ICS 35.040
L80

# 中华人民共和国国家标准

GB/T XXXXX—XXXX

# 信息安全技术　数据安全能力成熟度模型

Information security techniques —Data security capability maturity model

（征求意见稿）

2017-08-17

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

# 目　　次

# 前　言

本标准依据GB/T1.1—2009给出的规则进行起草。

本标准由全国信息安全标准化技术委员会（SAC/TC 260）提出并归口。

本标准主要起草单位：阿里巴巴（北京）软件服务有限公司、中国电子技术标准化研究院、中国信息安全测评中心、北京奇虎科技有限公司、联想（北京）有限公司、国家信息安全工程技术研究中心、公安部第三研究所、清华大学、中国信息安全认证中心、中国科学院软件所、中国移动通信集团公司、北京天融信科技股份有限公司、中国科学院信息工程研究所、北京华宇信息技术有限公司、陕西省信息化工程研究院、西北大学、北京易华录信息技术股份有限公司、新华三集团、勤智数码科技股份有限公司、北京数字认证股份有限公司、启明星辰信息技术集团股份有限公司、海信集团、银川市大数据管理服务局、南京中新赛克科技有限责任公司、北京微步在线科技有限公司、上海观安信息技术有限公司、亚信科技（成都）有限公司。

本标准主要起草人：梅婧婷、李克鹏、薛勇、潘亮、郑斌、朱红儒、叶润国、胡影、叶晓俊、谢安明、孙明亮、郑新华、柯妍、徐雨晴、宋玲娓、刘玉岭、苗光胜、潘正泰、张锐卿、任卫红、金涛、任兰芳、常玲、赵蓓、唐海龙、罗海龙、孙晓军、李正、孙骞、赵江、陈驰、马红霞、高冀鹏、鲁晋、杨宇波、刘伟、谢江、周薇茹、杜青峰、薛坤、程瑜琦、尤其。

# 引　言

伴随着大数据技术的发展和普及，组织机构在业务发展、企业运营等关键环节利用大数据技术对业务进行优化以发掘出更多的数据价值。大量的组织机构参与到大数据产业中，提供对外的各种数据服务，成为数据源提供者、数据计算平台提供者、数据服务或应用提供者等大数据产业相关的角色；同时在组织的内部管理运营过程中，组织机构利用大数据技术使能业务的发展和组织的运营，极大程度改变了其传统工作模式和业务发展方向，同时，对组织机构的数据安全管理带来了新的挑战。数据的高速流通性让组织机构内部信息系统、网络区域之间的边界越发模糊；而在大数据技术的广泛应用中，大数据的特性如大容量、多种类和可变性都对组织机构的数据管理能力提出了更高的要求。

组织机构除了关注自身业务中产生的数据之外，也开始采集外部第三方组织或人员的数据来丰富自己的数据资源，数据在不同组织机构间的流通和加工成为不可避免的趋势。数据作为组织机构的重要资产，一方面面临着传统环境中数据安全的相关风险，另一方面也面临着大数据环境下所特有的数据安全风险。数据安全成为了当前产业环境下各类组织机构共同关注的安全命题。

数据安全的管理需要基于以数据为中心的管理思路，从组织机构业务范围内的数据生命周期的角度出发，结合组织机构各类数据业务发展后所体现出来的安全需求，开展数据安全保障。数据安全能力成熟度模型（以下简称“模型”）关注于组织机构开展数据安全工作时应具备的数据安全能力，提出对组织机构的数据安全能力成熟度的分级评估方法，来衡量组织机构的数据安全能力，促进组织机构了解并提升自身的数据安全水平，促进数据在组织机构之间的交换与共享，发挥数据的价值。

# 信息安全技术　数据安全能力成熟度模型

## 1　范围

本标准基于大数据环境下电子化数据在组织机构业务场景中的数据生命周期，从组织建设、制度流程、技术工具以及人员能力四个方面构建了数据安全过程的规范性数据安全能力成熟度分级模型及其评估方法。

本标准适用于组织机构数据安全能力的自身评估，也适用于第三方机构对组织机构的数据安全保障能力进行评估。

## 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，仅所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 25069—2010 信息安全技术　术语

GB/T 20261—2006 信息安全技术 系统安全工程-能力成熟度模型

GB/T AAAAA—AAAA 信息技术 大数据 术语

GB/T BBBBB—BBBB 信息技术 大数据参考框架

GB/T CCCCC—CCCC 信息安全技术 个人信息安全规范

GB/T DDDDD—DDDD 信息安全技术 大数据服务安全能力要求

GB/T EEEEE—EEEE 信息技术 数据管理能力成熟度模型

## 3　术语、定义和缩略语

GB/T 25069—2010中界定的以及下列术语和定义适用于本文件。

### 3.1　术语和定义

3.1.1

**数据安全　data security**

以数据为中心的安全，保护数据的可用性、完整性和机密性。

注：本标准是从组织建设、制度流程、技术工具以及人员能力等方面对组织机构的数据进行安全保护。

3.1.2

**数据安全能力　data security capability**

组织机构在组织建设、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能力。

3.1.3

**成熟度　maturity**

对一个组织的有条理的持续改进能力的度量，对实现特定过程的连续性、可持续性、有效性和可信度的度量。

3.1.4

**成熟度模型 maturity model**

对一个组织机构的成熟度进行度量的模型，包括一系列的代表能力和进展的特征、属性、指示或是模式。模型的内容通常是最佳实践的举例说明。成熟度模型提供一个组织机构衡量其当前的实践、流程、方法的能力水平的基准，并设置提升的目标和优先级。当一个模型被广泛应用于某个特定的行业，这个行业可以基于模型，来评估本行业的组织机构的成熟度等级。

3.1.5

**组织机构 organization**

安排了责任、权利和关系的一组人员和设施。

3.1.6

**安全过程域 security process area**

实现同一安全目标的一系列数据安全相关活动、过程的集合。

3.1.7

**数据脱敏 data desensitization**

通过模糊化等方法对原始数据的处理，达到屏蔽敏感信息的一种数据保护方法。

3.1.8

**数据产品 data product**

直接或间接使用数据的产品，包括但不限于能访问原始数据，提供数据计算、数据存储、数据交换、数据分析、数据挖掘、数据展示等应用的软件产品。

3.1.9

**数据加工 data processing**

对原始数据进行抽取、转换、加载的过程；包括开发数据产品或数据分析。

3.1.10

**合规 compliance**

对数据所适用的法律法规的遵循。

## 3.2 缩略语

下列缩略语适用于本标准：

| | |
|---|---|
| ACL | 访问控制列表（Access Control List） |
| CMM | 能力成熟度模型（Capability Maturity Model） |
| DDOS | 分布式拒绝服务（Distributed Denial of Service） |
| DLP | 数据防泄漏（Data Loss Prevetion） |
| TLS | 传输层安全（Transport Layer Security） |
| SSL | 安全套接层（Secure Sockets Layer） |

# 4 数据安全能力成熟度模型架构

## 4.1 模型架构

本标准借鉴能力成熟度模型（CMM）的思想，以CMM的通用实践来衡量能力成熟度等级，以《信息安全技术 大数据服务安全能力要求》中的安全要求为基础，指导组织机构如何持续达到所对应的安全要求。数据安全能力成熟度模型的模型架构由以下三方面构成（如图1所示）：

——数据生命周期安全：围绕数据生命周期，提炼出大数据环境下，以数据为中心，针对数据生命周期各阶段建立的相关数据安全过程域体系。

——安全能力维度：明确组织机构在各数据安全领域所需要具备的能力维度，明确为制度流程、人员能力、组织建设和技术工具四个关键能力的维度。

——能力成熟度等级：基于统一的分级标准，细化组织机构在各数据安全过程域的 5 个级别的能力成熟度分级要求。

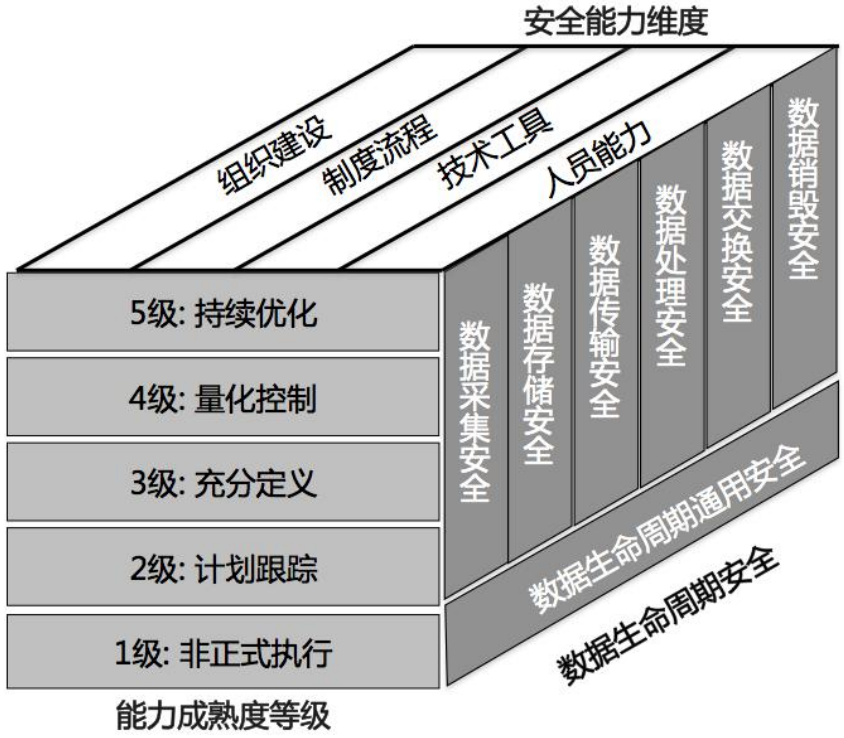


图 1　数据安全能力成熟度模型架构

对于图1的模型架构的说明如下：

1）基于电子数据在组织机构内的数据生命周期，明确定义各阶段特定的数据安全过程域和数据生命周期通用的安全过程域。各阶段特定的数据安全过程域，包括数据采集、数据存储、数据传输、数据处理、数据交换和数据销毁这六个阶段中，各阶段特定的数据安全过程域。数据生命周期通用的安全过程域，是与各个生命周期都相关的，通用的数据安全过程域，比如策略与规程、合规性管理等方面。

2）本标准对组织机构的数据安全保障能力的成熟度的分级评估，是基于各成熟度等级下的数据安全能力通用实践所定义的分级评估方法，对各阶段特定的数据安全基本实践和数据生命周期通用的安全基本实践的实现的成熟度等级进行评估。

## 4.2　数据生命周期安全

### 4.2.1　数据生命周期

基于大数据环境下数据在组织机构业务中的流转情况，定义了数据生命周期的6个阶段，具体各阶段的定义如下：

——数据采集：指新的数据产生或现有数据内容发生显著改变或更新的阶段。对于组织机构而言，数据的采集既包含在组织机构内部系统中生成的数据也包含组织机构从外部采集的数据。

