ICS 35.020
L 70/84

团　体　标　准

T/CITIF 003—2023

信息技术服务 数据安全能力模型

Data security capability model during information technology service

2023-01-13 发布　　2023-01-13 实施

中国电子信息行业联合会　发布

目　　次

前　言

本标准按照 GB/T 1.1-2020 给出的规则起草。

请注意本文件的其他内容可能涉及专利，本文件的发布机构不承担识别这些专利的责任。

本标准由中国电子信息行业联合会提出并归口。

本标准主要起草单位：广州赛宝认证中心服务有限公司、国网河北省电力有限公司信息通信分公司、国网内蒙古东部电力有限公司数字化事业部、贵州省大数据应用推广中心、云上贵州大数据产业发展有限公司、东软集团股份有限公司、北京安华金和科技有限公司、北京网御星云信息技术有限公司、北京启明星辰信息安全技术有限公司、北森云计算有限公司、浙江省义乌市数据管理中心、浙江省数据安全服务有限公司、浙江海莱云智科技有限公司、北京四方远望企业管理有限公司、中科锐眼(天津)科技有限公司、福建中信网安信息科技有限公司、贵州银行股份有限公司、贵州省电子认证科技有限公司、贵州领航视讯信息技术有限公司、贵州中软云上数据技术服务有限公司、贵州多彩宝互联网服务有限公司、贵州省邮电规划设计院有限公司、贵州省通信产业服务有限公司。

本标准主要起草人：李尧、陈艳、段沛鑫、胡友杰、王云辉、霍之刚、张涛、张宏伟、韩朱旸、贺敏、赵振文、李筑、侯婷婷、杨超、李博、李鹏飞、王红华、周廷珽、葛诗春、王仕品、邹蓉、张元猛、薄凯凯、陈龙、王丽、张帮军、李昕、郭鹏程、蒋纳成、李孟、何松林、袁青霞、史正伟、金华松、高翔、冯瑞廷、胡蕾、姚冬、张吉权、李婷、罗林尧、王俊、史正伟、田野、郑如顺、陈超、李飞、蔡荣、李岚、周承熙、赵杭。

引　言

数字时代，数据已成为重要生产要素及国家基础性战略资源，我国也在持续推进并加强数据安全治理工作。2021年，全国人大常委会第二十九次会议通过了我国首部数据保护领域专项法律《中华人民共和国数据安全法》，以国家法律的形式对我国数据安全保护工作提出要求，并明确说明我国促进并支持数据安全检测评估、认证等服务发展和活动开展。大数据、5G、人工智能、物联网等新技术在各个行业应用的同时，数据安全风险的危害性和外溢性已对政治、科技、经济和社会等多个领域产生了负面影响。在当前数据安全发展的形势下，标准的实施将给信息技术服务行业提供有力帮助。

为科学有效地评价信息技术服务提供者的数据安全能力水平，指导信息技术服务提供者数据安全能力，数据安全能力模型标准应运而生。本标准提出了信息技术服务过程中信息技术服务提供者数据安全的能力要求。

本标准典型的应用场景包括：

1）信息技术服务提供者利用本标准建设自身数据安全能力，并进行评估和改进；

2）信息技术服务需求者利用本标准对信息技术服务提供者数据安全能力进行评估；

3）第三方机构依据本标准对信息技术服务提供者的数据安全能力进行客观评估。

信息技术服务 数据安全能力模型

1 范围

本文件提出了信息技术服务提供方在服务过程中保障数据安全的能力成熟度模型框架，定义了信息技术服务提供方在服务安全保障能力、数据处理安全能力、服务安全交付能力等方面的成熟度等级要求。

本标准适用于：

1）信息技术服务提供者利用本标准建设自身数据安全能力，并进行评估和改进；

2）信息技术服务需求者利用本标准对信息技术服务提供者数据安全能力进行评估；

3）第三方机构依据本标准对信息技术服务提供者的数据安全能力进行客观评估。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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 37988-2019《 信息安全技术 数据安全能力成熟度模型》

GB/T 41479-2022《信息安全技术 网络数据处理安全要求》

GB/T 25069-2022《信息安全技术 术语》

3 术语和定义

3.1

信息技术 information technology；IT

信息通信技术 information and communication technology；ICT

为采集、表示、处理、传输、交换、描述、管理、组织、存储、检索、输出数字信息而开发、维护和使用的技术。

[来源：GB/T 25069-2022，3.692]

3.2

数据 data

指任何以电子或者其他方式对信息的记录。

[来源：GB/T 41479—2022,3.1]

3.3

数据安全 data security

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。

[来源：GB／T 37988-2019，3.1]

3.4

数据安全能力 data security capability

组织在组织建设、制度流程、技术工具以及人员能力等方面对数据的安全保障。

[来源：GB／T 37988-2019，3.5]

3.5

能力成熟度 capability maturity

对一个组织有条理的持续改进能力以及实现特定过程的连续性、可持续性、有效性和可信度的水平。

[来源：GB／T 37988-2019，3.6]

3.6

能力成熟度模型 capability maturity model

对一个组织的能力成熟度进行度量的模型，包括一系列代表能力和进展的特征、属性、指示或者模式。

注：能力成熟度模型为组织衡量其当前的实践、流程、方法的能力水平提供参考基准，并设置明确的提升目标。

[来源：GB／T 37988-2019，3.7]

3.7

数据处理 data processing

数据的收集、存储、使用、加工、传输、提供、公开等。

[来源：GB/T41479—2022 3.3]

3.8

合规 compliance

对数据安全所适用的法律法规的符合程度。

[来源：GB／T 37988-2019，3.16]

4 信息技术服务数据安全能力模型架构

4.1 能力维度域

信息技术服务数据安全能力模型标准共分为3个能力域：服务安全保障能力、数据处理安全能力、服务安全交付能力。

4.2 能力等级

信息技术服务数据安全能力模型能力等级分为“初始级”、“发展级”、“稳健级”、“优秀级”、“卓越级”5个等级，等级依次递增。

表1 能力等级

信息技术服务数据安全能力等级	共性特征	说明

等级1：初始级	组织未在任何业务中建立成熟稳定的信息技术服务数据安全管理机制,仅根据临时需求或基于个人经验对信息技术服务数据安全进行管理。	随机、无序、被动地执行安全过程，依赖于个人经验，无法复制。
等级2：发展级	组织对实施信息技术服务有基本的数据安全意识，在关键业务中初步建立了信息技术服务数据安全管理机制。	基本建成框架性的信息技术服务数据安全管理过程，有相关的制度，但没有形成体系化。
等级3：稳健级	组织对实施信息技术服务有较高的数据安全意识，信息技术服务的数据安全全面覆盖业务和相关部门；组织对标准过程进行制度化，为组织定义标准化的文档。	相关制度较为完整，已基本形成体系化；在组织级别实现了安全过程的规范执行。
等级4：优秀级	组织的信息技术服务数据安全能力发展战略和目标清晰，形成了完善的 能力管理体系；并为组织的数据安全建能力建立了可测量目标，以量化测量作为修正行动的基础。	相关制度完善，已完全体系化；建立了量化目标，相关过程可度量。
等级5：卓越级	组织基于业务综合发展的需要，实施基于量化提升的信息技术服务数据安全能力体系；改进组织能力，改进过程有效性；持续优化管理机制，以保证符合组织发展战略的实际需要。	根据组织的整体目标，不断改进和优化相关过程；实施基于量化提升的信息技术服务数据安全能力体系，并形成了推动业务变革的机制；在行业内分享最佳实践，成为行业标杆。

4.3 指标体系框架

信息技术服务数据安全能力成熟度模型指标体系包含3个一级指标，15个二级指标，如下图所示：

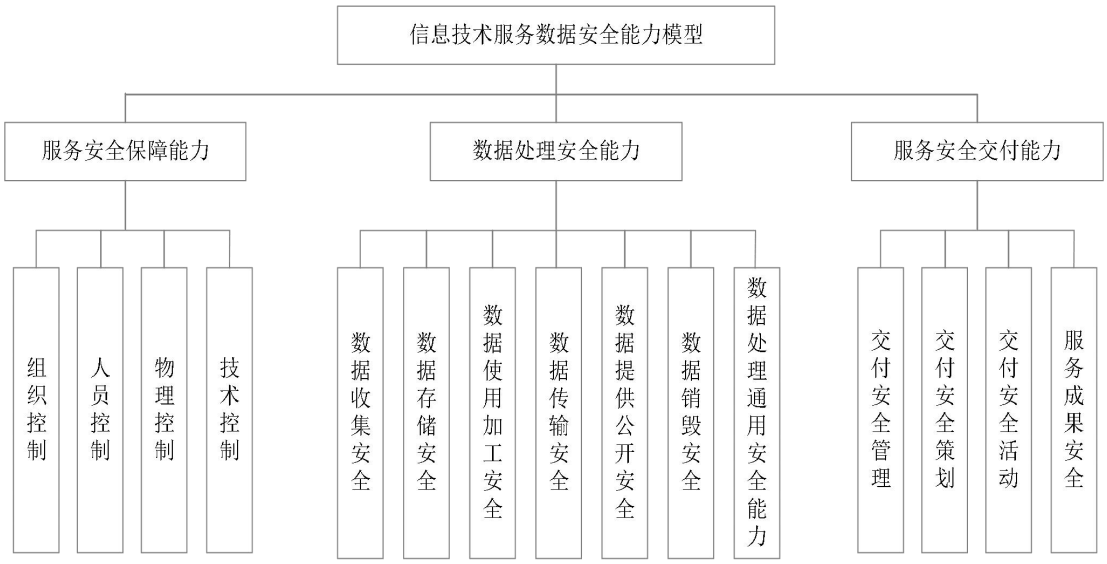

图1 信息技术服务数据安全能力成熟度模型指标体系框架

5 服务安全保障能力

信息技术服务提供方应从组织控制、人员控制、物理控制和技术控制四个方面提升组织的安全保障能力。

5.1 组织控制

5.1.1 等级 1：初始级

该等级的信息技术服务数据安全能力要求描述如下:

