，是否由该数据的数据安全管理负责人员评估使用真实数据的必要性，以及确定该场景下适用的数据脱敏规则及方法。

查验数据脱敏处理管理规范和制度，是否建立数据脱敏处理技术应用安全评估机制，对脱敏后的数据可恢复性进行安全评估，是否对于可恢复形成原始数据的脱敏方法（含算法）进行安全加强。演示企业业务测试系统数据库，企业是否使用未脱敏的数据用于业务系统的开发测试。

演示企业数据脱敏工具，是否能对数据脱敏处理过程相应的操作进行记录，提供数据脱敏处理安全审计能力。

6.4.4 数据分析

查验企业数据使用管理制度，企业是否明确了数据使用安全策略和操作规程。查验企业业务支撑系统是否提供停止定向推送信息的功能，用户选择停止接收定向推送信息时，是否停止推送信息，并为用户提供删除或匿名化定向推送所基于用户数据的必要选项。查验企业分析利用所掌握的数据资源，发布市场预测、统计信息、用户信用等信息，是否遵循国家相关法律法规要求，是否存在发布虚假信息、损害他人合法权益等情况。

查验企业数据使用管理制度，是否明确大数据分析结果输出和使用的安全检查、合规风险评估和授权流程，避免分析结果输出中包含可恢复的个人信息、重要数据等数据和结构标识，从而防止个人信息、重要数据等敏感信息的泄漏。

查验企业数据使用相关日志记录，是否对数据使用操作进行记录，以备对分析结果质量和可信性进行数据溯源。

演示企业业务和业务支撑系统，是否具备信息化技术手段或机制，对违规使用数据的行为进行有效的识别、监控和预警。

6.4.5 个人信息使用

演示企业个人信息使用相关平台，核验除为达到用户授权同意的使用目的所必需外，企业处理个人信息时是否消除明确身份指向性，避免精确定位到特定个人。特殊情况下（如：信用体系评价、被监护人行踪轨迹、执法部门协助等），是否告知用户应用场景及可能对用户产生的影响。

演示企业个人信息使用相关系统平台，核验企业在开发测试、统计分析、投诉处理、精确营销、外呼、催欠等活动过程中，对使用相关系统平台所展示的个人信息是否进行去标识化处理。

查验企业业务获取用户同意记录，核验企业因业务需要，确需改变个人信息使用目的或改变个人信息使用规则时，是否再次征得用户明示同意；是否针对目的变更后的情况，进行个人信息安全风险评估，重新调整安全措施。

注：改变年满14的未成年人的个人信息使用目的或规则时，应征得未成年人或其监护人的明示同意；不满14周岁的，应征得其监护人的明示同意。

企业是否向用户提供多种参与对其信息处理的方法，包括访问、更正、删除、撤回同意、注销账户、获取自身信息等。

有关个人信息的处理安全保护措施，是否遵守GB/T35273-2020第7章的要求。

6.5 数据开放共享

依据YD/T 3802-2020第12章要求开展评估。

6.5.1 开放共享规范

查验企业数据开放共享相关制度文件，是否区分数据开放共享场景，对应不同的数据开放共享场景建立相应的数据开放共享安全策略和操作规程，明确数据开放共享范围、内容与有效控制机制。

查验企业数据开放共享相关业务系统的审批记录，是否建立数据开放共享的审核制度和规范的数据共享审核流程，审核开放共享数据的数据内容，确认属于满足数据开放共享业务场景的需求范围及未超出授权范围开放共享数据。

查验企业数据开放共享相关业务系统的审计记录，是否落实数据开放共享安全审计制度，审计结果至少留存6个月备查。

查验企业保密协议或合作合同，是否通过保密协议等方式明确数据开放共享双方应承担的安全责任，应具备的数据保护手段、限制数据使用范围和场景等。

6.5.2 开放共享溯源

通过技术验证企业数据共享相关业务系统，是否具备数据开放共享场景下的数据溯源方法（如对数据进行签名、添加数字水印等），防止数据被恶意删除、随意篡改和滥用。对于包含个人敏感信息的数据，是否能够及时跟踪、记录数据流向、数据接收者信息、处理操作等信息，保障出现数据安全问题时，能够分析问题根因，追查数据出现问题的环节和责任人。