——数据存储：指非动态数据以任何数字格式进行物理存储的阶段。

——数据处理：指组织机构在内部针对动态数据进行的一系列活动的组合。

——数据传输：指数据在组织机构内部从一个实体通过网络流动到另一个实体的过程。

——数据交换：指数据经由组织机构内部与外部组织机构及个人交互过程中提供数据的阶段。

——数据销毁：指通过对数据及数据的存储介质通过相应的操作手段，使数据彻底丢失且无法通过任何手段恢复的过程。

特定的数据所经历的生命周期由实际的业务场景所决定，并非所有的数据都会完整的经历六个阶段。

### 4.2.2 数据安全过程域体系

安全过程域体系覆盖数据生命周期的六个阶段，包含各生命周期阶段通用的安全过程域和各生命周期阶段下的安全过程域，如图2所示。


图 2 数据安全过程域体系

## 4.3 安全能力维度

### 4.3.1 能力构成

通过对各项安全过程所需具备安全能力的量化，可供组织机构评估每项安全过程的实现能力。安全能力从组织建设、制度流程、技术工具及人员能力四个维度展开。

——组织建设：数据安全组织机构的架构建立、职责分配和沟通协作。

——制度流程：组织机构关键数据安全领域的制度规范和流程落地建设。

——技术工具：通过技术手段和产品工具固化安全要求或自动化实现安全工作。

——人员能力：执行数据安全工作的人员的意识及专业能力。

### 4.3.2 组织建设

从承担数据安全工作的组织机构建设应具备的能力出发，从以下方面进行能力的级别区分：

——数据安全组织架构对组织业务的适用性；

——数据安全组织机构承担的工作职责的明确性；

——数据安全组织机构运作、沟通协调的有效性。

### 4.3.3 制度流程

从组织机构在数据安全层面的制度流程建设，以及制度流程的执行情况出发，从以下维度进行能力的级别区分：

——数据生命周期关键控制节点授权审批流程的明确性；
——相关流程制度的制定、发布、修订的规范性；
——安全要求及流程落地执行的一致性和有效性。

#### 4.3.4 技术工具

从组织机构用于开展数据安全工作的安全技术、应用系统和自动化工具出发，从以下维度进行能力的级别区分：

——数据安全技术在数据全生命周期过程中的利用情况，针对数据全生命周期安全风险的检测及响应能力；
——利用技术工具对数据安全工作的自动化支持能力，对数据安全制度流程的固化执行能力。

#### 4.3.5 人员能力

从组织机构内部承担数据安全工作的人员应具备的能力出发，从以下维度进行能力的级别区分：

——数据安全人员所具备的数据安全能力是否能够满足复合型能力要求(对数据相关业务的理解力以及专业安全能力)；
——数据安全人员的数据安全意识以及关键数据安全岗位员工的数据安全能力的培养。

### 4.4 成熟度等级定义

组织机构的数据安全能力成熟度模型具有 5 个成熟度等级，成熟度等级的定义如下：

——等级 1（非正式执行），是指具备随机、无序、被动的安全过程；
——等级 2（计划跟踪），是指具备主动、非体系化的安全过程；
——等级 3（充分定义），是指具备正式的规范的安全过程；
——等级 4（量化控制），是指安全过程可量化；
——等级 5（持续优化），是指安全过程可持续优化。

## 5 数据安全能力通用实践

### 5.1 能力级别 1—非正式执行

#### 5.1.1 能力等级描述

在这一级别，数据安全过程域的基本实践通常被执行。但基本实践的执行可能未经严格的计划和跟踪，而是基于个人的知识和努力。组织机构内的个人可标识出一个数据安全过程应被执行，并同意这个数据安全过程会在需要时执行。

该能力级别包含如下公共特征：

- 公共特征1.1 — 执行基本实践。

#### 5.1.2 公共特征 1.1 — 执行基本实践

##### 5.1.2.1 公共特征描述

此公共特征的通用实践只是保证过程域的基本实践以某种方式执行。但是，数据安全管理的一致性、性能和质量会因缺乏适当控制而存在极大的差异。

组织机构在数据安全过程域未有效的执行相关工作，仅在部分业务场景中/项目执行过程中根据临时的需求执行了相关工作，却未形成成熟的机制保证相关工作的持续有效进行，执行相关工作的人员能力也未得到有效的保障。所执行的过程可称为“非正式过程”。

#### 5.1.2.2 组织建设

未针对数据安全过程域的工作开展建立数据安全相关的团队/岗位和职责。

#### 5.1.2.3 制度流程

未建立与数据安全过程域相关的数据安全工作相关的制度流程，数据安全工作的开展多为对特定业务需求的响应而触发。

#### 5.1.2.4 技术工具

未部署技术工具以固化数据安全制度流程和提升数据安全能力。

#### 5.1.2.5 人员能力

未安排具备数据安全过程域相关知识背景的人参与到数据安全保障工作中。

### 5.2 能力级别 2—计划跟踪

在这一级别上，过程域基本实践的执行是经计划并被跟踪的，并对实践情况进行验证。数据安全管理应符合指定的标准和需求。通过测量来跟踪过程域的执行情况，因此，使组织机构能够基于实际实践活动进行管理。与非正式实践级别间的主要区别是过程实践被计划和管理。

该能力级别包含如下公共特征：

- 公共特征2.1 — 规划执行；
- 公共特征2.2 — 规范化执行；
- 公共特征2.3 — 验证执行；
- 公共特征2.4 — 跟踪执行。

#### 5.2.1 公共特征 2.1 — 规划执行

##### 5.2.1.1 公共特征描述

该公共特征的基本实践集中在过程域以及相关的基本实践执行的规划方面，因而涉及到过程文档的编制，过程工具的提供，过程实践的计划，规划执行的培训，过程资源的分配以及过程执行的责任分配。这些通用实践为规范化的过程执行提供了最根本的基础。

##### 5.2.1.2 组织建设

基于数据安全过程域的内容，规划关键数据安全管理的团队/岗位所需要的任务和责任，该团队/岗位主要负责对数据安全过程域中的关键安全管理规则的制定。任务和责任应规定到，包括内部、外部的和过程实践相关的所有相关方。

##### 5.2.1.3 制度流程

以数据为中心建立数据安全制度流程，并将数据安全制度流程形成标准化文档，并通过技术工具进行固化，使制度流程按照设计的方式执行。在此模型中，一个组织机构或一个项目中的过程无需与过程域一一对应。因此，覆盖一个过程域的过程可能可以以不止一种方式进行描述（例如以政策、标准等方式），一个过程描述可能包含不止一个过程域。

对数据安全制度流程的实践进行规划，和对数据安全工程和项目类的过程域规划可以按照项目计划的形式存在，而组织类的计划可以在组织机构层面上进行。

#### 5.2.1.4 技术工具

规划为执行数据安全过程域基本实践所需要的技术工具，来确保数据安全过程的执行。

为支持数据安全过程域的规划执行提供适当的工具。

#### 5.2.1.5 人员能力

为执行数据安全过程域基本实践规划充分的人力资源，分配其所需要的任务和责任，规划适当的培训，来确保过程的执行。

### 5.2.2 公共特征 2.2 — 规范化执行

#### 5.2.2.1 公共特征描述

该公共特征的通用实践注重于对过程实践的控制程度，需要使用过程执行计划、执行基于标准和程序的过程、对数据安全过程实施配置管理等。这些通用实践构成了验证数据安全过程执行的重要基础。

#### 5.2.2.2 组织建设

基于数据安全过程域的内容，分配在数据安全过程域中所涉及的承担关键数据安全管理职责的团队/岗位，该团队/岗位主要负责对数据安全过程域中的关键安全管理规则的落实。

#### 5.2.2.3 制度流程

针对该数据安全过程域中的关键的风险点提出了相应的安全要求，并将相应的要求以制度流程的形式进行了文档化。

对数据安全制度流程进行规范化执行，在执行过程域中，使用文档化的计划、标准指导实践。基于过程描述执行的过程称为“描述的过程”。

将数据安全制度流程实施配置管理，进行版本控制和/或变更控制。配置管理可视项目具体情况，组织机构可采用工具和/或人工方式。配置管理应提前做好规划。

#### 5.2.2.4 技术工具

根据行业内对相关数据安全过程域的技术产品的普及度，以及组织机构内实现自动化安全控制的可行性，组织机构已经优先采用了普及度较高的技术工具或执行了可行度较高的自动化安全控制。

#### 5.2.2.5 人员能力

从事数据安全过程域相关工作的人员具备对该数据安全过程域的关键风险的安全管理的背景知识和规范化执行数据安全过程的能力。

### 5.2.3 公共特征 2.3 — 验证执行

#### 5.2.3.1 公共特征描述

该公共特征的通用实践注重于确认过程按预定的方式执行。因此这个通用实践涉及到验证执行过程与可应用的计划是一致的，以及对数据安全过程的审计。这些通用实践构成了跟踪过程实践能力的重要基础。

#### 5.2.3.2 组织建设

基于数据安全过程域的内容，分析在数据安全过程域中所涉及的承担关键数据安全管理职责的团队/岗位，该团队/岗位主要负责对数据安全过程域中的关键安全管理规则的制定。

验证组织机构的团队/岗位与可用标准、需求及测量目标的一致性。对于组织建设的验证过程和审计活动应在计划中进行定义。

#### 5.2.3.3 制度流程

验证制度流程与可用标准、需求及测量目标的一致性。对于制度流程的验证过程和审计活动应在计划中进行定义。

#### 5.2.3.4 技术工具

验证支撑数据安全过程的技术工具与可用标准、需求及测量目标的一致性。对于技术工具的验证过程和审计活动应在计划中进行定义。

#### 5.2.3.5 人员能力

验证人员能力与可用标准、需求及测量目标的一致性。对于人员能力的验证过程和审计活动应在计划中进行定义。

### 5.2.4 公共特征 2.4 — 跟踪执行

#### 5.2.4.1 公共特征描述

该公共特征的通用实践注重于控制数据安全项目进展的能力。因此，该过程通过可测量的计划跟踪过程执行，当过程实践与计划产生重大偏离时采取修正行动。这些通用实践形成了达到充分定义过程能力的根本基础。

#### 5.2.4.2 组织建设

对数据安全工作相关的组织建设定期进行跟踪，通过测量来检查跟踪数据安全组织建设工作执行的状态，并建立对项目级别的组织建设测量的历史记录。

当数据安全组织机构与计划的数据安全组织机构之间有重大差别时适当地采取修正措施。进展可能由于估算的不精确、实践受外部因素的影响、作为计划基础的需求变动而与计划发生偏离。修正措施可能包括改变组织架构与职责，改变计划，或二者兼有。

#### 5.2.4.3 制度流程

对数据安全工作相关的制度流程定期进行跟踪，通过测量来检查跟踪数据安全制度流程工作执行的状态，并建立对制度流程的测量历史记录。

当数据安全制度流程与计划的数据安全制度流程间有重大差别时适当地采取修正措施。进展可能由于估算的不精确、实践受外部因素的影响、作为计划基础的需求变动而与计划发生偏离。修正措施可能包括改变制度流程，改变计划，或二者兼有。

#### 5.2.4.4 技术工具

对数据安全工作相关的技术工具定期进行跟踪，通过测量来检查跟踪数据安全技术工具的状态，并建立对技术工具的测量历史记录。

当技术工具与计划执行的效果有重大差别时适当地采取修正措施。进展可能由于估算的不精确、实践受外部因素的影响、作为计划基础的需求变动而与计划发生偏离。修正措施可能包括改变技术工具，改变计划，或二者兼有。