未在任何业务建立成熟稳定的组织安全管理机制,仅根据临时需求或基于个人经验对信息安全进行管理。

5.1.2 等级 2：发展级

除达到 1 级要求外，该等级的信息技术服务数据安全能力要求描述如下:

a） 管理制度：应基于信息安全需求，应建立日常管理活动中常用的安全管理制度，包括数据安全管理制度；

b） 岗位设置：应设立系统管理员等岗位，并定义各个岗位的工作职责。

5.1.3 等级 3：稳健级

除达到 2 级要求外，该等级的信息技术服务数据安全能力要求描述如下:

a） 管理制度：应基于信息安全需求，建立较完善的信息安全制度，包括物理、网络、主机系统、数据、应用、建设和运维等管理内容；

b） 岗位设置：应设立系统管理员、审计管理员和安全管理员等，岗位设置合理，职责明确；

c） 信息安全策略：应制定组织信息安全策略和目标，并建立数据安全目标，指导组织信息安全管理；

d） 风险评估：开展风险评估工作，其中包括数据安全风险评估，有针对性的落实信息安全要求，实现安全风险的有效控制；

e） 资产管理：应建立资产管理制度，识别组织资产并定义相应的保护责任；

f） 信息安全事件：应建立信息安全事件管理制度，对信息安全事件进行报告、响应和处置；

g） 信息分级：信息应按照法律要求、价值、重要性及其对未授权泄露或修改的敏感性进行分级管理；

h） 访问控制：应基于业务和信息安全要求，建立访问控制策略，识别用户身份，控制用户访问权限；

i） 供应商管理：应建立供应商管理制度，评估供应商服务过程中的风险，签到相应的安全协议，并对供应商进行监控和评审；

j） 合规管理：应建立合规管理制度，避免违反与信息安全相关的法律、法规、规章或合同义务。

k） 云服务信息安全：应根据组织的信息安全要求建立获取、使用、管理和退出云服务的流程；（可裁剪项）。

5.1.4 等级 4：优秀级

a） 除达到3级要求外，该等级的信息技术服务数据安全能力要求描述如下:

b） 体系建设：建立完善的信息安全管理体系，持续改进，并通过第三方认证；

c） 项目中的信息安全：信息安全应纳入项目管理，确保与项目和可交付成果相关的信息安全风险（包括数据安全风险）在整个项目生命周期的项目管理中得到有效解决；

d） 业务连续性管理：应根据业务连续性目标和连续性要求，规划、实施、维护和测试信息系统的准备情况。

5.1.5 等级 5：卓越级

除达到 4 级要求外，该等级的信息技术服务数据安全能力要求描述如下:

a） 量化管理：每个管理过程应建立量化的信息安全指标，定期测量，不断优化控制措施；

b） 流程工具化：将安全管理流程工具化，优化管理流程，提高管理效率。

5.2 人员控制

5.2.1 等级 1：初始级

该等级的信息技术服务数据安全能力要求描述如下:

未在任何业务建立成熟稳定的人员安全管理措施，仅根据临时需求或基于个人经验对人员安全进行管理。

5.2.2 等级 2：发展级

除达到 1 级要求外，该等级的信息技术服务数据安全能力要求描述如下:

a） 背景调查：在加入组织之前，应对拟入职人员进行背景核查，考虑到适用的法律、法规和道德规范；

b） 安全教育和培训：组织人员和相关利益方应接受适当的信息安全意识、教育和培训。

5.2.3 等级 3：稳健级

除达到 2 级要求外，该等级的信息技术服务数据安全能力要求描述如下:

a） 背景调查：在加入组织之前，对关键岗位进行深度的背景核查，并与业务要求、要访问的信息分级和感知的风险成比例；

b） 安全教育和培训：组织人员和相关利益方应接受相应的信息安全意识、教育和培训，以满足岗位的安全要求；并定期更新与其工作职能相关的组织信息安全方针、专题策略和程序；

c） 保密协议：员工和其他相关方应确定、记录、定期审查和签署反映组织信息保护需求的保密或不泄露协议；

d） 违规处理：应正式制定并传达纪律程序，以对违反信息安全政策的人员和其他相关方采取行动；

e） 离职管理：信息安全责任和义务在雇佣关系终止或变更后仍然有效，应予以定义、执行，并传达给相关人员和其他相关方。

5.2.4 等级 4：优秀级

除达到 3 级要求外，该等级的信息技术服务数据安全能力要求描述如下:

a） 相关方人员管理：对相关方人员（包括外包方、合作伙伴等）进行相应的安全管理，包括背景调查、安全教育和培训、退出管理等；

b） 远程工作：当远程工作的人员（包括员工或其他相关方人员）在组织场所外访问、处理或存储信息时，应采取安全保护措施。

5.2.5 等级 5：卓越级

除达到 4 级要求外，该等级的信息技术服务数据安全能力要求描述如下:

a） 安全考核：应根据岗位职责，对每个岗位人员进行安全考核，以不断提升人员的信息安全意识和能力。

5.3 物理控制

5.3.1 等级 1：初始级

该等级的信息技术服务数据安全能力要求描述如下:

未在任何业务建立成熟稳定的物理安全控制措施，仅根据临时需求或基于个人经验对物理安全进行管理。

5.3.2 等级 2：发展级

除达到 1 级要求外，该等级的信息技术服务数据安全能力要求描述如下:

a） 物理环境：应建立物理环境管理措施，对组织信息和设施进行防护，防止丢失、未授权的物理访问、损坏和干扰；

b） 机房建设：根据信息安全需求，应建立机房，安置和保护重要的基础设施和计算机设备。（可裁剪项）

5.3.3 等级 3：稳健级

除达到 2 级要求外，该等级的信息技术服务数据安全能力要求描述如下:

a） 机房建设：应根据业务安全需求建立符合要求的机房，在消防、温湿度、防盗、防水、电力供应等方面满足安全要求。

b） 介质管理：应建立介质管理措施，对介质的使用、标记和处置进行管理；

c） 设备维护和处置：应建立设备维护流程，评估设备变更和维护的风险，应审批维修和服务，监督维修过程。

5.3.4 等级 4：优秀级

除达到 3 级要求外，该等级的信息技术服务数据安全能力要求描述如下:

a） 设备维护和处置：含有存储介质的设备带出工作环境时其中重要数据应加密；含有存储介质的设备在报废或重用前，应进行完全清除或被安全覆盖。

5.3.5 等级 5：卓越级

除达到 4 级要求外，该等级的信息技术服务数据安全能力要求描述如下:

a） 技术工具：应具备技术工具，有效的监控物理环境、机房、基础设施和设备。

5.4 技术控制

5.4.1 等级 1：初始级

该等级的信息技术服务数据安全能力要求描述如下:

未在任何业务建立成熟稳定的技术控制措施，仅根据临时需求或基于个人经验对信息处理设施进行管理。

5.4.2 等级 2：发展级

除达到 1 级要求外，该等级的信息技术服务数据安全能力要求描述如下:

a） 终端安全：应建立基本的终端管理措施，保护终端设备的安全；

b） 系统操作安全：应建立基本的系统操作安全措施，包括权限管理、容量管理和恶意代码防护等；

c） 网络安全：建立网络设备和设施的管理措施，以保障网络的安全和可用性。

5.4.3 等级 3：稳健级

除达到 2 级要求外，该等级的信息技术服务数据安全能力要求描述如下:

a） 终端安全：应采用身份鉴别、恶意代码防护和审计等手段，保障重要终端设备的安全，保护存储在用户终端设备上、由用户终端设备处理或通过用户终端设备访问的信息；

b） 系统操作安全：应对系统进行脆弱性管理、日志管理、数据备份、数据防泄漏管理等；

c） 网络安全：根据信息安全需求，对网络进行区域化管理，并保障各类网络（公共网络、第三方网络或无线网络）传输的数据的机密性和完整性；

d） 密码技术：应定义并实施有效使用加密的规则，包括密钥管理；

e） 安全开发：应制定开发过程中的安全措施，保障信息安全在信息系统开发生命周期中得到设计和实现。

5.4.4 等级 4：优秀级

除达到 3 级要求外，该等级的信息技术服务数据安全能力要求描述如下:

a） 冗余：应根据业务服务和信息系统可用性的要求，应设计和实施具有适当冗余的系统架构，以满足这些要求。

5.4.5 等级 5：卓越级

除达到 4 级要求外，该等级的信息技术服务数据安全能力要求描述如下:

a） 集中管控：对设备进行集中监测；对审计数据进行汇总和集中分析；对安全策略、恶意代码、补丁升级等进行集中管理；对各类安全事件进行识别、报警和分析。

6 数据处理安全能力

6.1 数据收集安全

6.1.1 等级 1：初始级

该等级的信息技术服务数据安全能力，未建立可持续的数据收集安全管理流程，仅根据临时需求或基于个人经验对个别数据收集进行安全合规管理。

6.1.2 等级 2：发展级

该等级的信息技术服务数据安全能力应满足以下要求：

a） 应有相关岗位负责数据收集安全管理；

b） 应明确服务的数据采集原则，保证数据采集的合法、正当；

c） 应明示个人信息采集的目的、方式和范围，并经被收集者同意；

d） 应具备保证数据收集过程安全性的技术能力；

e） 应具备对数据源进行鉴别和记录的技术能力。

6.1.3 等级 3：稳健级

除达到二级要求外，该等级的信息技术服务数据安全能力应满足以下要求：

a） 应设立数据采集安全管理的岗位，该岗位人员应能够充分理解数据收集的合规要求、安全要求和业务要求，并能够根据要求提出针对性的解决方案；

b） 应建立并执行数据收集管理流程，明确数据采集的原则、流程和方法，建立风险评估和合规管理机制，确保数据尤其是重要数据、个人信息等敏感数据的合规性、正当性；

c） 应明确数据源管理流程，对数据源进行鉴别和记录，确保数据源的合规性；

d） 应具备按照数据收集管理要求建立相应技术措施的能力，例如数据校验、合规校验、数据源鉴别和记录等技术，保证数据收集过程的合规性、正当性、一致性；
e） 应具备技术能力实现数据收集、数据源鉴别的日志记录功能，并确保日志记录的完整性；
f） 应具备保证数据收集过程中重要数据、个人信息等敏感数据不被泄漏的技术能力。

6.1.4 等级 4：优秀级

除达到三级要求外，该等级的信息技术服务数据安全能力应满足以下要求：
a） 数据收集应明确范围、数量和频度，明确数据收集过程中个人信息和重要数据的知悉范围；
b） 风险评估应针对收集的数据范围、类型、数据源、频度、渠道、方式进行评估；
c） 应定期评估数据收集安全管理的效果，如数据收集安全管理在服务的覆盖率、制度流程执行效果、数据收集合规率等；
d） 应建立并执行数据追溯管理流程，明确数据源类型和标记方式，明确追溯策略、追溯数据格式、追溯数据安全存储与使用的管理制度等；
e） 应定期开展法律法规合规性审核工作，包括数据收集和数据追溯的审核，并依据审核结果增强或改进与数据服务相关的访问控制与合规性保障机制和策略；
f） 应具备跟踪和记录数据收集和获取过程的技术能力，支持对数据收集和获取操作过程的可追溯；
g） 应具备对所收集的数据和数据源进行统一校验的技术能力；
h） 应具备标记数据源类型的技术能力，实现对服务过程中各类数据源的统计和分析；
i） 应具备对关键追溯数据进行备份恢复和安全保护的技术能力。

6.1.5 等级 5：卓越级

除达到四级要求外，该等级的信息技术服务数据安全能力，应跟踪评审数据采集安全管理运行效果，根据法律法规、行业要求和服务需求的更新，持续优化数据收集、鉴别、记录和追溯等方面的管理流程和技术能力。

6.2 数据存储安全

6.2.1 等级 1：初始级

该等级的信息技术服务数据安全能力，未建立可持续的数据存储安全管理流程，仅根据临时需求或基于个人经验处理了数据存储安全需求。

6.2.2 等级 2：发展级

该等级的信息技术服务数据安全能力应满足以下要求：
a） 应有相关岗位负责数据存储安全管理；
b） 应明确物理存储和逻辑存储的管理要求并按要求执行；
c） 应具备对物理存储和逻辑存储进行身份认证、访问控制的技术能力；
d） 应具备对物理存储和逻辑存储进行监控和预警的技术能力；
e） 应具备对数据进行备份和恢复的技术能力。

6.2.3 等级 3：稳健级

除达到二级要求外，该等级的信息技术服务数据安全能力应满足以下要求：
a） 应设立负责物理存储、逻辑存储、数据备份管理的岗位，相关岗位人员应熟悉不同数据存储技术的差异，能够充分理解数据存储的合规要求、安全要求和业务要求，并能够根据要求提出针对性的解决方案。

b）应建立并执行物理存储和逻辑存储安全管理流程，明确购买获取、资产标识、格式化、安全配置、身份认证、访问控制、使用审批、数据隔离、加密管理、版本管理、监控预警、日志记录和检查审计等管理要求；

c）应建立并执行数据备份与恢复管理流程，明确备份恢复策略、操作规程以及定期检查和更新工作流程；

d）应建立并执行数据生存周期各阶段数据归档的操作流程，明确归档数据的访问控制、压缩、加密等安全措施；

e）应基于合规要求明确数据备份的有效期，明确过期数据的处理流程和安全管控措施，对超出有效期的存储数据应具备再次获取数据控制者授权的能力；

f）应具备对物理存储和逻辑存储进行安全配置扫描的技术能力，定期开展安全扫描和检测，确保数据存储符合不断变化的安全配置要求；

g）应具备对物理存储和逻辑存储的身份认证、访问控制和操作行为进行记录和审计的技术能力，确保数据存储符合相关安全要求；

h）应具备监控物理存储和逻辑存储的使用记录、性能指标、错误或损坏情况的技术能力，对超过安全阈值的风险进行预警；

i）应具备按照数据的分类分级要求提供相应加密存储的技术能力；

j）应具备建立数据备份和恢复技术工具的能力，以保证相关工作的自动执行；

k）针对备份和归档数据，应具备上述技术能力保证其安全，并具备定期检查其完整性和可用性的技术能力。

6.2.4 等级 4：优秀级

除达到三级要求外，该等级的信息技术服务数据安全能力应满足以下要求：

a）应明确分层的逻辑存储授权管理规则和授权操作要求，具备对数据逻辑存储结构的分层和分级保护能力；

b）应明确数据分片和分布式存储安全规则，如数据存储完整性规则、多副本一致性管理规则、存储转移安全规则，以满足分布式存储下分片数据完整性、一致性和保密性保护要求；

c）应明确数据冗余强一致性、弱一致性等控制要求，以满足不同一致性水平需求的数据副本多样性和多变性存储管理要求；

d）应对数据备份的场景、数量、频率进行定期的统计，了解数据备份工作的开展情况；

e）应具备建立物理存储管理系统的技术能力，确保存储媒体的标识、使用和传送过程得到严密管理；

f）应具备建立数据存储安全配置管理工具的能力，实现安全配置的统一管理和控制；

g）应具备建立可伸缩数据存储架构的技术能力，以满足数据量持续增长、数据分类分级存储等需求；

h）应具备根据数据分类分级要求实行相应加密存储策略的技术能力；

i）应具备满足应用层、数据层、操作系统层、数据存储层等不同层次数据存储加密需求的技术能力；

j）备份和归档数据的安全技术措施包括但不限于对备份和归档数据的访问控制、压缩或加密管理、完整性和可用性管理，确保对备份和归档数据的安全性、存储空间的有效利用、安全存储和安全访问；

k）应具备过期存储数据及其备份数据彻底删除或匿名化的技术方法和机制，能够验证数据已被完全删除、无法恢复或无法识别到个人，并告知数据控制者和数据使用者；

l）应通过风险提示和技术手段避免非过期数据的误删除，确保在一定时间窗口内的误删除数据可以手动恢复；

m） 数据存储架构应具备跨机柜或跨机房容错部署能力；
n） 应具备数据时效性自动检测能力，包括但不限于告警、自动删除和拒绝访问等，以保证数据的及时删除、更新和有效性。

6.2.5 等级 5：卓越级

除达到四级要求外，该等级的信息技术服务数据安全能力应满足以下要求：
a） 应建立在线/离线的多级数据归档方式，支持海量数据的有效归档、恢复和使用；
b） 应具备数据副本或数据备份存储的多种压缩策略和实现技术，确保压缩数据副本或数据备份的完整性和可用性；
c） 应为不同时效性的数据建立分层的数据存储方法，应具备按时效性自动迁移数据分层存储的能力；
d） 应具备数据时效性自动检测能力，包括但不限于告警、自动删除和拒绝访问等，以保证数据的及时删除、更新和有效性；
e） 存储系统应具备数据存储跨地域的容灾能力；
f） 应跟踪评审数据存储安全管理运行效果，根据法律法规、行业要求和服务需求的更新，持续优化物理存储、逻辑存储、数据备份恢复等方面的管理流程和技术能力。

6.3 数据使用加工安全

6.3.1 等级 1：初始级

该等级的信息技术服务数据安全能力，未建立可持续的数据使用加工安全管理流程，仅根据个人经验和常识、法律法规或合同协议、临时需求等对数据使用加工进行安全管理。

6.3.2 等级 2：发展级

该等级的信息技术服务数据安全能力应满足以下要求：
a） 应有相关岗位负责数据使用加工安全管理；
b） 应明确数据使用加工的安全要求、合规要求和合同要求，并按要求执行；
c） 应具备数据脱敏等技术能力防范数据使用、加工等数据处理过程中的数据泄露风险；
d） 应具备对数据使用加工等数据处理活动进行记录和审计的技术能力，确保数据处理行为的可追溯性。