6.5.3 开放共享接口

查验企业接口规范相关制度文件，是否针对涉及个人信息的应用开放接口进行有效管理，是否记录接口的访问参数，如账号、内容等信息，并进行必要的关联分析，防止数据滥用、数据窃取等行为。

查验企业与数据开放共享接口调用方签署的合作协议，是否在合作协议中明确了对数据的使用目的、供应方式、保密约定等。

查验企业数据接口管理制度及数据接口清查记录，是否定期对本企业对外数据接口进行清查，是否对不符合要求的对外数据接口立刻予以关停。

6.5.4 个人信息开放共享

查验企业开放共享个人信息情况记录，比对业务用户协议或隐私政策文件，核验企业在经法律授权或具备合理事由确需开放共享时，是否违背采集阶段告知的使用目的，或超出告知的使用范围开放共享。

通过系统演示，企业是否提供合理有效的措施帮助个人信息主体了解数据接收方对个人信息的保存、使用等情况，并保障个人信息主体的权利，例如，查询、访问、更正、删除、注销账户、撤回已同意的授权等。

有关个人信息的开放共享安全保护措施，是否遵守GB/T35273-2020第9章的要求。

6.5.5 接收者要求

查验企业针对数据开放共享接收者的安全管理记录，是否在其他组织机构开放共享用户数据时，对数据接收者资质能力进行审核、评估，确保数据接收者满足合作方管理要求，是否采取相应安全保障措施保障用户数据在开放共享过程中的安全，是否通过合同明确用户数据接收者对用户数据的安全保密责任。

6.5.6 脱敏要求

演示企业业务，是否在用户端（如网站、APP、账单、业务登记单、显示屏幕等展示场景）显示个人敏感信息时，采取去标识化处理等措施防止个人信息主体之外的其他人员未经授权获取个人敏感信息。个人信息主体身份验证通过或者主动选择后，可完整查看个人敏感信息。

6.6 数据销毁

依据YD/T 3802-2020第13章要求开展评估。

6.6.1 销毁制度

查验企业数据销毁相关制度文件，是否结合数据分类分级管理制度和安全需求，建立数据销毁安全策略和操作规程，明确销毁对象、原因（如数据业务下线、用户退出服务、节点失效、过多备份、数据试用结束、超出数据保存期限等）和流程、存储介质销毁处理策略和操作规程。

查验企业数据销毁相关制度文件，是否建立数据销毁审批机制，设置销毁相关监督角色，监督操作过程；查验企业数据销毁记录文件，是否留存审批记录，留存时间是否满足6个月。

演示企业业务和业务支撑系统是否针对数据销毁建立完善的操作审批机制，采用多人操作模式，限制单人拥有完整操作权限。

6.6.2 销毁处置

演示企业数据销毁工具，是否建立有效的数据销毁方法和技术，是否依据数据介质存储内容的重要性，明确各类存储介质（闪存、移动硬盘、固态硬盘、硬盘、磁带、光盘等）的销毁方法和机制，是否对不同作用的存储介质，提供不同的销毁措施，实现数据的硬销毁和软销毁，确保数据及其副本内容以不可逆方式销毁，如针对用户注销服务、存储介质维护需要带出机房等场景可采用多遍覆盖、删除密钥、执行固件擦除命令等安全数据删除方式，针对介质报废等场景，可采取高压击穿、消磁、粉碎等物理损毁手段。

查验企业数据销毁工作记录，是否验证数据销毁效果，保证数据销毁后系统内的文件、目录和数据库记录等资源所在的存储空间被释放或重新分配前得到完全清除，不可恢复；是否对销毁后所涉及的资源进行回收，包括账号、物理资源、云资源、系统存储空间、数据共享途径等，并进行登记记录。