#### 5.2.4.5 人员能力

对数据安全工作相关的人员能力定期进行跟踪，通过测量来检查跟踪数据安全人员能力的状态，并建立对人员能力的测量历史记录。

当数据安全人员能力与计划的人员能力间有重大差别时适当地采取修正措施。进展可能由于估算的不精确、实践受外部因素的影响、作为计划基础的需求变动而与计划发生偏离。修正措施可能包括改变人员能力，改变计划，或二者兼有。

### 5.3 能力级别 3 — 充分定义

在这一级别，基本实践按照充分定义的过程执行。充分定义的过程是依据对文档化的标准过程进行裁剪并经批准的过程版本。这一过程与计划跟踪级的主要区别在于利用组织机构范围内的过程标准来管理和规划。

该能力级别包括以下公共特征：

- 公共特征 3.1 — 定义标准过程；
- 公共特征 3.2 — 执行已定义的过程；
- 公共特征 3.3 — 协调安全实践。

#### 5.3.1 公共特征— 定义标准过程

##### 5.3.1.1 公共特征

该公共特征的通用实践注重于组织机构标准过程的制度化。过程制度化的起因和基础可能是一个或多个相似过程在特定项目中的成功应用。一个组织机构的标准过程可能需要适合特定环境的使用，所以也应考虑到如何进行裁剪。因此，要为组织机构定义标准化的过程文档，要为满足特定用途对标准过程进行裁剪。这些通用过程形成了执行已定义过程必要的基础。

##### 5.3.1.2 组织建设

组织机构设立了实体或虚拟的团队，该团队主要负责针对该数据安全域建立有效的安全保护机制，包括但不限于建立组织机构统一的安全管理策略、制度和流程，并制定并面向组织机构范围内提供整体的技术标准解决方案。

该团队与数据安全过程域相关的部门（如业务部门、法律部门等）共同合作，建立有效的沟通和推进机制。

该团队已明确了数据安全的组织机构和岗位，数据安全人员的角色及其职责分配，并建立有效的工作考核机制。

##### 5.3.1.3 制度流程

对数据安全过程域进行数据安全风险评估，并参考相关的安全管理体系的方法论，建立了适应于组织机构自身在数据安全过程域的标准制度流程。

建立数据安全域的标准制度流程，包括但不限于与组织机构结构和数据业务相一致的安全策略、具有明确管控要求的制度规范、用于相关管控要求落地的流程、指导整体工作执行的实施指南。

组织机构针对该数据安全过程域的制度流程建立标准的培训和宣传方案，实现对与该数据安全过程域相关的团队和人员在对制度流程的理解上的一致性。

#### 5.3.1.4 技术工具

建立数据安全过程域相关的在线化平台固化并记录相关的流程，在组织机构内部建设、部署数据安全技术产品，强化安全控制。

其中，与数据安全过程域强关联的技术产品包含关键的产品功能，组织机构内基于具体的业务场景实现了对数据安全技术产品的有效运营，以保证产品功能对组织机构的业务场景的适应性。

#### 5.3.1.5 人员能力

从事数据安全工作的人员具备数据安全标准资质，具备在数据安全领域的工作经验，能够充分理解组织机构在该数据安全过程域的安全风险并具备集合具体的业务场景制定风险改进方案的能力。

### 5.3.2 公共特征 3.2 — 执行已定义过程

#### 5.3.2.1 公共特征描述

该公共特征注重于充分定义过程的可重复执行。因此提出了已定义过程的使用，针对有缺陷的过程结果和工作产品的核查，过程执行及其结果数据的使用。该通用实践构成了协调安全实践的重要基础。

#### 5.3.2.2 组织建设

组织机构设立了负责针对该数据安全域执行进行有效安全保护的实体或虚拟的团队。

该团队与数据安全过程域相关的部门（如业务部门、法律部门等）共同合作，建立有效的沟通和推进机制，实现数据安全要求和技术落地方案在数据安全过程域相关场景下的有效推行。

该团队已明确了相关人员在该数据安全过程域下的专职职责，建立执行缺陷复查的检查工作的考核机制。

#### 5.3.2.3 制度流程

组织机构针对该数据安全过程域的制度流程建立了有效的培训和宣传方案，实现对与该数据安全过程域相关的团队和人员在对制度流程的理解上的一致性。使用充分定义的过程，并建立专门的缺陷复查过程域，针对过程域的适当工作产品进行缺陷复查。

#### 5.3.2.4 技术工具

针对该数据安全过程域中的安全管理要求，一方面建立相应的在线化平台固化并记录相关的流程，另一方面结合行业内的优秀产品方案在组织机构内部建设、部署相应的技术产品，强化相应的安全控制。

使用技术工具收集测量数据，得到更积极的应用并且为下一级的定量管理奠定了基础。

#### 5.3.2.5 人员能力

从事数据安全工作的人员具备数据安全标准资质，具备在数据安全领域的工作经验，能够有效执行已定义的数据安全过程。

从事数据安全工作的人员能够充分理解组织机构在该数据安全过程域的安全风险，具备集合具体的业务场景制定风险改进方案，并执行已制定的风险改进方案的能力。

### 5.3.3 公共特征 3.3—协调实践

#### 5.3.3.1 公共特征描述

此公共特征侧重于单个业务系统和组织活动的协调。许多重大活动都是由业务系统中的不同工作组和代表业务系统的组织服务组共同完成的。缺乏协调将会导致数据安全风险和不可比的结果。因此应确定业务系统内、各业务系统之间、组织机构外部活动的协调机制。这些通用实践是获得定量控制过程能力的必要基础。

#### 5.3.3.2 组织建设

数据安全的组织机构能够协调业务系统内、组织机构的不同业务系统之间，以及与组织机构外部之间的标准执行实践，保证数据安全组织建设相关标准的统一执行。

#### 5.3.3.3 制度流程

数据安全的制度流程能够协调业务系统内、组织机构的不同业务系统之间，以及与组织机构外部之间的标准执行实践，保证数据安全制度流程相关标准的统一执行。

#### 5.3.3.4 技术工具

数据安全的技术工具能够协调业务系统内、组织机构的不同业务系统之间，以及与组织机构外部之间的标准执行实践。保证数据安全过程域中技术工具的安全管理标准统一执行。

#### 5.3.3.5 人员能力

数据安全人员能够协调项目组内、组织机构的不同项目组之间，以及与组织机构外部之间的标准执行实践。保证数据安全过程域中人员能力相关资质管理标准的统一执行。

### 5.4 能力级别 4 — 量化控制

这个级别收集、分析执行的详细测量。这将获得对过程能力和改进能力的量化理解以预测执行情况。这个级别执行的管理是客观的，数据安全管理的质量是量化的。这一级与充分定义级的主要区别在于定义的过程是定量的理解和控制。

该能力级别包括如下公共特征：

- 公共特征 4.1 — 建立可测的安全目标；
- 公共特征 4.2 — 客观地管理执行。

### 5.4.1 公共特征 4.1 — 建立可测的安全目标

#### 5.4.1.1 公共特征描述

该公共特征的通用实践侧重于为组织机构的数据安全建立可测量目标。因此这个公共特征提出了安全目标的建立。这些通用实践为客观地执行管理提供了必要的基础。

#### 5.4.1.2 组织建设

结合组织机构战略安全目标、业务系统的特定要求和优先级或业务策略，将安全目标分解落实到数据安全数据安全相关的团队/岗位的职责中，以利于安全目标的量化可测量、可执行。

#### 5.4.1.3 制度流程

量化地确定已定义的过程，测量活动要被嵌入到过程定义中。建立与数据安全过程域相关的数据安全工作相关的制度流程，数据安全工作的开展多为对特定业务需求的响应而触发。

#### 5.4.1.4 技术工具

根据定量的安全目标，对技术工具提出相应的功能和性能需求。在已有的技术工具的基础上实现对关键数据安全能力的量化培训和提升。在已有的该数据安全过程域的安全技术产品的基础上，进一步结合组织机构具体的业务场景，对安全技术产品的功能和设置进行更为细致化的管理，从而实现产品能力上的更加细化的量化安全控制。

#### 5.4.1.5 人员能力

关键岗位的数据安全人员具备较高的数据安全能力，能够在理解组织机构整体数据安全目标的基础上考虑负责的数据安全过程领域的安全工作开展方式。

### 5.4.2 公共特征 4.2 — 客观地管理执行

#### 5.4.2.1 公共特征描述

该公共特征的通用实践侧重于确定过程能力的量化测量并使用量化测量来管理这一过程。这个公共特征提出了量化地确定过程能力和以量化测量作为修正行动的基础。这些通用实践构成了获得持续改进能力的必要基础。

#### 5.4.2.2 组织建设

组织机构应明确进行定量执行的工作要求，在工作团队中设置负责数据收集、存储和分析的角色和人员，提供相应的资源，从而在工作中能够客观地监督过程的执行。

#### 5.4.2.3 制度流程

在过程执行中收集测量数据，对各项工作的执行情况及其效果进行客观的度量，为过程的持续改进提供决策依据。

当过程未按定义过程能力执行时，适当地采取修正行动。基于对过程能力的理解，识别出现偏差的原因，并制定出适当的纠正、预防措施，提出何时和采取何种修正行动。

针对组织机构在该数据安全过程域的制度流程进一步细化，针对所适应的关键业务场景基于组织机构统一的制度流程细化成相应的管理细则，从而提升其可落地性。制度流程的细化主要由承担数据安全职责的具体业务团队来负责并在该团队范围内进行发布和推广，例如基于组织机构制定的数据对外交换的原则，各业务团队可基于其相关的数据交换的业务场景中所涉及的对外交换的数据，制定出详细的适用于该团队业务场景的对外数据交换的安全细则。

组织机构进一步关注制度流程的执行效果，从安全要求、流程执行的有效性方面进行持续的跟踪和效果度量，从而反馈到相关制度流程的内容修订上。

#### 5.4.2.4 技术工具

提供技术工具支持数据的采集、存储、分析和管理等工作。

#### 5.4.2.5 人员能力

关键岗位的数据安全人员具备客观地管理执行的意识和能力，自觉地根据制度流程要求，采用技术工具进行数据的采集和分析。

## 5.5 能力级别 5 — 持续优化

在这个级别上，基于组织机构的商务目标并针对过程的有效性和执行效率建立量化执行目标。通过执行已定义过程和有创建的新概念、新技术的量化反馈来保证对这些目标进行持续过程改进。这一级与定量控制级的主要区别在于已定义的过程和标准过程基于对这些过程变化效果的量化理解，进行连续调整和改进。

安全过程可持续优化，实时跟踪行业的最佳实践和业务的最新动向，制度流程和技术工具持续调整以更好适应业务发展，沉淀下来的数据安全最佳实践能推广至行业供其他组织机构借鉴。

该能力级别包括如下公共特征：

- 公共特征 5.1 — 改进组织能力；
- 公共特征 5.2 — 改进过程有效性。

#### 5.5.1 公共特征 5.1 — 改进组织能力

该公共特征的通用实践注重于在整个组织机构范围内标准过程的使用进行比较和在这些不同使用之间进行比较。当这些过程被使用时，寻找改进标准过程的机会，分析产生的缺陷以标识对标准过程的其它可能改进。因此，这个公共特征对过程的有效性建立了目标、标识对标准过程的改进以及分析对标准过程的可能变更。这些通用实践构成了改进过程有效性的必要基础。