6.3.3 等级 3：稳健级

除达到二级要求外，该等级的信息技术服务数据安全能力应满足以下要求：
a） 应设立负责数据使用加工安全管理的岗位，该岗位人员能够有效评估数据使用加工的安全风险和合规风险，能够充分理解数据使用加工的合规要求、安全要求和业务要求，并能够根据要求提出针对性的解决方案；
b） 应依据法律法规、行业要求和服务要求，建立并执行数据使用加工安全管理流程，明确数据使用加工的安全策略、权限管控、需求审核、风险评估、合规审查，以及数据使用加工行为和结果使用的审批流程；
c） 针对数据尤其是重要数据、个人信息等敏感数据的，应定期开展安全、合规和影响的风险评估，执行风险处置，以保证数据使用加工等数据处理活动的保密性、完整性、可用性以及合规性；
d） 应对涉及数据使用加工的用户、终端设备、数据应用或组件执行有效的访问控制技术措施，实现对其身份的真实性和合法性的保证；

e） 应对数据的授权、访问、脱敏、导入导出、使用、分析、加工等数据处理活动和行为进行监控，完整记录处理日志，定期进行安全审计，确保未超出数据授权范围；
f） 在使用加工完成后应对数据缓存进行清理，以保证数据处理过程中涉及的数据不会被恢复。

6.3.4 等级 4：优秀级

除达到三级要求外，该等级的信息技术服务数据安全能力应满足以下要求：
a） 应具备违约责任、缔约过失责任、侵权责任等数据使用加工风险分析和处理能力；
b） 应明确脱敏数据治理要求，明确不同分类分级数据的脱敏处理流程，在评估方法等方面反映脱敏治理效果；
c） 应具备脱敏数据识别和脱敏效果验证技术手段，确保数据脱敏的有效性和合规性；
d） 应具备建立数据使用加工管理系统的技术能力，及时响应数据处理的安全风险并进行在线审核；
e） 应具备数据脱敏技术与数据权限管理系统的联动机制，以及数据使用前的脱敏；
f） 应具备技术能力监控并防范数据使用、加工等数据处理过程中的安全风险，对可能涉及的安全风险进行批量的分析和跟进，避免输出的数据处理结果包含可恢复的个人信息、重要数据等数据和结构标识（如用户鉴别信息的重要标识和数据结构），以防止数据处理结果危害个人隐私、公司商业价值、社会公共利益和国家安全；
g） 应具备对数据滥用行为进行有效的识别、监控和预警的技术能力。

6.3.5 等级 5：卓越级

除达到四级要求外，该等级的信息技术服务数据安全能力应满足以下要求：
a） 通过风险监控与审计实现对数据使用加工的安全风险进行自动化分析和处理；
b） 应持续跟踪业务新需求、数据脱敏新技术和最佳实践、合规新要求新变化等，持续改进数据脱敏规则和手段；
c） 应实现对非结构化数据、组合数据的数据脱敏；
d） 持续更新优化数据使用加工安全的技术措施，降低数据泄漏、丢失和损坏等风险；
e） 应跟踪评审数据使用加工安全管理运行效果，根据法律法规、行业要求和服务需求的更新，持续优化数据的授权、访问、脱敏、导入导出、使用、加工、分析等数据处理活动的管理流程和技术能力。

6.4 数据传输安全

6.4.1 等级 1：初始级

该等级的信息技术服务数据安全能力，未建立可持续的数据传输安全管理流程，仅根据临时需求或基于个人经验进行管理和实施防控措施。

6.4.2 等级 2：发展级

该等级的信息技术服务数据安全能力应满足以下要求：
a） 应有相关岗位负责数据传输安全管理；
b） 应根据合规要求和性能的需求，明确需要加密传输的数据范围和加密算法。
c） 应具备数据传输场景加密的技术能力，保证数据传输安全；
d） 应具备数据接口调用的身份鉴别和访问控制的技术能力；
e） 应具备核心网络设备和链路冗余建设的技术能力。

6.4.3 等级 3：稳健级

除达到二级要求外，该等级的信息技术服务数据安全能力应满足以下要求：

a） 应设立管理数据加密、密钥管理岗位人员，负责实现具体场景下的数据传输加密。相关人员应了解常用的安全通道方案、身份鉴别和认证技术、数据加密算法、数据传输安全管理方式等；

b） 应明确数据传输安全管理规范，明确数据传输安全要求(如传输通道加密、数据内容加密、签名验签、身份鉴别、数据传输接口安全等)，确定需要对数据传输加密的场景；

c） 应明确对数据传输安全策略的变更进行审核的技术方案；

d） 应具备身份鉴别和认证、传输数据加密、跨安全域间的数据接口调用安全、数据内容、流量监控和审计的技术能力；

e） 应具备对关键网络设备节点、网络传输链路和数据传输通道进行冗余建设的技术能力；

f） 应具备防范网络可用性及数据泄露风险的技术措施，如负载均衡、防入侵攻击、数据防泄漏检测与防护等设备。

6.4.4 等级 4：优秀级

除达到三级要求外，该等级的信息技术服务数据安全能力应满足以下要求：

a） 应在数据分类分级定义的基础上，明确提出对不同类型、级别的数据的加密传输要求，包含对数据加密算法的要求和密钥的管理要求；

b） 应具备传输数据的完整性检测、数据容错或恢复、接口过滤、异常处理的技术能力；

c） 应具备限制或过滤接口不安全输入参数的技术能力，为接口提供异常处理、传输通道安全配置、密码算法配置、密钥管理等技术能力；

d） 应具备通过相关指标定量分析网络可用性及数据防泄漏检测的技术能力，并有针对性地解决问题，提升网络可用性。

6.4.5 等级 5：卓越级

除达到四级要求外，该等级的信息技术服务数据安全能力应满足以下要求：

a） 具备网络安全设备的健康状态检查及自动化切换的技术能力；

b） 每个传输链路上的节点应部署独立密钥对和数字证书，保证各节点身份鉴别的有效性；

c） 应综合量化敏感数据加密和数据传输通道加密的实现效果和成本，定期审核并调整数据加密的实现方案；

d） 应采用统一的数据加方案，根据不同数据类型和级别进行数据加密处理，保证数据加密功能的统一性；

e） 应跟进传输通道加密保护的技术发展，评估新技术对安全方案的影响，适当引入新技术以应对最新的安全风险；

f） 应及时跟进最近技术及相关制度，进行数据接口服务和安全管理的持续改进。

6.5 数据提供公开安全

6.5.1 等级 1：初始级

该等级的信息技术服务数据安全能力，未建立可持续的数据提供公开安全管理，仅根据临时需求或基于个人经验在个别场景考虑了数据提供公开的安全风险。

6.5.2 等级 2：发展级

除达到一级要求外，该等级的信息技术服务数据安全能力应满足以下要求：

a） 应由相关人员负责对数据提供公开方案进行安全风险管控；

b） 应明确核心业务数据提供公开的安全制度和审核流程，明确数据提供公开安全的制度要求；

c） 针对重要数据、个人信息等敏感数据的共享、转让等数据提供公开场景，应具备数据脱敏和加密的技术能力；
d） 应具备数据脱敏、在线审批发布的技术方式保证数据公开的安全。

6.5.3 等级 3：稳健级

除达到二级要求外，该等级的信息技术服务数据安全能力应满足以下要求：
a） 应设立数据提供公开安全的管理岗位，相关人员应能够充分理解组织的数据提供公开规程，并根据数据提供公开的业务执行相应的风险评估，从而提出实际的解决方案；
b） 应制定数据提供公开安全的制度流程，明确数据提供公开的审核制度，严格审核数据提供公开合规要求；
c） 应采取必要措施建立数据公开事件应急处理流程；
d） 应具备技术能力确保重要数据、个人信息等敏感数据在共享、转让、发布等数据提供、公开场景的安全合规，如数据脱敏、数据加密、安全通道、共享交换区域等；
e） 具备对数据提供、公开过程及数据进行监控和审计的技术能力，涉及的数据应符合业务需求且没有超出数据授权范围；
f） 具备数据发布管理系统，实现数据发布的内容审核和流程审批的统一管理机制。

6.5.4 等级 4：优秀级

除达到三级要求外，该等级的信息技术服务数据安全能力应满足以下要求：
a） 应针对关键的数据资源，明确提供公开的细则和审核流程；
b） 应细化明确各类数据提供公开场景的审核流程，从审核的有效性和审核的效率层面充分考虑流程节点的提供公开流程；
c） 具备规范所提供数据的格式的技术能力，如机器可读的格式规范；
d） 具备建立统一的数据共享转让系统的技术能力，提示数据共享转让的安全风险并进行在线审核；
e） 应建立统一的数据发布管理系统，提示数据发布安全风险并进行在线审核；
f） 应配置数据提供、公开技术机制或服务组件，明确数据提供安全基线要求。

6.5.5 等级 5：卓越级

除达到四级要求外，该等级的信息技术服务数据安全能力，应跟踪评审数据提供公开安全管理执行效果，根据法律法规、行业要求和服务需求的更新，持续优化数据公开安全方面的管理流程和技术能力。

6.6 数据销毁安全

6.6.1 等级 1：初始级

该等级的信息技术服务数据安全能力，未建立可持续的数据销毁安全管理流程，仅根据临时需求或基于个人经验对存储介质或数据进行了销毁。

6.6.2 等级 2：发展级

该等级的信息技术服务数据安全能力应满足以下要求：
a） 应有相关岗位负责存储介质和数据销毁管理；
b） 应依据数据销毁管理要求和合规要求，执行存储介质或数据的销毁工作；
c） 应具备对存储介质进行物理销毁的技术能力；
d） 应具备对数据内容进行擦除销毁的技术能力。