查验企业数据销毁管理制度，是否制定数据存储介质销毁监管措施，是否设置销毁相关监督角色，监控销毁介质登记、审批、交接等介质销毁过程，并对销毁过程进行记录，形成数据销毁报告。

6.6.3 销毁情形

查验企业数据相关制度文件、业务用户协议或隐私政策文件，是否在制度中明确并通过业务用户协议或隐私政策文件与用户进行约定：“若出现兼并、重组、破产等情形，要求数据承接方承接数据安全责任和义务。没有数据承接方的，将对数据作销毁处理。法律、行政法规另有规定的，从其规定”。

6.6.4 个人信息销毁

有关个人信息的销毁安全保护措施，是否遵守GB/T35273-2020第8.3至8.5条内容。

附　录 A

（参考性附录）

数据安全评估报告模板

（封面）

（企业简称）数据安全评估报告

业务名称：XXXX

（企业名称）

年　　月

1 业务/平台/企业数据安全基本情况

1.1 业务/平台名称

……

1.2 业务功能介绍

……

1.3 企业数据安全管理情况介绍

……

2 数据安全评估流程

2.1 评估人员组成

……

2.2 评估实施流程

……

3 数据安全评估矩阵

……

4 存在问题分析

……

5 整改建议

……

6 整改落实情况

……

7 复核结果及签字

7.1 复核结果

7.2 评估结果签字确认表（需盖章）

……

附 录 B

（参考性附录）

数据安全评估指标项

评估项	评估指标	评估要点
组织机构	机构职责	明确数据安全管理牵头部门
		明确部门职责分工
	人员保障	数据安全岗位职责
		数据安全人员配备
制度建设	资产梳理	数据资产梳理制度
		数据梳理记录
		数据资产清单
		数据资产变更记录
	分类分级	数据分类分级策略和标准
		数据分类分级管理标识
		差异化技术保障措施
	权限管理	数据访问权限管理要求
		数据处理活动平台系统账号管理
		数据处理活动平台系统权限管控
		业务支撑系统访问控制
	日志留存	重点环节日志留存管理
		日志记录完整、准确、可查
		日志记录时间要求
		日志操作权限控制
	安全审计	数据安全审计制度
		数据安全审计规范
		数据安全审计平台
		数据安全审计报告
	应急响应	数据安全事件应急响应制度
		数据安全事件应急预案
		数据安全事件应急演练
		数据安全事件处置
	举报投诉处理	数据安全投诉处理制度
		公开举报投诉渠道
		举报投诉处理记录
	教育培训	数据安全教育培训制度
		数据安全教育培训周期
		数据安全教育培训人员
		数据安全教育培训计划
		数据安全教育培训内容

		数据安全教育培训考核
	合作方管理	合作方数据安全管理制度
		合作方安全风险监督管理
		合作方数据安全保护责任约束
		合作方系统接入管理
		合作方人员账号管理
		合作方物理环境管理
	平台系统安全管理	安全制度规范
		三同步
		接口安全管理
		系统安全防护
		密钥管理
		处理安全
		异常检测
全生命周期管理	数据采集	数据采集合法正当
		用户数据采集明示同意
		停止采集
	数据传输	数据传输安全管理
		数据加密传输
		传输接口安全管理
		跨境传输安全评估
	数据存储	数据存储安全管理
		数据存储系统安全部署
		数据存储系统访问控制
		数据存储介质管理
		数据备份与恢复
		用户个人信息存储
	数据使用	数据使用安全规范
		数据访问控制
		数据脱敏处理
		数据分析安全
		个人信息正当使用
	数据共享	数据共享规范管理及审批
		数据开放共享溯源
		开放共享接口管理
		接收者资质审核
		个人敏感信息去标识化
		个人信息开放共享安全保护
	数据销毁	数据销毁管理要求
		数据销毁场景及手段
		数据销毁责任及用户权益保护