##### 5.5.1.1 组织建设

组织架构的设置与国际上领先的数据安全管理理念符合，且能更好适应业务发展的战略规划，具备及时调整的以促进业务发展的能力。

##### 5.5.1.2 制度流程

为改进过程有效性，根据组织机构的业务目标和当前过程能力建立量化目标。实时跟踪数据安全管理领域的最佳实践和业务的最新动向，预先判断业务在数据安全领域所面临的风险，并在制度流程上进行持续性的优化。通过改变组织机构的标准过程族连续地改进过程，从而提高过程有效性。

##### 5.5.1.3 技术工具

基于数据安全技术的最新进展以及组织机构沉淀下来的数据安全技术能力，结合业务发展的实际情况引入先进的技术工具提升数据安全控制的有效性。

##### 5.5.1.4 人员能力

密切关注国内外最新的数据安全标准及规范，加强行业领域内的专家交流，结合本组织机构的特点合理优化并组织机构内的数据安全解决方案。

#### 5.5.2 公共特征 5.2 — 改进过程有效性

该公共特征的通用实践注重于制定处于连续受控改进状态下的标准过程。因此这个公共特征提出消除标准过程产生缺陷的原因和持续改进的标准过程。

##### 5.5.2.1 组织建设

组织架构的设置与国际上领先的数据安全管理理念符合，且能更好适应业务发展的战略规划，具备及时调整的以促进业务发展的能力。

##### 5.5.2.2 制度流程

为改进过程有效性，根据组织机构的业务目标和当前过程能力建立量化目标。实时跟踪数据安全管理领域的最佳实践和业务的最新动向，预先判断业务在数据安全领域所面临的风险，并在制度流程上进行持续性的优化。执行缺陷的因果分析。有选择的消除已定义过程中缺陷产生的原因。在这个公共实践中，意味着公共原因和特殊原因的变化，并且每一种缺陷都会导致采取不同的行动。

#### 5.5.2.3 技术工具

基于数据安全技术的最新进展以及组织机构沉淀下来的数据安全技术能力，结合业务发展的实际情况引入先进的技术工具提升数据安全控制的有效性。

#### 5.5.2.4 人员能力

密切关注国内外最新的数据安全标准及规范，加强行业领域内的专家交流，结合本组织机构的特点合理优化并组织机构内的数据安全解决方案。

执行该过程的人员一般为参与分析的人员。这是一种事前和反复的因果分析活动。以前具有相似属性的项目缺陷可作为目标改进区。

## 6 数据生命周期通用的安全基本实践

### 6.1 策略与规程

#### 6.1.1 数据安全策略与规程

##### 6.1.1.1 数据安全过程域描述

通过建立组织机构整体的数据安全策略及规程，以实现对数据全生命周期的安全风险管控。

##### 6.1.1.2 数据安全能力基本实践

a) 组织建设：设立数据安全的团队/岗位负责组织机构的数据安全策略与规程的制定、修订和落地。（《要求》5.1.1 a）b)）

b) 制度流程：

1) 依据组织机构的业务战略，建立数据安全方针和目标，并基于此建立以数据生命周期为核心思想的数据安全制度体系，相关制度均从目的、范围、岗位、责任、管理层承诺、内外部协调及合规性方面提出明确的要求。（《要求》5.1.1 a）b））

2) 建立了数据安全策略与规程的分发流程，策略和规程均能被组织机构各部门、岗位和人员获取。（《要求》5.1.1 c） ）

3) 制定并实施与安全策略和规程相适应的大数据平台和大数据应用实施细则,包括外部数据资源整合、数据共享、数据发布等数据供应链安全管理细则、合同要求及审核机制。（《要求》5.1.1. d） ）

4) 建立策略及规程的评审、发布流程，并确定适当的频率和时机对策略和规范进行更新，以确保其持续的适宜性和有效性。（《要求》5.1.1 e）f） ）

c) 技术工具：建立了数据安全策略及规程管理的技术工具，通过该技术工具面向组织机构全体员工发布对策略及规范的解读材料，以便于策略规范的落地推进。（《要求》5.1.1 c） d））

d) 人员能力：

1) 负责数据安全顶层方针、策略制定的人员了解组织机构的业务发展目标，能够将数据安全工作目标和业务发展目标进行有机的结合。（《要求》5.1.1 a） 、5.1.2 a）b） ）

2) 负责数据安全策略与规程编写的人员掌握信息安全管理体系建设的知识，并具有专业的规范撰写能力。（《要求》5.1.1 a）、 b)、c)、d） ）

3) 负责数据安全策略及规范推广的人员能够对数据安全管理的方针、策略和制度规范进行准确解读，能够以员工和相关方易理解的方式通过培训等形式进行宣传。（《要求》5.1.1 c ））

## 6.2 数据与系统资产

### 6.2.1 数据资产

#### 6.2.1.1 数据安全过程域描述

通过建立针对组织机构数据资产的有效管理手段，从资产的类型、管理模式方面实现统一的管理标准。

#### 6.2.1.2 数据安全能力基本实践

a) 组织建设：设置数据安全的团队/岗位负责组织机构统一的数据资产管理工作，主要负责对数据资产管理的规范制定和落地推动，并由各业务团队的具体人员承担各业务范围内的数据资产管理工作。（《要求》5.2.1.1 a）b)c)d)e)）

b) 制度流程：

1) 制定数据资产的安全管理规范，明确数据资产的安全管理目标和安全原则，管理规范明确了数据资产的登记制度，定义了数据资产的数据管理者和安全管理者在组织机构中的角色定位和所应承担的职责，并提出数据资产的分类管理要求。（《要求》5.2.1.1 a）c））

2) 建立数据资产分类分级方法和操作指南，以及数据资产分类分级的变更审批流程和机制。（《要求》5.2.1.1 b））

3) 建立数据资产清单，明确数据资产管理范围和属性。（《要求》5.2.1.1 d））

4) 建立组织机构内部数据资产管理过程中需要数据管理者和安全管理者需要参与的审批流程，并清晰定期其在各流程中所承担的审批职责。（《要求》5.2.1.1 b））

5) 定期审核和更新数据资产安全管理相关的安全规范、操作细则。（《要求》5.2.1.1 e））

6) 依据数据资产和数据主体安全分级要求建立相应的标记策略、访问控制、数据加解密、数据脱敏等安全机制和管控措施。（《要求》5.2.1.2 a））

7) 建立组织机构业务所需的内外部数据资产的安全治理原则和数据资源整合规范。（《要求》5.2.1.2 b））

c) 技术工具：

1) 建立组织机构统一的数据资产管理平台，通过技术工具整体量化组织机构内部的数据资产情况，实现对数据资产的统一管理，包括但不限于标识数据的数据管理者和安全管理者，数据资产等级，数据资产数据量，各等级的数据资产的分布情况等信息，从而便于数据管理人员进行整体的数据资产现状统计。（《要求》5.2.1.2 c））

2) 量化数据管理者和安全管理者在相关数据安全流程中的参与情况，调整数据管理者和安全管理者的职责要求。（《要求》5.2.1.2 a））

d) 人员能力：具备对组织机构内部数据资产管理需求的理解，以及对数据资产所涉及业务范围的整体概念的理解，能够建立适用于组织机构业务实际情况的可落地的管理制度。（《要求》5.2.1.1 a）b)c)d)e)、《要求》5.2.1.2 a)b)c））

### 6.2.2 系统资产

#### 6.2.2.1 数据安全过程域描述

通过建立针对组织机构内部信息系统资产的有效管理手段，从资产的类型、管理模式方面实现统一的管理标准。

#### 6.2.2.2 数据安全能力基本实践

a) 组织建设：设置专门的团队/岗位负责组织机构统一的信息系统资产管理工作，主要负责对信息系统资产管理的规范制定和落地推动，并由各业务团队的具体人员承担各业务范围内的信息系统资产管理工作。（《要求》5.2.2.1 a）、b)、c)、d)、e)）

b) 制度流程：

1) 制定信息系统资产的安全管理制度，明确信息系统资产安全管理目标和安全原则、信息系统资产的全生命周期管理要求、资产登记要求和分类标记要求，并针对安全管理制度执行定期审核和更新。 （《要求》5.2.2.1 a）、e））

2) 建立信息系统资产建设和运营管理制度和机制，明确规划、设计、采购、开发、运行、维护及报废等资产管理过程的安全要求。（《要求》5.2.2.1 b））

3) 建立组织机构内的信息系统资产登记机制，形成整体的信息系统软硬件资产清单，明确系统资产安全责任主体及相关方，并及时更新系统资产相关信息。（《要求》5.2.2.1 c））

4) 建立和实施信息系统资产分类和标记规程，使资产标记易于填写和依附在相应的系统资产上。（《要求》5.2.2.1 d））

5) 建立信息系统资产更新、运营风险评估和供应链安全审查规程和制度。（《要求》5.2.2.2 b））

c) 技术工具：

1) 针对易通过技术工具执行资产登记、分类标记的信息系统，实现自动化的属性标识工作。（《要求》5.2.2.1 d））

2) 组织机构建立信息系统资产管理平台，能够通过技术工具整体量化组织机构内部的信息系统资产情况，包括但不限于整体的信息系统资产数量等信息，具备系统资产统一注册、管理和使用监控等能力，从而便于信息系统管理人员进行整体的信息系统资产现状统计。（《要求》5.2.2.2 a））

d) 人员能力：负责组织机构统一的信息系统资产管理工作的人员具备对组织机构内部信息系统资产管理需求的理解，以及对信息系统资产所涉及业务范围的整体概念的理解，能够建立适用于组织机构业务实际情况的可落地的管理制度。（《要求》5.2.2.1 a）、b）、c）、d）、e））

## 6.3 组织和人员管理

### 6.3.1 组织管理

#### 6.3.1.1 数据安全过程域描述

通过建立组织机构内部负责数据安全工作的职能部门及岗位，并明确职能部门及岗位承担的数据安全责任，防范人员管理过程中存在的安全风险。

#### 6.3.1.2 数据安全能力基本实践

a) 组织建设：

1) 基于组织机构的数据安全方针及策略，充分定义了组织机构内部正式的数据安全职能部门/岗位，数据安全的职能框架包括但不限于：（《要求》5.3.1.1 a）、c)）

- 数据安全规范及标准：负责组织机构内数据安全相关的规范制度和详细标准的制定，为组织机构数据安全相关工作的开展提供依据和要求。
- 数据安全技术及产品：负责组织机构内数据安全技术的应用、数据安全产品的开发和部署，建立整体的技术防护及应急保障体系。

- 数据安全监控及审计：负责建立组织机构内的数据安全风险管理体系，对数据全生命周期的安全风险进行审计，从风险的预防、发现、跟进等环节实现对风险的有效管理。
- 数据安全宣传与促进：负责面向组织机构内全体人员普及数据安全相关知识，通过多种形式推广数据安全的风险防范思路和方法，提高组织机构内全体人员的数据安全意识，促进数据安全工作的具体落地。
- 数据安全合作与交流：负责与监管机构进行持续的沟通，并在行业内交流数据安全的实践经验、开展相关合作以促进行业的整体发展。
- 信息系统安全管理：负责信息系统的安全规划、安全建设、安全运营和系统维护工作，实现基础信息系统的安全管理。