6.6.3 等级 3：稳健级

除达到二级要求外，该等级的信息技术服务数据安全能力应满足以下要求：

a） 应设立负责数据销毁管理的岗位，该岗位人员应熟悉物理销毁和逻辑销毁技术，能够评估数据销毁的安全风险和合规风险，能够充分理解数据销毁的合规要求、安全要求和业务要求，并能够根据要求提出针对性的解决方案；

b） 应依照相关法律法规、标准规范的要求，建立存储介质和数据的销毁管理流程，明确销毁审批机制和操作程序，明确销毁的监控机制，监督操作过程，并对销毁审批以及登记、交接和销毁过程进行监控和记录；

c） 应按照数据分类分级要求建立销毁策略，针对不同的存储介质，明确不同数据销毁的场景、销毁对象、销毁方式和销毁要求；

d） 针对各类存储介质和数据，应具备硬销毁和软销毁的数据销毁方法和技术措施，如基于安全策略、基于分布式杂凑算法等数据分布式存储的销毁策略与机制；

e） 数据销毁技术措施应确保以不可逆方式销毁敏感数据及其副本内容；

f） 应具备统一的存储介质销毁工具，包括但不限于物理销毁、消磁设备等工具，能够实现对各类介质的有效销毁。

6.6.4 等级 4：优秀级

除达到三级要求外，该等级的信息技术服务数据安全能力应满足以下要求：

a） 应建立数据销毁效果评估机制，定期开展销毁记录检查和效果评估；

b） 明确已共享或已被其他用户使用的数据销毁管控措施；

c） 应具备对数据的销毁需求进行明确标识的技术措施，并可通过该技术措施提醒数据管理者及时发起对数据的销毁；

d） 应具备避免误销毁数据的技术措施；

e） 应由经过认证的机构或设备对存储媒体进行物理销毁，或联系经认证的销毁服务商进行存储媒体销毁。

6.6.5 等级 5：卓越级

除达到四级要求外，该等级的信息技术服务数据安全能力，应跟踪评审数据销毁的运行效果，根据法律法规、行业要求和服务需求的更新，持续优化存储介质和数据的销毁管理流程和技术能力。

6.7 数据处理通用安全能力

6.7.1 数据识别管理

6.7.1.1 等级 1：初始级

该等级的信息技术服务数据安全能力，未建立可持续的数据识别管理流程，仅根据临时需求或基于个人经验对个人信息、重要数据、跨境数据、数据质量等进行数据识别。

6.7.1.2 等级 2：发展级

该等级的信息技术服务数据安全能力应满足以下要求：

a） 应有相关人员负责数据识别管理；

b） 应根据业务特性和外部合规要求形成管理流程，对核心业务的关键数据和数据质量进行管理。

6.7.1.3 等级 3：稳健级

除达到二级要求外，该等级的信息技术服务数据安全能力应满足以下要求：

a） 应设立数据识别工作管理岗位，相关人员应了解数据识别合规要求，熟悉数据质量管理要求；

b） 应对核心业务的关键数据进行数据识别，识别哪些数据属于个人信息、重要数据、跨境数据等；

c） 应采用技术措施实现对服务所涉及的个人信息、重要数据等敏感数据进行数据识别和质量管理，并实现异常数据及时告警或更正。

6.7.1.4 等级 4：优秀级

除达到三级要求外，该等级的信息技术服务数据安全能力应满足以下要求：

a） 应对所有业务的关键数据进行识别，包括识别个人信息、重要数据、敏感数据和其他信息，形成数据保护目录，并及时更新；

b） 应采用技术措施实现数据质量分级，实现不同级别和类型的数据管理；

c） 应采用技术措施实现对数据质量进行分析、预判和盘点，实现数据质量问题定位和修复管理。

6.7.1.5 等级 5：卓越级

除达到四级要求外，该等级的信息技术服务数据安全能力，应跟踪评审数据识别管理执行效果，根据法律法规、行业要求和服务需求的更新，持续优化数据识别等方面的管理流程和技术能力。

6.7.2 数据分类分级管理

6.7.2.1 等级 1：初始级

该等级的信息技术服务数据安全能力，未建立可持续的数据资产和分类分级管理流程，仅根据临时需求或基于个人经验对个别业务开展了数据资产和分类分级管理。

6.7.2.2 等级 2：发展级

该等级的信息技术服务数据安全能力应满足以下要求：

a） 应有相关岗位负责数据分类分级和资产管理；

b） 核心业务应制定数据资产登记制度，建立数据资产清单，明确数据资产管理的相关方；

c） 应根据业务特性和外部合规要求，对核心业务的关键数据进行分类分级管理。

6.7.2.3 等级 3：稳健级

除达到二级要求外，该等级的信息技术服务数据安全能力应满足以下要求：

a） 应设立负责数据安全分类分级、数据资产管理岗位，相关人员应了解组织整体的数据分类分级的安全原则和数据分类分级的合规要求；

b） 应对组织的数据资产进行统一管理，负责数据资产管理规范的制定和落地推动；

c） 应定义组织整体的数据分类分级的安全原则。明确分类分级原则、方法和操作指南；

d） 应明确了解数据分类分级的合规要求；

e） 应采用数据识别技术或工具，实现对核心业务数据的分类分级标识。

6.7.2.4 等级 4：优秀级

除达到三级要求外，该等级的信息技术服务数据安全能力应满足以下要求：

a） 应明确数据资产更新、运营风险评估和供应链安全审查的规程和制度，在组织层面建立数据资产安全管理制度，定义数据资产的相关角色定位和职责；

b） 当法律法规、重大业务发生变化时，应及时更新数据分类分级目录；

c） 应采用分级分类技术或工具实现数据的分类分级管理，并实现数据的分类分级防护。

6.7.2.5 等级 5：卓越级

除达到四级要求外，该等级的信息技术服务数据安全能力，应跟踪评审数据分类分级管理执行效果，根据法律法规、行业要求和服务需求的更新，持续优化数据分类分级等方面的管理流程和技术能力。

6.7.3 数据风险防控管理

6.7.3.1 等级 1：初始级

该等级的信息技术服务数据安全能力，未建立可持续的数据风险评估和处置流程，仅根据临时需求或基于个人经验对个别服务实施了数据风险评估和处置。

6.7.3.2 等级 2：发展级

该等级的信息技术服务数据安全能力应满足以下要求：

a） 应有相关人员负责数据风险防控；

b） 核心业务应明确数据数据风险防控的原则或要求,如对数据安全缺陷、漏洞进行识别;

c） 应对涉及数据风险项进行审核,针对具体的数据风险场景制定了相应的风险防控方案。

6.7.3.3 等级 3：稳健级

除达到二级要求外，该等级的信息技术服务数据安全能力应满足以下要求：

a） 应设立负责数据风险防控管理岗位，相关人员能够基于合规性要求、相关标准对数据风险分析中所可能引发的数据安全风险进行有效的评估,并能够针对分析场景提出有效的解决方案；

b） 应制定整体的数据风险防控原则和相应的技术支持方案；

c） 应明确数据风险防控的规范，明确数据风险防控的评估流程,对数据风险的来源、风险分析、风险处置等的审核;

d） 应能够基于合规性要求、相关标准对数据风险分析中所可能引发的数据聚合的安全 风险进行有效的评估,并能够针对分析场景提出有效的解决方案；

e） 应采用数据安全合规风险识别技术或相关工具监控和审计个人信息、重要数据、关键数据的日常情况。

6.7.3.4 等级 4：优秀级

除达到三级要求外，该等级的信息技术服务数据安全能力应满足以下要求：

a） 应采取必要的监控审计措施,确保实际进行的分析操作与分析结果使用与其声明的一致,整体保证数据风险防控的预期。

6.7.3.5 等级 5：卓越级

除达到四级要求外，该等级的信息技术服务数据安全能力，应跟踪评审数据风险防控管理执行效果，根据法律法规、行业要求和服务需求的更新，持续优化数据风险防控等方面的管理流程和技术能力。

6.7.4 数据审计溯源管理

6.7.4.1 等级 1：初始级

该等级的信息技术服务数据安全能力，未建立可持续的数据安全审计和溯源管理流程，仅根据临时需求或基于个人经验对个别服务进行了数据安全审计和溯源措施。

6.7.4.2 等级 2：发展级

该等级的信息技术服务数据安全能力应满足以下要求：

a） 应有相关岗位负责数据安全审计溯源管理；
b） 应对核心系统数据的生命周期全过程进行安全审计和溯源；
c） 核心业务应建立数据安全审计监控相关规则，明确对数据生存周期各阶段的数据访问和操作进行监控的方案(如实时监控、定期批量监控等)；
d） 应明确制定组织内部各类数据访问和操作的日志记录、安全监控、审计溯源的制度。

6.7.4.3 等级 3：稳健级

除达到二级要求外，该等级的信息技术服务数据安全能力应满足以下要求：

a） 组织应设立数据审计溯源管理岗位，相关人员应了解数据访问和操作涉及的数据范围，具备对安全风险的判断能力；
b） 应明确数据访问和操作涉及的数据范围，具备对安全风险的判断能力；
c） 应采用自动和人工审计相结合的方法或手段对数据的高风险操作进行监控；
d） 应采用针对数据访问和操作的日志监控技术措施，实现对数据异常访问和操作进行告警，敏感数据以及特权账户对数据的访问和操作都纳入重点的监控范围；
e） 应采用必要的数据防泄漏实时监控技术措施，监控及报告个人信息、重要数据等敏感数据的外发行为；
f） 应采用技术措施对数据交换服务流量数据进行安全监控和分析。

6.7.4.4 等级 4：优秀级

除达到三级要求外，该等级的信息技术服务数据安全能力应满足以下要求：

a） 应充分理解数据监控和审计的要求，能够识别数据泄漏风险.并及时采取措施；
b） 应建立统一的数据访问和操作的日志监控技术工具，量化数据访问和操作引发的数据安全风险，实现对数据安全风险的整体感知；
c） 应记录数据交换服务接口调用事件信息，监控是否存在恶意数据获取、数据盗用等风险；
d） 应具备对数据的异常或高风险操作进行自动识别和实时预警的能力。

6.7.4.5 等级 5：卓越级

除达到四级要求外，该等级的信息技术服务数据安全能力，应跟踪评审数据审计溯源管理执行效果，根据法律法规、行业要求和服务需求的更新，持续优化数据审计溯源方面的管理流程和技术能力。

6.7.5 数据合规管理

6.7.5.1 等级 1：初始级

该等级的信息技术服务数据安全能力，未建立可持续的数据合规管理流程，仅根据临时需求或基于个人经验考虑了数据安全、个人信息保护、跨境数据传输的合规要求。

6.7.5.2 等级 2：发展级

该等级的信息技术服务数据安全能力应满足以下要求：

a） 应有相关岗位负责数据合规管理；

b） 应识别在数据安全、个人信息保护、跨境数据传输等方面的合规要求，将合规要求更新至相关制度流程中，并在重要环节设置相应的管控措施；

c） 针对涉及数据处理活动的合同或协议，应明确数据的使用目的、供应方式、保密约定和安全责任义务等合规要求；

d） 应具备技术能力支持数据安全、个人信息保护、跨境数据传输的合规管理。

6.7.5.3 等级 3：稳健级

除达到二级要求外，该等级的信息技术服务数据安全能力应满足以下要求：

a） 应设立数据合规管理的岗位，该岗位人员应能够充分理解数据安全、个人信息保护、跨境数据传输的合规要求，并能够根据要求提出针对性的解决方案；

b） 应依据相关法律法规、标准规范的要求，建立并执行数据安全、个人信息保护、跨境数据传输的合规管理流程；

c） 应建立相关法律法规、标准规范的数据合规资料库，相关人员可以通过该资料库查询合规要求；应定期跟踪合规要求的变化更新合规资料库，分析和解读新要求，及时发送给相关方以宣贯执行；

d） 应对数据处理活动变化、重要数据流向变化建立变更管控机制，以控制可能引发的合规风险；

e） 应采用必要的技术手段和控制措施实现重要数据、个人信息等敏感数据的安全保护，例如在数据处理过程中进行匿名化、去标识化；

f） 应建立重要数据、个人信息等敏感数据的监控技术措施，防范数据安全事件；

g） 应定期对数据安全策略、规范、制度和管控措施进行风险评估，并及时响应。

6.7.5.4 等级 4：优秀级

除达到三级要求外，该等级的信息技术服务数据安全能力应满足以下要求：

a） 应定期开展数据安全、个人信息保护、跨境数据传输的合规风险评估,建立并完善合规管理流程的指导细则；

b） 应定期或在发生重大安全事件后，对合规管理流程进行审核和检验，并及时响应；

c） 在业务调整、人员岗位调整、数据处理活动或相关系统、组件变更时，应妥善处理重要数据、个人信息等敏感数据，防范数据安全和合规风险；

d） 应具备量化组织整体合规情况的技术能力，并将合规结果通过图形化方式报给需方，以保证需方对信息技术服务的合规情况得到有效了解；

e） 应具备针对数据安全、个人信息保护、跨境数据传输的数据处理行为和风险进行监控的技术能力，定期审计相关操作记录；

f） 应具备针对多源数据集汇聚和关联后个人信息利用的安全风险分析和保护的技术能力。

6.7.5.5 等级 5：卓越级

除达到四级要求外，该等级的信息技术服务数据安全能力应满足以下要求：

a） 应关注并跟进监管机构的合规要求动态，并及时更新合规管理流程；

b） 应关注相关行业内数据安全、个人信息保护、跨境数据传输方面的合规动态，能够根据合规要求以及业务需求变化，及时更新数据安全、个人信息保护、跨境数据传输的整体解决方案。

6.7.6 数据安全需求管理

6.7.6.1 等级 1：初始级

该等级的信息技术服务数据安全能力，未建立可持续的数据安全需求管理流程，仅根据临时需求或基于个人经验收集并实现了数据安全需求。

6.7.6.2 等级 2：发展级

该等级的信息技术服务数据安全能力应满足以下要求：

a） 应有相关岗位负责数据安全需求分析工作；

b） 应对重要服务开展数据安全需求分析工作。

6.7.6.3 等级 3：稳健级

除达到二级要求外，该等级的信息技术服务数据安全能力应满足以下要求：

a） 应设立数据安全需求管理的岗位，该岗位人员应能够充分挖掘和理解数据在合规管理、安全管理和业务方面的安全需求，对涉及数据处理的业务开展数据安全需求分析和管理，确保安全需求的有效制定和规范化表达；

b） 应建立数据安全需求分析的管理流程和评审机制，明确安全需求内容要求；

c） 应依据法律法规、标准规范等要求，分析数据安全合规需求；

d） 应结合涉及数据处理的服务目标和业务特性，明确数据安全需求和安全规划实施的优先级；

e） 应识别涉及数据处理的服务所面临的弱点和威胁，分析数据安全风险和应对措施需求。

6.7.6.4 等级 4：优秀级

除达到三级要求外，该等级的信息技术服务数据安全能力应满足以下要求：

a） 应使用数据驱动分析方法或安全需求工程思想进行数据安全需求分析，确保数据安全需求的有效表达；

b） 应建立数据安全需求分析管理系统，该系统记录所有服务的数据安全需求的申请、分析以及相关安全方案，以保证对所有服务的数据安全需求分析过程的有效追溯。

6.7.6.5 等级 5：卓越级

信息技术服务提供者在开展信息技术服务时，在优秀级基础上，应持续更新优化数据安全需求分析管理技术措施，降低安全风险。

除达到四级要求外，该等级的信息技术服务数据安全能力，应跟踪评审数据安全需求管理的运行效果，根据法律法规、行业要求和服务需求的更新，持续优化数据安全需求挖掘和分析等方面的管理流程和技术能力。

6.7.7 数据处理环境安全

6.7.7.1 等级 1：初始级

该等级的信息技术服务数据安全能力，未建立成熟稳定的数据处理环境安全管理流程，仅根据临时需求或基于个人经验针对个别服务关注了数据处理环境安全。

6.7.7.2 等级 2：发展级

该等级的信息技术服务数据安全能力应满足以下要求：

a） 应有相关岗位负责数据处理环境安全管理；

b） 针对重要服务的数据处理环境，单独建立了身份认证、访问控制、安全配置等安全措施。

6.7.7.3 等级 3：稳健级

除达到二级要求外，该等级的信息技术服务数据安全能力应满足以下要求：

a） 应设立统一负责数据处理环境安全管理的岗位，该岗位人员应熟悉数据处理活动所特有的安全风险和合规风险，能够充分理解数据数据处理活动的合规要求、安全要求和业务要求，并能够根据要求提出针对性的解决方案；

b） 应依据数据分类分级的安全要求和合规要求，针对不同类型和级别的数据的处理环境，包括数据处理相关系统、组件和终端设备，建立并执行相应的安全控制措施，包括不限于身份认证、访问控制、安全配置、数据脱敏、密码技术、数据防泄漏等技术措施，以防范数据泄露、丢失、损坏、篡改、伪造、滥用和非授权访问等风险；

c） 应建立并执行数据处理环境的安全管理流程，以有效管理数据处理安全控制措施的运行；

d） 应建立并执行终端设备的数据安全管理规范，明确终端设备的安全配置管理和数据防泄漏管理要求，实现终端设备与人员的有效绑定，实施网络准入、防病毒、加解密或数据防泄漏等技术措施等；

e） 应对需要身份鉴别的用户、数据应用或组件进行身份标识和鉴别，身份标识具有唯一性，鉴别信息具有复杂度要求并定期更换，多次登录失败后应采取必要的保护措施；

f） 应明确适合数据处理环境的数据加解密处理要求和密钥管理要求；

g） 应具备建立数据权限管理系统的技术能力，明确数据权限授权审批流程，实现与数据处理相关系统的联动机制，保证用户在访问数据前已获得授权；

h） 基于数据处理相关系统的多租户的特性，应对不同的租户实现数据、系统功能、会话、调度和运营环境等资源的隔离控制；

i） 应建立数据处理时效性管理流程，明确数据处理活动的有效期、到期时数据的处理流程以及过期数据的安全管理要求；

j） 应具备建立数据处理日志管理工具的能力，能够监控数据全生命周期的处理行为，能够记录用户在数据处理相关系统上的操作行为，能够完整记录处理日志；

k） 应对数据处理的数据范围、权限和处理活动开展定期审计，确定用户或合作方对数据的处理未超出授权范围。

6.7.7.4 等级 4：优秀级

除达到三级要求外，该等级的信息技术服务数据安全能力应满足以下要求：

a） 应建立身份认证和访问控制管理系统，支持数据处理相关系统的接入，实现对用户、数据应用或组件访问数据资源的身份鉴别、访问控制和权限管理的联动；

b） 应采用多因素鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现；

c） 应建立面向数据应用或组件的访问控制机制，包括访问控制时效的管理和验证，以及数据应用接入的合法性和安全性取证机制；

d） 针对分布式处理环境，应明确外部服务组件注册与使用审核、分布式处理节点间可信连接认证、节点和用户安全属性周期性确认、数据文件标识和用户身份鉴权、数据副本节点更新检测及防止数据泄漏等方面进行安全要求和控制；