2) 组织机构层面建立数据安全领导小组，指定机构最高管理者或授权代表担任小组组长，并明确组长责任与权力。（《要求》5.3.1.1 b））

3) 职能岗位设计时考虑了职责分离的原则，并建立组织机构内部监督管理职能部门，对组织机构内部的数据安全管理的相关职能岗位的操作行为进行安全监督管理。（《要求》5.3.1.1 d））

4) 建立体系化的大数据安全管理机构，组织机构最高管理人员应作为大数据安全领导小组组长，且配备必要的管理人员和技术人员。（《要求》5.3.1.2 a））

5) 设置专职的大数据服务安全岗位，建立规范化的大数据服务安全保护、评估及考核专职队伍。（《要求》5.3.1.2 b））

b) 制度流程：

1) 制定数据安全职能的工作规范，以明确各职能岗位之间的协作关系，明确了各职能岗位的运行配合机制。（《要求》5.3.1.1 a））

2) 制定大数据安全追责制度，定期对责任部门和安全岗位组织安全检查，形成检查报告。（《要求》5.3.1.1 e））

c) 技术工具：在组织机构通过技术工具以公开信息且可查询的形式面向全员公布数据安全职能部门的组织架构。（《要求》5.3.1.1 a，5.3.1.2 a））

d) 人员能力：

1) 负责执行数据安全职能设置的人员能够明确组织机构的数据安全工作目标。（《要求》5.3.1.1 a））

2) 能够充分理解数据安全职能现状，并具备基于职能运作的效果有效调整职能设置的能力。（《要求》5.3.1.2 a）、b））

### 6.3.2 人员管理

#### 6.3.2.1 数据安全过程域描述

通过对人力资源管理过程中各环节的安全管理,有效降低对组织机构内部的员工和第三方员工的管理过程中存在的安全风险。

#### 6.3.2.2 数据安全能力基本实践

a) 组织建设：明确在人力资源管理过程中承担数据安全管理职责的岗位，该岗位负责对数据安全需求的分析及落地方案的制订和推进。（《要求》5.3.2.1 a）、b）、c）、d）、e）、f）、g））

b) 制度流程：

1) 制定人力资源安全策略，明确不同岗位人员在数据生命周期各阶段数据服务和系统服务相关的工作范畴和安全管控措施。（《要求》5.3.2.1 a））

2) 制定大数据服务人员招聘、录用、上岗、调岗、离岗、考核、选拔等人员安全管理制度，将数据安全相关的环节固化到涉及的人力资源流程中。制度中明确要求在录用重要岗位人员前对其进行背景调查，确保符合相关的法律、法规、合同和道德要求，并与所有涉及大数据服务岗位人员签订安全责任协议；明确大数据服务重要岗位的兼职和轮岗、权限分离、多人共管等安全管理要求；建立在岗人员安全责任奖惩管理机制，将员工在职期间在数据安全方面的义务和职责纳入人力资源激励和惩罚的范畴，并按照规定对造成大数据安全损失的人员给予相应的处理，记录并保存相关信息；在重要岗位人员调离或终止劳动合同时，与其签订保密协议。（《要求》5.3.2.1 b）、c）、d）、e）、g））

3) 制定第三方人员安全管理制度，对接触个人信息、重要数据等数据的人员进行审批和登记，并要求签署保密协议，定期对这些人员行为进行安全审查。（《要求》5.3.2.1 f））

4) 明确关键岗位人员背景调查范围，定期对关键岗位人员进行背景审查；对员工候选者的背景调查中也包含了对候选者的专业能力的调查。（《要求》5.3.2.2 a））

c) 技术工具：通过技术化手段将人力资源安全相关的流程通过系统平台自动化实现。（《要求》5.3.2.1 a）、b）、c）、d）、e）、f)、g））

d) 人员能力：

1) 负责人力资源安全管理的人员应充分理解人力资源管理流程中可对安全风险进行把控的环节。并通过培训、考试等手段提升全体人员数据安全意识水平。（《要求》5.3.2.1 a）、b）、c）、d）、e）、f)、g））

2) 明确关键岗位人员安全能力要求，并确定他们培训技能考核内容与考核指标，定期对关键岗位人员进行审查和能力考核。（《要求》5.3.2.2 b））

### 6.3.3 角色管理

#### 6.3.3.1 数据安全过程域描述

通过对大数据安全管理过程中各角色的安全管理,有效降低对组织机构内部的员工和第三方员工的管理过程中存在的安全风险。

#### 6.3.3.2 数据安全能力基本实践

a) 组织建设：明确在人力资源管理过程中承担数据安全管理职责的岗位，该岗位负责对数据安全需求的分析及落地方案的制订和推进。（《要求》5.3.3.1 a）、b)、c)）

b) 制度流程：

1) 建立大数据相关的安全角色，明确安全角色的分配策略和授权范围。（《要求》5.3.3.1 a））

2) 建立用户角色及角色权限冲突的定期审查机制，及时更新用户角色及角色权限授权信息。（《要求》5.3.3.1 b））

3) 明确大数据安全相关重要岗位及其角色安全要求，建立重要岗位角色清单和授权机制。（《要求》5.3.1.1 c））

4) 依照大数据业务需求和大数据系统架构建立分层的角色体系、职责分离等大数据业务安全角色管理机制。（《要求》5.3.3.2 a））

5) 建立用户应用上下文感知的角色启动、停用与禁用的动态管理策略、规程和机制。（《要求》5.3.3.2 b））

c) 技术工具：通过技术化手段将角色管理相关的规则与组织机构的身份认证管理平台进行联动，自动化实现相关安全控制。（《要求》5.3.3.1 a）、b)、c)）

d) 人员能力：负责角色管理的人员应充分理解角色管理流程中可对安全风险进行把控的环节,通过培训、考试等手段提升各角色人员数据安全意识水平。（《要求》5.3.3.1 a）、b)、c)）

#### 6.3.4 人员培训

##### 6.3.4.1 数据安全过程域描述

通过对人力培训管理过程中各环节的管理，有效提升组织机构内部的员工和第三方员工的数据安全意识和数据安全能力水平。

##### 6.3.4.2 数据安全能力基本实践

a) 组织建设：明确组织机构内部承担人员数据安全培训管理职责的岗位，该岗位负责对数据安全培训需求的分析及落地方案的制订和推进。（《要求》5.3.4.1 a）、 b）、c））

b) 制度流程：

1) 制定大数据安全岗位人员的安全培训计划，并对培训计划定期审核和更新。（《要求》5.3.4.1 a））

2) 制定大数据安全关键岗位转岗、岗位升级等相应的人员安全培训计划，并对培训计划定期审核和更新。 （《要求》5.3.4.1 b））

3) 按计划对相关人员开展数据安全培训，包括政策、法律、法规、标准等合规性培训，并对培训结果进行评价、记录和归档。 （《要求》5.3.4.1 c））

4) 根据不同的业数据各类业务场景下的数据安全培训计划和培训材料。（《要求》5.3.4.2 a））

c) 技术工具：

1) 通过技术化手段将数据安全人员培训相关的流程通过系统平台自动化实现。（《要求》5.3.4.1 a）、 b）、c））

2) 通过在线的人员培训管理平台，量化管理人员培训的效果。（《要求》5.3.4.1 a）、 b)、c）、5.3.4.2 a））

d) 人员能力：固化了针对员工、第三方人员进行数据安全能力培训的环节，通过培训、考试等手段提升全体人员数据安全能力水平。（《要求》5.3.4.1 a）、 b）、c）、5.3.4.2 a））

### 6.4 业务规划与管理

#### 6.4.1 战略规划

##### 6.4.1.1 数据安全过程域描述

通过建立组织层面大数据安全战略规划体系，保证大数据战略规划与组织机构的大数据业务规划相适应。

##### 6.4.1.2 数据安全能力基本实践

a) 组织建设：设立专门的大数据战略规划岗位，负责对制定组织机构整体的战略规划并推进阶段性的规划执行；同时，设立大数据安全战略规划评估小组，负责机构安全规划评估，确保大数据安全策略、安全目标和战略规划内容的合规性。（《要求》5.4.1.1 c））

b) 制度流程：

1) 依据机构大数据安全战略规划目标，制定大数据安全规划各阶段目标、任务和工作重点，并对战略规划目标和安全规划实施过程进行监督与控制。（《要求》5.4.1.1 b））

2) 建立大数据安全管理纲领性文件，包括但不限于：数据治理、数据质量、元数据，以及平台与应用安全相关的数据所有权、数据开放与共享等安全策略。（《要求》5.4.1.2 b））

3) 建立大数据安全规划动态调整制度，并通过信息化平台进行管理。（《要求》5.4.1.2 a））

c) 技术工具：

1) 建立组织机构统一的信息化平台对大数据安全战略规划面向组织机构内部全员进行发布，以该信息可被全员所知悉。（《要求》5.4.1.1 a）、b)、c））

2) 通过组织机构的信息化平台执行对大数据安全规划的动态管理。（《要求》5.4.1.2 a））

d) 人员能力：负责该项工作的人员均具有战略规划能力，并对组织机构的数据安全管理的业务需求有充分的理解，通过培训和宣传等手段实现各业务的数据管理人员对战略规划的一致性理解。（《要求》5.4.1.1 a）、b)、c））

### 6.4.2 需求分析

#### 6.4.2.1 数据安全过程域描述

通过建立针对组织机构业务的大数据安全需求分析体系，分析组织机构内大数据业务的安全需求。

#### 6.4.2.2 数据安全能力基本实践

a) 组织建设：针对开展大数据业务的团队均设立了对应的安全需求分析的岗位，负责在大数据业务规划阶段开展安全需求分析工作，确保安全需求的有效制定和规范化表达。（《要求》5.4.2.1 a）、b）、c）、d）、e））

b) 制度流程：

1) 建立大数据业务的安全需求分析的指南，明确安全需求分析工作需要依据国家法律、法规、标准与主管机构的政策规范要求，分析大数据业务所面临的安全合规性需求；依据组织机构的业务战略规划目标、大数据业务的目标和特定，分析大数据业务的安全需求；识别大数据业务面临的威胁和自身脆弱性，分析大数据业务的安全风险和应对措施需求；依据组织机构的业务战略规划，明确大数据业务安全需求和安全规划实施的优先级。(《要求》5.4.2.1 b）、c）、d）、e））

2) 使用数据驱动分析方法或安全需求工程思想进行大数据安全需求分析，确保大数据安全需求的有效制定和规范化表达。（《要求》5.4.2.2 a））

c) 技术工具：建立承载大数据业务的安全需求分析的平台，该平台记录所有的大数据业务的需求分析的申请、需求分析以及相关安全方案，以保证对所有的大数据业务的安全需求分析过程的有效追溯。（《要求》5.4.2.1 a）、b）、c）、d）、e））

d) 人员能力：负责该项工作的人员均具有需求分析挖掘能力，对组织机构的数据安全管理的业务场景有充分的理解，并通过培训实现各业务的需求分析人员对大数据安全需求分析标准的一致性理解。（《要求》5.4.2.1 a）、b）、c）、d）、e））