e） 应对分布式处理过程中不同数据副本节点数据的完整性和一致性进行定期检测；

f） 应建立数据分布式处理节点的服务组件自动维护和管控措施，包括虚假节点监测、 故障用户节点确认和自动修复的技术机制；

g） 应具备对密文数据进行搜索、排序、计算等透明处理的技术能力；

h） 应建立分布式处理过程中的数据泄漏控制机制，防止数据处理过程中的调试信息、日志记录等不受控制输出导致受保护个人信息、重要数据等敏感数据的泄漏。

6.7.7.5 等级 5：卓越级

应跟踪评审数据处理环境安全管理运行效果，根据法律法规、行业要求和服务需求的更新，持续优化数据全生命周期的处理活动和环境的管理流程和技术能力。

7 服务安全交付能力

7.1 交付安全管理

服务提供方在向需方提供运行信息技术服务的过程中通过实施管理动作，确保服务交付过程中数据安全得到有效控制。

7.1.1 等级 1：初始级

该等级的信息技术服务数据安全能力应满足以下要求：

a） 供方未建立成熟稳定的交付数据安全管理机制，仅根据个人经验对服务交付过程的数据安全进行管理。

7.1.2 等级 2：发展级

该等级的信息技术服务数据安全能力应满足以下要求：

a） 服务提供方在交付服务前，应确定服务过程数据安全目标；

b） 应根据服务过程数据安全目标采取措施对服务交付过程的数据安全进行控制。

7.1.3 等级 3：稳健级

除达到二级要求外，该等级的信息技术服务数据安全能力应满足以下要求：

a） 服务数据安全目标应根据需方需求确定，明确落实措施，确保目标的实现；

b） 供方应在服务交付过程中明确服务数据安全组织机构和服务数据安全职责；

c） 供方应在服务实施过程中保证必要的要素资源，确保服务数据安全目标落实措施的实现；

d） 供方应关注服务数据安全目标的达成情况，及时发现问题并对发现的问题提出改进建议；

e） 供方应对服务数据安全风险进行识别，有针对性的落实服务数据安全要求，实现信息技术服务数据安全风险的有效控制。

7.1.4 等级 4：优秀级

除达到三级要求外，该等级的信息技术服务数据安全能力应满足以下要求：

a） 供方应根据信息技术服务需求和内外部环境的变化，动态调整服务数据安全目标，并及时调整技术和管理的安全控制措施，以确保需方数据安全得到保护；

b） 供方应在服务交付过程中建立数据安全管理制度要求以满足：所提供的信息技术服务需求、服务需求方的数据安全管理要求；

c） 供方应持续开展交付数据安全制度执行情况的检查和改进活动，定期评审服务数据安全管理制度要求的有效性；

d） 供方应定期开展服务数据安全检查工作，检查内容覆盖：服务数据安全目标达成情况；数据安全风险控制及控制措施落实情况；数据安全制度及流程要求执行情况；数据安全技术工具应用情况；

e） 供方应对服务数据安全工作开展情况定期总结分析，提出建议并改进，以提升服务数据安全保障水平；

f） 供方应跟踪识别新的数据安全风险，定期对数据安全风险进行回顾。

7.1.5 等级 5：卓越级

除达到四级要求外，该等级的信息技术服务数据安全能力应满足以下要求：

a） 供方应能够实现服务数据安全控制过程可视化，并能够利用量化数据对控制过程进行持续改进；

b） 供方应具备数据安全风险动态监测能力，对服务过程中数据安全风险控制措施实现动态调整。

7.2 交付安全策划

供方在服务交付过程中通过策划数据安全控制活动，保障服务交付过程中数据安全。

7.2.1 等级 1：初始级

该等级的信息技术服务数据安全能力应满足以下要求：

a） 供方未建立成熟稳定的交付数据安全策划机制或流程，仅根据个人经验对服务交付过程的数据安全进行策划。

7.2.2 等级 2：发展级

该等级的信息技术服务数据安全能力应满足以下要求：

a） 供方应围绕服务数据安全目标及识别出的服务数据安全风险，对服务数据安全控制进行策划；

b） 供方应与需方明确服务数据安全目标并将保障工作纳入服务内容。

7.2.3 等级 3：稳健级

除达到二级要求外，该等级的信息技术服务数据安全能力应满足以下要求：

a） 供方应策划制定服务数据安全控制措施实施方案、检查计划和改进计划；

b） 供方应在服务策划时进行成本预算，平衡风险控制措施与开支；

c） 供方应策划配备能够满足服务数据安全要求的管理人员和专业技术人员；

d） 供方应根据服务数据安全需求准备必要的数据安全技术工具、手册指南、知识库；

e） 供方应明确服务过程中数据安全考核要求、计算办法和奖惩措施；

f） 供方应按照策划的内容实施服务数据安全控制，并对实施过程的关键信息进行记录，必要时将信息记录入服务报告；

g） 供方应通过策划内容与实施结果的对比检查，确认风险措施的落实情况，并对发现的问题提出改进建议。

7.2.4 等级 4：优秀级

除达到三级要求外，该等级的信息技术服务数据安全能力应满足以下要求：

a） 供方应策划对服务数据安全控制措施的执行情况进行定期审计评估，分析潜在的问题；

b） 供方应策划检查实施过程中遗留数据安全隐患问题的处理情况；

c） 供方应策划定期总结分析服务数据安全目标未达成项，提出并实施改善建议，跟踪反馈；

d） 供方应策划调查分析服务中发生的数据安全事件事态，提出并实施改善意见，跟踪反馈；

e） 供方应策划对存在漏洞的风险控制措施，提出并实施改善意见，跟踪反馈；

f） 供方应策划定期向需方报告其需要关注和处置的数据安全风险。

7.2.5 等级 5：卓越级

除达到四级要求外，该等级的信息技术服务数据安全能力应满足以下要求：

a） 供方应针对所开展的不同类型信息技术服务，策划储备有适宜的服务数据安全控制方案，并能够提供充足的资源保障；

b） 供方应设置专职团队，跟踪数据安全发展趋势，储备前瞻性的数据安全技术手段，具备解决服务团队及需方数据安全问题的能力。

7.3 交付安全活动

供方通过向需方提供风险识别、安全防护、监测预警和响应处置等交付安全活动，以保障服务交付过程中数据安全。

7.3.1 等级 1：初始级

该等级的信息技术服务数据安全能力应满足以下要求：

a） 供方未形成成熟稳定的交付数据安全活动，仅根据个人经验在服务交付过程实施相关控制活动。

7.3.2 等级 2：发展级

该等级的信息技术服务数据安全能力应满足以下要求：

a. 风险识别：

1） 供方应识别服务交付过程中的数据安全风险和供应链安全风险。

b. 安全防护：

1） 供方应从环境安全防护、操作安全防护、数据接口防护方面制定服务交付过程中的数据安全防护措施，并在服务实施过程中落实。

c. 监测预警:

1） 供方在服务交付过程中应对数据处理、系统运行、服务实施过程开展风险监测活动；

2） 供方应针对服务交付过程定期开展数据安全检查评估活动。

d. 响应处置

1） 能响应需方要求建立数据安全事件应急预案，满足需方要求；

2） 能响应需方要求制定数据安全事件应急预案演练计划，参与或协助需方进行数据安全事件应急演练。

7.3.3 等级 3：稳健级

除达到二级要求外，该等级的信息技术服务数据安全能力应满足以下要求：

a. 风险识别：

1） 应识别服务交付过程中的数据资产，建立并维护数据资产目录清单；

2） 应对服务交付过程中涉及数据处理活动的组件进行威胁及脆弱性识别，分析其对数据安全的影响，形成数据安全风险分析报告，并制定风险应对的措施；

3） 应建立数据处理活动安全风险知识库；

4） 应定期自行开展或邀请第三方专业机构开展数据安全风险识别和分析工作；

5） 应定期对供应链上下游组织的数据处理活动中的数据安全风险进行分析和评估。

b. 安全防护：

1） 应制定数据安全风险管理相关的服务数据安全基线配置清单；

2） 应建立移动终端设备、开源软件及第三方服务组件的准入规范要求；

3） 应定期对账号权限进行核查，禁用非法账号、闲置账号、过期账号；

4） 应建立数据高风险操作清单及其管控措施；

5） 应制定数据服务接口安全控制策略，明确规定使用接口的安全限制和安全控制措施。

c. 监测预警:

1) 应具备对数据处理活动相关的威胁情报收集、分析和利用能力，掌握服务交付过程中所面临的数据安全威胁信息；

2) 应在服务交付过程中，建立监测规则和安全基线，能根据预定义的阈值对服务实施过程中的数据安全事态进行告警；

3) 应在服务交付过程中，制定针对信息系统运行过程数据安全风险监测的要求，并定期开展监测活动；

4) 应制定服务持续监控机制，对服务安全措施进行持续监测；

5) 应定期对服务安全控制措施进行检查，并在爆发网络攻击、重大安全漏洞时，及时配合需方要求开展专项安全检查。

d. 响应处置

1) 应建立数据安全事件应急预案，包括应急组织机构与职责、数据安全事件分类分级、监测与预警、应急处置流程、保障措施等内容；

2) 应按照确定的方法和流程对重要信息系统实施风险评估，用于对任何可能对组织造成数据安全损害的风险进行影响分析；

3) 应建立数据安全事件应急预案演练计划，保存演练记录和演练总结报告；

4) 应开展数据安全事件应急预案培训，培训内容覆盖全流程的数据处理活动、关键业务及数据安全应急所需的安全应对控制措施；

5) 应采用监测工具与人工相结合的方式对信息系统所承载的业务数据进行日常监控与预警，以跟踪和判别业务数据是否超出了预警条件；

6) 数据安全事件应急预案应取得需方认可，建立数据安全事件应急处理、协调、沟通渠道；

7) 在数据安全事件涉及个人信息时,及时告知受影响个人信息主体，涉及大量个人信息的，按规定及时向有关主管部门报告；

8) 在数据安全事件处置完成后，应对数据安全事件进行总结分析，形成安全事件处置报告，报告经组织审批后向需方报告。

7.3.4 等级 4：优秀级

除达到三级要求外，该等级的信息技术服务数据安全能力应满足以下要求：

a. 风险识别：

1) 应能够将数据资产识别、数据分类分级等数据安全能力应用到服务交付过程的数据资产识别中；

2) 应在涉及重要数据和个人信息的服务交付时，交付前进行数据安全风险识别，形成风险应对措施，并及时报备给需方；

3) 应针对数据共享、数据发布、数据导入导出等重点风险场景，定期进行隐患排查和风险处置，识别潜在的风险隐患；

4) 应对服务供应链上下游组织的产品和服务的脆弱性和威胁进行识别，形成供应链风险分析报告。

b. 安全防护：

1) 应具备针对海量数据或复杂类型数据进行安全保护的技术及方法；

2) 应能够在服务交付过程中利用数据防泄露、数据脱敏、个人信息去标识化等安全技术手段；

3) 应在服务交付过程中建立数据接口清单，明确数据服务接口安全规范。

c. 监测预警:

1) 应与专业机构建立数据安全威胁情报共享机制，持续提高风险应对处置和防范能力；

2) 应建立针对重要数据和个人信息流转监测机制，并采取技术措施及时发现对这些数据的违规操作或数据泄露等安全风险；
3) 应建立重要数据和个人信息异常处理上报机制，当重要数据或个人信息发生泄露、非法篡改等情况时，及时协助需方采取处置措施；
4) 应具备在服务交付过程中对数据系统越权访问、高频访问、恶意操作等异常行为发现、记录、统计和分析的能力；
5) 应对监测记录的服务监测数据进行关联和分析，定期向需方报告其数据资产的安全状态；
6) 应定期采取模拟攻击方式对交付过程涉及的数据处理活动及其组件进行安全风险评估，持续提升风险监测的能力。

d. 响应处置

1) 应建立数据安全事件应急响应最佳实践知识库，包括数据泄露、数据篡改、数据破坏、网络勒索等不同类型的安全事件及处置办法，并用于应急响应培训及演练计划；
2) 制定安全事件归因数据溯源策略和机制，跟踪和记录数据处理活动及其相关的数据服务，确保能对数据安全事件进行溯源；
3) 识别数据安全事件发生时需要备份和归档的信息技术服务数据，制定数据安全事件发生时数据备份、归档与恢复的计划，并配置必要的数据备份、归档与恢复工具。

7.3.5 等级 5：卓越级

除达到四级要求外，该等级的信息技术服务数据安全能力应满足以下要求：

a. 风险识别：

1) 应能够在服务交付过程中，通过技术手段对数据资产分类分级等安全属性进行自动化标记识别，并动态更新数据资产目录；
2) 应能够在服务交付过程中，定义数据服务供应链上下游组织的数据交换共享的格式规范、接口规范，约定数据提供和数据获取方式等技术或管理措施；
3) 应能够及时向服务供应链上下游的组织，发布所识别的供应链风险及应对风险的建议措施，确保数据供应链风险可控。

b. 安全防护：

1) 应具备在服务交付过程中，建立覆盖数据感知、保护、预警、响应等一体化的数据安全防护体系；
2) 应能够在服务交付过程中，制定供应链中数据流转安全管控策略，并通过技术手段对数据流转操作进行控制；
3) 应具备对重要数据和个人信息等服务接口的调用进行风险识别和安全性分析的能力。

c. 监测预警:

1) 应能够在服务交付过程中，采用自动化技术机制，对数据资产、系统脆弱性、安全事件等威胁情报进行综合分析，对数据安全态势进行可视化展示，并进行主动式的数据安全威胁检测、预警和应急处置；
2) 应在服务交付过程中具备对数据处理活动及其服务接口的访问进行自动化监控和应急处置的能力；
3) 应在服务交付过程中，具备利用数据防泄漏实时监控工具的能力，对异常或高风险的数据交换行为进行实时监控，发现异常时可有效阻断数据传输；
4) 应在服务交付过程中，能够使用自动化的监控工具对服务监控信息进行记录与保存，并确保信息的准确性；
5) 应跟踪数据安全的发展动态和趋势，结合服务交付的实际情况及时更新、完善服务交付过程的数据安全检查评估内容，定期开展专项安全检查评估工作。

d. 响应处置

1) 数据安全事件管理和应急响应机制应随着组织实际情况不断调整、更新和完善,并定期对组织员工开展流程培训和宣贯；

2) 建立异地容灾备份和恢复操作规范，配置系统容灾备份和灾难恢复专业团队，确保灾备中心具备按照业务系统重要性和其影响面要求及时接管信息系统的数据处理活动的能力；

应参与国际、国家或行业相关标准制定。在业界分享最佳实践,成为行业标杆。

7.4 服务成果安全

7.4.1 等级 1：初始级

该等级的信息技术服务数据安全能力应满足以下要求：

供方未建立成熟稳定的服务成果数据安全要求机制，未采用明确措施保证服务成果的数据安全要求，仅根据个人经验对服务成果的数据安全进行管理。

7.4.2 等级 2：发展级

除达到一级要求外，该等级的信息技术服务数据安全能力应满足以下要求：

a） 供方建立成熟稳定的服务成果数据安全要求机制；

b） 供方按照需方服务成果的数据安全要求，制定符合要求的计划措施，并跟踪执行。

7.4.3 等级 3：稳健级

除达到二级要求外，该等级的信息技术服务数据安全能力应满足以下要求：

a） 供方有专人负责服务成果数据安全管理工作；

b） 供方根据需方要求，实现对服务成果权生命周期安全管理；

c） 项目级服务成果数据安全要求，需与组织级数据安全要求一致；

d） 建立并实施评价和分析服务成果数据安全的检查计划，并跟踪执行；

e） 建立并实施评价和分析服务成果数据安全的改进计划，并跟踪执行；

f） 开展组织级服务成果数据安全评审工作。

7.4.4 等级 4：优秀级

除达到三级要求外，该等级的信息技术服务数据安全能力应满足以下要求：

a） 供方有独立的部门负责服务成果数据安全管理工作，并具备承担该工作的能力，掌握服务成果数据安全管理知识，掌握本企业信息技术数据安全管理体系；

b） 供方按照制度或要求对服务成果数据安全进行监测、评审并记录，保留记录文档；对服务成果数据安全检查结果进行分析评估，提供持续改进建议。各项检查结果作为实施交付计划数据安全要求和体系改进的输入项，并得到运用；

c） 供方对所有涉及服务成果的管理文档、分析报告和过程实施记录进行管理；

d） 供方分析和改善未达服务成果数据安全的情况、用户投诉情况、用户不满意情况；

e） 分析服务成果数据安全，改善实施交付数据安全要求，挖掘服务价值；

f） 建立内部主动服务改进机制，跟踪服务成果数据安全改善情况。

7.4.5 等级 5：卓越级

除达到四级要求外，该等级的信息技术服务数据安全能力应满足以下要求：

a） 利用技术工具，服务成果数据安全内容可自动及时获取，并应有全生命周期管理；
b） 利用技术工具，基于量化数据分析和评测项目级服务成果数据安全的情况和发展趋势；
c） 利用技术工具，基于量化数据评价服务成果数据安全与需方的业务匹配程度，实现动态调整数据安全策略；
d） 基于服务成果数据安全中获取的数据，及时优化服务成果数据安全方案和内容；
e） 建立针对服务成果数据安全的量化分析方法，重点分析实施交付中的优势内容、存在的不足，以及对客户满意度的影响和对改进服务成果数据安全的价值等；
f） 建立对服务成果数据安全的评价、复用的方法，实施定期评价，并与信息技术数据安全要求行关联。

参 考 文 献

[1] ISO/IEC 27002:2022 信息安全、网络安全和隐私保护-信息安全控制
[2] GB/T 37988-2019 信息安全技术 数据安全能力成熟度模型
[3] GB/T 41479-2022 信息安全技术 网络数据处理安全要求
[4] GB/T 25069-2022 信息安全技术 术语