### 6.4.3 元数据安全

#### 6.4.3.1 数据安全过程域描述

通过建立组织机构的元数据管理体系，实现对组织机构内元数据的有效管理。

#### 6.4.3.2 数据安全能力基本实践

a) 组织建设：

1) 设立了固定的团队/岗位负责组织机构的统一元数据管理工作建立相应的原则并提供统一的技术工具，并由各业务的数据管理团队/岗位负责具体的元数据管理执行工作。(《要求》5.4.3.1 a）、b）、c）、d））

2) 定义了元数据管理的工作职责；进行了元数据管理的业务分配；设定了专职的元数据管理人员。（《要求》5.4.3.1 a）、b）、c）、d））

b) 制度流程：

1) 制定了组织机构的元数据管理的规范要求；满足了对元数据的制度流程的需求响应。

2) 建立大数据服务相关元数据及其管理规范，如数据域、字段类型、表结构、逻辑存储和物理存储结构及管理方式。（《要求》5.4.3.1 a））

3) 建立了大数据服务安全架构相应的安全元数据管理规范，如口令策略、权限列表、授权

策略。（《要求》5.4.3.1 b））

4) 建立了元数据访问控制策略，明确元数据管理角色及其授权控制机制。（《要求》5.4.3.1 c））

5) 建立了元数据操作审计制度，确保元数据操作的可追溯。（《要求》5.4.3.1 d））

6) 建立了大数据服务所涉及元数据安全管理纲领性文件，以及平台与应用安全相关的数据所有权、数据开放与共享等安全策略。（《要求》5.4.3.2 a））

7) 依据资产分类分级策略建立了元数据安全属性自动分级制度。（《要求》5.4.3.2 b））

8) 依据元数据安全属性建立标记策略规范和标记定义，依据元数据安全属性实现元数据标记管理机制。（《要求》5.4.3.2 c））

9) 建立大数据服务平台与应用安全相关的数据所有权、数据开放与共享等安全策略。

c) 技术工具：

1) 建立了组织机构统一的元数据管理平台，将各领域的元数据通过集中的平台面向组织机构内部提供，包括但不限于数据存储、数据计算、数据应用相关的元数据管理。（《要求》5.4.3.1 a））

2) 根据元数据安全管理规范和访问控制策略，实现了元数据管理角色及其授权控制的技术手段；（《要求》5.4.3.1 b）、c)）

3) 根据审计制度要求，采集元数据操作日志，实现了元数据操作的追溯技术。（《要求》5.4.3.1 d））

4) 基于元数据管理建立可视化的功能，在元数据管理平台上以数据标签的形式实现对数据的存储、访问、所属业务，以及字段级、表级、应用级的数据上下游关系等信息的量化管理，实现对元数据的统一管理。（《要求》5.4.3.2 a））

5) 实现了元数据安全属性自动分级。（《要求》5.4.3.2 b））

d) 人员能力：负责该项工作的人员均了解元数据管理的理论基础，并对组织机构的元数据管理的业务需求有充分的理解。通过培训实现各业务的数据管理人员对元数据管理工作标准的一致性理解。（《要求》5.4.3.1 a）、b）、c）、d），5.4.3.2 a）、b））

## 6.5 数据供应链管理

### 6.5.1 数据供应链

#### 6.5.1.1 数据安全过程域描述

通过建立组织机构的数据供应链管理机制，防范组织机构上下游的数据供应过程中的安全风险。

#### 6.5.1.2 数据安全能力基本实践

a) 组织建设：设置了组织机构整体的数据供应链管理团队，负责制定整体的数据供应链管理要求和解决方案。（《要求》5.5.1.1 a）、b）、c）、d）、e）、f））

b) 制度流程：

1) 制定了组织机构整体的数据供应链安全管理规范，定义数据供应链安全管理方针以明确数据供应链安全目标、原则和范围其中，并明确供应链上下游的责任和义务、与供应链上下游的合作协议的相关要求、以及组织机构内部的审核原则，确保数据供应链上下游对数据交换、使用和利用符合法律法规。其中，合作协议明确大数据服务数据供应链中数据的使用目的、供应方式、保密约定等。（《要求》5.5.1.1 a）、b）、c）、d））

2) 建立对数据供应链上下游的大数据服务提供者和大数据使用者的行为进行合规性审核的流程。（《要求》5.5.1.1 f））

3) 制定了数据供应链上下游数据活动安全风险和数据安全管理能力评估规范。（《要求》

5.5.1.2 a））

c) 技术工具：

1) 建立组织机构整体的数据供应链库，用于管理数据供应链目录和相关数据源数据字典，便于及时查看并更新组织机构上下游数据链路的整体情况，并用于事后追踪分析数据供应链上下游对法律法规的遵循情况。（《要求》5.5.1.1 e））

2) 基于对数据供应链的相关记录，建立对数据供应链上下游的大数据服务提供者和大数据使用者的行为进行合规性审核和分析工具。（《要求》5.5.1.1 e）、f））

3) 量化组织机构整体的数据供应链情况，对上下游数据供应的需求、对象和方式进行分类整理，以及时发现并跟进数据供应链管理过程中存在的潜在风险。（《要求》5.5.1.1 b））

d) 人员能力：负责该项过程的人员应具备对组织机构上下游数据供应链的整体了解，并具备推进供应链管理方案落地的能力。（《要求》5.5.1.1 a）、b）、c）、d）、e）、f）、5.5.1.2 a））

### 6.5.2 数据服务接口

#### 6.5.2.1 数据安全过程域描述

通过建立组织机构的数据服务接口管理机制，防范组织机构数据接口调用过程中的安全风险。

#### 6.5.2.2 数据安全能力基本实践

a) 组织建设：设定了对数据服务接口安全进行统一管理的团队，负责制定相应的安全规则并提供技术方案用于规则的推行。（《要求》5.5.2.1 a）、b）、c）、d））

b) 制度流程：

1) 制定数据服务接口安全控制策略,明确规定使用服务接口的安全限制和安全控制措施,如身份鉴别、授权策略、访问控制机制、签名、时间戳、安全协议等。（《要求》 5.5.2.1 a））

2) 建立数据服务接口安全规范，包括接口名称、接口参数、接口安全要求等。（《要求》5.5.2.1 b））

c) 技术工具：

1) 提供对数据服务接口的安全限制和安全控制措施，如身份鉴别、授权策略、访问控制机制、签名、时间戳、安全协议等，并对服务接口的参数进行限制/过滤，一旦发现异常会触发告警机制。（《要求》5.5.2.1 a）、b））

2) 统一收集数据服务接口的相关记录日志，并建立相应针对服务接口访问的防线的审计工具。（《要求》5.5.2.1 c））

3) 对大数据平台与应用内跨安全域间的接口调用采用安全通道、加密传输等安全机制。(《要求》5.5.2.1 d））

4) 建立服务接口安全监管技术机制，可以对接口访问进行必要的自动化监控和处理。(《要求》5.5.2.2 a））

5) 对接口访问进行必要的自动化监控和处理基础上，进行不同安全管理和工程过程的持续改进工作。（《要求》5.5.2.1 a）、b）、c）、d）、5.5.2.2 a））

d) 人员能力：具备对数据服务接口的相关业务使用场景理解能力和安全风险的评估能力。(《要求》5.5.2.1 a）、b）、c）、d）、5.5.2.2 a））

## 6.6 合规性管理

### 6.6.1 个人信息保护

#### 6.6.1.1 数据安全过程域描述

通过组织机构其业务所适用的法律法规要求，在相关业务环节和内部运营流程中开展个人信息保护工作，以实现对个人信息的全生命周期安全防护。

#### 6.6.1.2 数据安全能力基本实践

a) 组织建设：设立了组织机构统一负责个人信息保护的团队，该团队包含法律合规人员、安全人员、业务人员、技术人员，为组织机构提供统一的个人信息保护的规范要求、制定相应的数据安全解决方案并推进其在组织机构整体范围内的落地。（《要求》5.6.1.1 a）、5.6.1.2 a））

b) 制度流程：

1) 依据《GB/T AAAAA—AAAA 信息安全技术 个人信息安全规范》的要求，建立组织机构统一的个人信息保护的制度规范。（《要求》5.6.1.1 a））

2) 该制度规范中明确了组织机构内部的个人信息保护的组织构成、职责和沟通机制，定义个人信息保护的原则，并围绕个人信息的收集、保存、使用、委托处理、共享、转让、公开披露制定可落地的规范要求，建立个人信息安全事件的处理机制。（《要求》5.6.1.2 a））

3) 基于组织机构内部各类业务场景所涉及的针对个人信息的不同的安全风险，在组织机构整体的个人信息制度规范的要求下建立详细的指导细则。（《要求》5.6.1.1 a））

4) 针对组织机构内部因业务架构、组织职能调整而引发的各类应用、设备下线环节，在下线流程中建立个人信息的跟进处理机制，实现对应用及设备中存储的个人信息的妥善转移、转存或销毁。（《要求》5.6.1.2 a））

c) 技术工具：

1) 采取必要的技术手段，包括但不限于针对个人信息在线采集的自动化控制以及在个人信息处理的相关安全控制工具等。（《要求》5.6.1.2 a））

2) 建立组织机构内部实现个人信息保护的整体安全技术方案，通过对组织机构内部的个人信息识别和溯源建立个人信息库管理，通过对个人信息的生命周期监控实现对合规现状全景的把控，通过技术手段实现对数据处理过程中的匿名化、去标识化、差分隐私保护、聚合风险分析。（《要求》5.6.1.2 b）、c））

3) 针对个人信息保护的技术手段如去标识有效性等，建立有效的评价机制，保证相关效果的量化管理。（《要求》5.6.1.2 d））

d) 人员能力：充分理解个人信息保护的标准，并具备基于标准要求制定解决方案的能力，并在组织机构内部针对个人信息保护的制度规范开展了针对全体员工的培训工作，以保证组织机构整体对合规工作开展要求的一致性理解。（《要求》5.6.1.1 a）、5.6.1.2 a）、b）、c）、d））

### 6.6.2 重要数据保护

#### 6.6.2.1 数据安全过程域描述

通过组织机构其业务所适用法律法规的要求，在相关业务环节和内部运营流程中开展重要数据保护工作，以实现对重要数据的全生命周期安全防护。

#### 6.6.2.2 数据安全能力基本实践

a) 组织建设：设立了组织机构统一负责重要数据保护的团队，该团队包含法律合规人员、安全人员、业务人员、技术人员，为组织机构提供统一的重要数据保护的规范要求、制定相应的数据安全解决方案并推进其在组织机构整体范围内的落地。（《要求》5.6.2.1 a）、b）、c）、d）、e），5.6.2.2 a）、b）、c））

b) 制度流程：

1) 依据网络安全法等法律法规中对重要数据的保护要求，建立组织机构统一的针对重要数据全生命周期保护的制度规范。（《要求》5.6.2.1 a）、b））
2) 针对组织机构内部因业务架构、组织机构职能变更而引发的重要数据流向发生的变化，建立有效的变更管控机制，以实现重要数据流向变化时可能引发的合规风险。（《要求》5.6.2.1 c））
3) 定期对重要数据保护的制度规范落地情况执行进行跟进，以及时更新相关规程保证其可落地性。（《要求》5.6.2.1 e））
4) 基于组织机构内部各类业务场景所涉及的针对重要数据的不同的安全风险，在组织机构整体的重要数据保护制度规范的要求下建立详细的指导细则。

c) 技术工具：
1) 依据网络安全法等法律法规中对重要数据的保护要求，制定针对重要数据的风险监控技术方案（《要求》5.6.2.1 b））
2) 记录重要数据的全生命周期操作行为日志，对重要数据生命周期相关操作行为进行合规性分析，以获取其合规性实践的整体情况。（《要求》5.6.2.1 d））
3) 具备对重要数据的自动化脱敏机制，支持如匿名、泛化、随机和加密等脱敏手段，并建立相应的脱敏有效性评价功能，以保证对重要数据保护的合规性要求的支持。（《要求》5.6.2.2 a））
4) 基于针对重要数据的风险监控平台，定期审核重要数据的相关操作记录，以保证对重要数据相关风险的量化管理，具备评价重要数据脱敏有效性的评估能力。尤其是针对大数据服务中所是沉淀的数据，应监控通过大数据服务中的沉淀数据获取重要数据的风险。（《要求》5.6.2.2 b）、c））

d) 人员能力：充分理解重要数据保护的合规性要求，并具备合规性要求制定解决方案的能力。（《要求》5.6.2.1 a）、b）、c）、d）、e)，5.6.2.2 a）、b）、c））

### 6.6.3 数据跨境传输

#### 6.6.3.1 数据安全过程域描述

通过组织机构其业务所适用法律法规的要求,在相关业务环节和内部运营流程中开展数据跨境传输过程中的安全控，以降低数据跨境传输的风险。

#### 6.6.3.2 数据安全能力基本实践

a) 组织建设：设立了组织机构统一负责数据跨境传输的团队，该团队包含法律合规人员、安全人员、业务人员、技术人员，为组织机构提供统一的数据跨境传输的规范要求、制定相应的数据安全解决方案并推进其在组织机构整体范围内的落地。（《要求》5.6.3.1 a）、b）、c)，5.6.3.2 a））

b) 制度流程：
1) 依据网络安全法等法律法规和标准中对数据跨境传输的安全要求，建立组织机构统一的数据跨境传输的制度规范，明确数据跨境传输的安全策略、管理制度、管理规范和管控措施。（《要求》5.6.3.1 a））
2) 建立业务中涉及数据跨境传输时相关的处理流程和审批流程。（《要求》5.6.3.1 a））
3) 基于组织机构内部各类业务场景所涉及的针对数据跨境传输的不同的安全风险，在组织机构整体的数据跨境传输安全制度规范的要求下建立详细的指导细则。(《要求》5.6.3.1 a）、b）、c））
4) 定期或在发生重大信息安全事件后，对数据跨境传输有关制度、流程和技术进行审查和检验，记录审查和检验结果并提交组织机构最高的数据安全管理组织审批。（《要求》

5.6.3.2 a））

c) 技术工具：

1) 建立数据跨境传输相应的在线审批流程，从而对数据跨境传输的相关申请和审批进行有效的记录，并分析整体安全合规情况。（《要求》5.6.3.1 a）、b）、c））

2) 基于针对数据跨境传输的审批平台，定期审核数据跨境传输的相关记录，以保证对数据跨境传输的合规风险的量化管理。（《要求》5.6.3.1 a）、b）、c））

3) 在组织机构的数据管理平台中标识需要满足数据跨境传输合规要求的数据，定期检测此类数据的存储地是否符合合规性要求、若发生跨境传输是否已完成相应的审批流程，以保证合规工作执行的有效性。（《要求》5.6.3.1 a）、b）、c））

d) 人员能力：充分理解数据跨境传输的合规性要求，并具备合规性要求分析合规风险并制定解决方案的能力。（《要求》5.6.3.1 a）、b）、c），5.6.3.2 a））

### 6.6.4 密码支持

#### 6.6.4.1 数据安全过程域描述

通过组织机构其业务所适用法律法规的要求，在相关业务环节和内部运营流程中应用相应的密码技术实现对相关数据的机密性保护。

#### 6.6.4.2 数据安全能力基本实践

a) 组织建设：设立了组织机构统一负责加密管理的团队，该团队包含法律合规人员、安全人员、业务人员、技术人员，为组织机构提供统一的加密管理的规范要求、制定相应的数据安全解决方案并推进其在组织机构整体范围内的落地。（《要求》5.6.4.1 a），5.6.4.2 a）、b））

b) 制度流程：

1) 按照国家密码管理规定使用和管理有关密码技术和设施，建立组织机构整体的加密管理规范，明确密钥生成、分发、存取、更新、备份和销毁的要求。（《要求》5.6.4.1 a））

2) 基于组织机构内部各类业务场景所涉及的加密管理建立详细的指导细则。（《要求》5.6.4.2 a））

c) 技术工具：

1) 建立组织机构统一的秘钥管理平台，通过该平台执行对秘钥的全生命周期的安全管理。（《要求》5.6.4.1 a））

2) 基于密钥管理操作性等有关标准规范，提供密钥集成管理的工具技术。（《要求》5.6.4.2 a））

3) 具备密文数据透明处理的技术能力。（《要求》5.6.4.2 b））

d) 人员能力：充分理解加密管理的合规性要求，并具备合规性要求制定解决方案的能力。（《要求》5.6.4.1 a），5.6.4.2 a）、b））

## 7 数据生命周期各阶段的安全基本实践

### 7.1 数据采集安全

#### 7.1.1 数据分类分级

##### 7.1.1.1 数据安全过程域描述

通过法律法规要求以及组织业务需求定义组织机构内部的数据分类分级原则，对生成/采集的数据进行数据分类分级的标识，为数据安全管理建立有效的安全基础。

##### 7.1.1.2 数据安全能力基本实践

a) 组织建设：
   1) 组织机构设立了负责数据安全分类分级工作的管理团队/岗位，该团队/岗位多与组织机构的数据管理团队和数据安全管理团队有关，主要负责对组织机构整体的数据安全分类分级的原则定义和能力提供。（《要求》6.1.1.1 a）、b）、c））
   2) 由各业务团队的数据管理者/数据安全管理者负责具体对数据的分类分级工作。（《要求》6.1.1.1 a）、b）、c））

b) 制度流程：
   1) 基于组织机构整体的数据分类分级原则，针对具体的关键业务场景制定数据安全分类分级的细则，针对不同类别和级别的数据制定相应的安全管理策略。（《要求》6.1.1.1 a)、b））
   2) 建立数据资产的类别和级别的建立及变更审核流程，通过该流程保证对数据分类分级的变更操作及其结果符合组织机构的策略要求。（《要求》6.1.1.1 c））

c) 技术工具：
   1) 建立数据的安全分类分级标识工具，在数据管理的平台上利用该工具，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，并由人工审核后再发布数据分类分级标识的结果；同时基于该平台，可实现在线的变更审核流程。（《要求》6.1.1.1 a)、b）、c））
   2) 对数据分类分级的操作、变更过程进行日志的记录和分析，以保证数据分类分级过程的可追溯性。（《要求》6.1.1.2 a））
   3) 记录数据自动化分类分级的结果与人工审核后的分类分级结果之间的差异，定期分析改进分类分级标识工具，以提升工具处理的准确度。（《要求》6.1.1.2 a））
   4) 记录人工审核阶段将数据安全级别向低级别调整的情况，定期审核此类场景下是否存在人为的错误。（《要求》6.1.1.2 a））

d) 人员能力：
   1) 负责该项工作的人员能够理解组织机构内数据所处的业务场景以及数据一旦发生泄漏所造成的风险。（《要求》6.1.1.1 a）、b）、c））
   2) 通过在相关管理团队中针对数据安全分类分级要求的进行培训，以实现组织机构内数据分类分级工作执行的有效性。（《要求》6.1.1.1 a）、b）、c））

### 7.1.2 数据收集和获取

#### 7.1.2.1 数据安全过程域描述

通过有效遵循国家法律法规、监管政策的要求，对数据的采集和获取过程执行了有效的安全控制，以保证对各类数据的合规收集。

#### 7.1.2.2 数据安全能力基本实践

a) 组织建设：
   1) 组织机构层面设立了负责数据采集安全的团队，该团队由法律团队人员、安全团队人员、业务团队人员共同组成。该团队负责制定相关的数据采集的安全要求，并推动相关要求、流程的落地实施。（《要求》 6.1.2.1 a）、b）、c）、d）、e）、f））
   2) 基于组织机构整体的数据采集保护原则，由涉及数据采集的业务团队设立相应的风险评估小组，对具体业务场景下的数据采集的风险评估和改进方案的制定，组织机构整体负责数据采集保护的团队提供对各业务团队风险评估小组工作的咨询和支持。（《要求》6.1.2.1 a）、b）、c）、d）、e）、f））

b) 制度流程：

3) 组织机构基于法律法规的要求制定并及时更新数据采集规范，该规范定义数据采集的原则，要求数据采集的业务场景中需明确采集数据的目的和用途，数据源的真实性、有效性，采集数据的范围和数据量在业务场景下对最小够用原则的符合性，并规范数据采集的渠道、数据的格式以及相关的流程和方式，从而保证数据采集的合规性、正当性和执行上的一致性。（《要求》 6.1.2.1 a）、c）、d））

4) 组织机构内部建立数据采集的风险评估流程，该流程要求组织机构内部负责数据采集安全的团队参与对数据采集的业务场景的安全风险评估，风险的评估基于组织机构整体的数据采集规范的要求执行，针对采集的数据源、采集的数据范围和频度、数据采集的渠道和方式、采集数据的类型进行风险评估，涉及采集个人信息和重要数据的业务场景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。（《要求》 6.1.2.1 b）、c））

5) 基于组织机构统一的数据采集保护原则，由数据采集的业务团队负责对其相关的业务场景制定风险评估的细则。（《要求》 6.1.2.1 a）、6.1.2.2 a））

c) 技术工具：

1) 在涉及数据采集的业务系统中建立了统一的在线采集流程，以保证组织机构内对个人信息采集流程实现的一致性和获授权过程的有效记录。（《要求》 6.1.2.1 e））

2) 针对在线的数据采集的功能模块实现对所采集数据的质量验证，确保采集数据的完整性、一致性和真实性。（《要求》 6.1.2.1 d））

3) 采取必要的技术手段保证数据收集和获取过程中个人信息和重要数据不被泄露。（《要求》6.1.2.1 f））

4) 采取必要的技术手段对采集的数据进行校验，以保证其完整性和一致性。（《要求》6.1.2.2 a））

5) 针对所有在线的数据采集过程执行有效的日志管理，实现对数据采集过程的可追溯性。（《要求》 6.1.2.2 b））

d) 人员能力：

1) 负责该项工作的人员从各自的专业角度保证对数据有效采集的合规需求、安全需求和业务需求的充分理解，并能够综合组织机构内的业务场景提出针对性的解决方案。（《要求》 6.1.2.1 a）、b）、c）、d）、e）、f））

2) 建立数据采集保护团队与涉及数据采集的业务团队之间的定期交流机制，实现数据采集原则的制定者与业务场景中原则的执行者之间及时的信息共享，提升组织机构内相关人员对合规要求以及对业务场景的理解力。（《要求》 6.1.2.1 a）、b）、c）、d）、e）、f）、6.1.2.2 a）、b））

### 7.1.3 数据清洗、转换与加载

#### 7.1.3.1 数据安全过程域描述

通过在数据执行清洗、转换与加载的过程中执行对数据的保护，以保证对数据的完整性、一致性和可用性。

#### 7.1.3.2 数据安全能力基本实践

a) 组织建设：组织机构内设立了统一的团队/岗位，明确数据清洗、转换和加载的原则、方法并提供相关技术能力，并由数据的管理/安全管理团队/岗位负责实际场景下的数据清洗、转换和加载的管理。（《要求》 6.1.3.1 a）、b）、c））

b) 制度流程：

1) 制定组织机构的数据清洗、转换和加载操作相关的安全管理规范，在规范中明确数据清

洗、转换与加载的要求、规则和方法。（《要求》 6.1.3.1 a）、b）、c））

2) 针对在个人信息和重要数据等数据，建立数据清洗、转换与加载过程中的数据还原和恢复规范。（《要求》 6.1.3.2 a））

c) 技术工具：

1) 组织机构提供统一的数据清洗、转换和加载工具，能够呈现清洗与转换前后数据间的映射关系；并建立不同数据源、不同安全域之间采集数据加载安全策略、加载方式和访问控制机制。（《要求》 6.1.3.1 a））

2) 通过工具建立统一的数据清理、转换和加载流程，明确人员权限、操作和执行步骤，可以保证对清洗、转换与加载过程中对数据的保护，确保数据正确性、一致性和可控性。（《要求》 6.1.3.1 b））

3) 根据数据分类分级原则，记录并保存数据清洗、转换和加载过程中个人信息、重要数据等敏感数据的处理过程。（《要求》 6.1.3.1 c））

4) 数据清洗、转换与加载工具具备一致性检测的能力。在有恢复需求或操作产生问题时，能有效的还原和恢复数据。（《要求》 6.1.3.2 a）、b））

d) 人员能力：通过培训宣传确保负责数清洗与数据转换实现的人员对清洗、转换与加载的规则理解的一致性，并提升人员的操作能力。（《要求》 6.1.3.1 a）、b）、c），6.1.3.2 a)、b））

### 7.1.4 质量监控

#### 7.1.4.1 数据安全过程域描述

通过建立组织机构的数据质量监控体系，来保证对数据采集过程中采集/生成的数据的准确性、及时性、完整性和一致性。

#### 7.1.4.2 数据安全能力基本实践

a) 组织建设：

1) 组织机构内成立了数据质量管理团队，由该团队负责制定统一的数据质量管理规范，并对各业务的数据管理人员进行规范的培训，由各团队的数据管理人员按照规范的要求执行对数据的标准化处理。（《要求》 6.1.4.1 a）、b）、c））

2) 建立数据质量管理团队与各团队的数据管理人员之间的有效沟通、反馈机制，能够持续、及时的针对数据质量管理工作进行适当的改进。（《要求》 6.1.4.1 a）、b）、c），6.1.4.2 a）、b））

b) 制度流程：

1) 定义数据源质量评价标准，制定了数据采集质量管理控制策略和规范，数据质量管理规范包含对数据的标准化格式的要求、数据的完整性要求、以及对数据故障应急相应机制要求。（《要求》 6.1.4.1 c））

2) 建立数据采集过程中质量监控规则，明确数据质量监控范围及监控方式。(《要求》6.1.4.1 a））

3) 明确采集数据质量的要素，建立异常事件处理流程和操作规范，并制定流程中相应的责任岗位。（《要求》 6.1.4.1 b））

4) 建立数据质量故障体系，并将故障处理的制度流程告知相关的数据管理人员。

5) 制定数据质量分级标准，明确不同级别、分类类型的数据采集、清洗、转换等数据采集处理流程质量要求。（《要求》 6.1.4.2 a））

6) 制定定期对数据质量进行分析、预判和盘点规范，明确数据质量问题定位和修复时间要求。（《要求》 6.1.4.2 a））

c) 技术工具：
   1) 结合元数据管理平台，对数据实现数据资产的等级划分，从而优先实现对关键数据的数据质量保障资源。（《要求》 6.1.4.1 a)、b)、c)）
   2) 利用工具对在线产生数据的平台执行在线数据监控，从而实现异常数据的及时订正，同时通过对在线数据的监控强化离线数据的一致性。（《要求》 6.1.4.1 a)、b)、c)）
   3) 建立数据质量的度量技术指标，并通过相关管理平台量化评估对各团队的数据质量管理的水平。（《要求》 6.1.4.2 a)、b)）
d) 人员能力：负责该项工作的人员具有数据质量管理的相关理论基础，并能够基于组织机构的实际数据质量管理需求开展相关工作的落地推进，通过培训实现各业务的数据管理人员对数据质量工作标准的一致性理解，并对负责该项工作人员的专业能力的定期考核。（《要求》6.1.4.1 a）、b）、c，6.1.4.2 a）、b））

## 7.2 数据传输安全

### 7.2.1 数据传输安全管理

#### 7.2.1.1 数据安全过程域描述

利用加密、签名、鉴别和认证等机制对传输中的敏感数据进行安全管理，监控数据传输时的安全策略实施情况，防止传输过程中可能引发的敏感数据泄漏和数据传输双方对身份的抵赖。

#### 7.2.1.2 数据安全能力基本实践

a) 组织建设：组织机构指定了团队负责数据传输安全管理的整体解决方案制定和技术能力提供，由各业务团队负责具体场景下数据传输安全管理的实现。（《要求》6.2.1 a） ）
b) 制度流程：
   1) 组织机构区分了安全域内、安全域间等不同的大数据服务相关的数据传输场景，统一制定了相应的数据传输安全策略和流程，在数据分类分级定义的基础上明确提出对相关类型、级别的数据的传输安全管理要求，其中应细化加密传输、签名验签、鉴别和验证的要求，建立了对数据传输安全策略变更进行审核和监控的制度，建立了数据传输接口安全管理工作规范，包括安全域内、安全域间等数据传输接口规范。（《要求》6.2.1 a)、b)、c)、d)、e)、f)，6.2.2 a））
   2) 针对不同数据传输场景制定了数据传输安全管理规范，该规范中应明确组织机构内负责数据传输管理的部门及其职责，并配套制定数据传输接口管理及传输策略变更审核和监控相应的流程。（《要求》6.2.1 a））
c) 技术工具：
   1) 提供满足数据传输安全策略相应的安全控制技术方案，包括安全通道、可信通道、数据加密等。（《要求》6.2.1 b)）
   2) 提供在构建传输通道前对两端主体身份进行鉴别和认证的技术方案和工具。（《要求》6.2.1 d））
   3) 提供对传输数据的完整性进行检测并执行恢复控制的技术方案和工具。（《要求》6.2.1 e））
   4) 提供对数据传输安全策略的变更进行审核和监控的技术方案和工具，部署了对通道安全配置、密码算法配置、密钥管理等保护措施进行审核及监控的技术工具。（《要求》6.2.1 f））
   5) 组织机构提供固定的安全通道或可信通道建立方法供技术人员调用，能够自动进行传输通道的建立和管理。（《要求》6.2.1 b)、d)）
   6) 组织机构提供固定的数据加密模块供开发传输功能的人员调用，该模块可自动识别数据的类型和级别进行数据加密处理，从而保证数据加密功能的统一性。（《要求》6.2.1 b)）

7) 组织机构提供统一的对通道安全配置、密码算法配置、密钥管理等保护措施进行审核和监控的工具，提高策略变更审核和监控的效果。(《要求》6.2.1 b)、f))
8) 每个传输链路上的节点都部署了独立的公钥/私钥对和数字证书，以保证各节点有效的身份鉴别和认证。(《要求》6.2.1 b))
9) 综合量化不同数据传输策略的实现效果和成本，定期审核并调整数据传输策略的实现方案。(《要求》6.2.1 a))
10) 基于法律法规的要求和业务的需求，在关键的业务网络架构汇总考虑网络的可用性建设需求，对关键的网络传输链路、网络设备节点实行冗余建设。(《要求》6.2.2 a))

d) 人员能力：了解市场上主流的安全通道和可信通道建立方案、身份鉴别和认证技术、数据加密算法和国家推荐的数据加密算法，从而能够基于具体的业务场景选择合适的数据传输安全管理方式，并具备针对数据传输安全管理要求在实际业务场景中制定解决方案的能力。(《要求》6.2.1 a）、b）、c）、d）、e）、f），6.2.2 a）)

## 7.3 数据存储安全

### 7.3.1 存储架构

#### 7.3.1.1 数据安全过程域描述

通过基于组织机构的数据量增长、数据存储安全需求和合规性要求制定适当的对存储架构，以实现对存储数据的有效保护。

#### 7.3.1.2 数据安全能力基本实践

a) 组织建设
1) 组织机构内设立了统一负责数据中心安全管理的团队/岗位，负责制定数据中心安全管理规范，并推进相关要求的落地实施。(《要求》6.3.1.1 a)、b)、c)、d)、e)，6.3.1.2 a)、b))
2) 基于数据存储所面临的合规性要求，组织机构内明确了负责数据加密的团队或岗位。(《要求》6.3.1.1 d))

b) 制度流程
1) 制定数据中心安全管理规范，包括但不限于物理安全、资产安全、人员访问控制等。(《要求》6.3.1.1 b))
2) 制定数据中心设备运行维护的操作规程，如标准操作流程、维护操作流程、应急操作流程等。(《要求》6.3.1.1 b)、c))
3) 制定数据存储安全策略，如用户身份标识与鉴别策略、数据访问控制策略、数据扩容及复制策略、数据存储完整性规则、多副本一致性管理规则、存储转移安全规则等。(《要求》6.3.1.1 b)、c))
4) 基于组织机构数据存储面临的合规性要求，在数据分类分级定义的基础上明确各类各级数据的加密存储要求，包括对数据加密算法的要求和数据加密密钥的管理要求，如对密钥使用时长的要求。(《要求》6.3.1.1 d))

c) 技术工具
1) 建立可伸缩数据存储架构，以满足数据量持续增长、数据分类分级存储等需求。该数据存储架构提供对个人信息、重要数据等加密存储能力，并具备数据存储跨机柜或跨机房容错部署能力。(《要求》6.3.1.1 a))
2) 统一提供有效的技术方案，对数据存储完整性和多副本一致性真实进行检测和恢复。(《要求》6.3.1.1 c))

3) 建立有效的数据加密工具，并提供有效的密钥管理机制已实现对密钥的全生命周期（存储、使用、分发、更新和销毁）的安全管理。（《要求》6.3.1.1 d)）
4) 确保存储架构具备数据存储跨地域的容灾能力。（《要求》6.3.1.2 e)）
5) 建立满足应用层、数据平台层、操作系统层、数据存储层等不同层次的数据存储加密需求的数据存储加密架构。 （《要求》6.3.1.1 d)、6.3.1.2 b)）
6) 组织机构提供固定的数据加密模块供存储功能的开发人员调用，该模块可自动识别数据的类型和级别进行数据加密处理，从而保证数据的加密功能的统一性。（《要求》6.3.1.1 d)、6.3.1.2 b)）

d) 人员能力
1) 负责数据中心安全管理工作的人员，熟悉数据存储架构并能够分析出数据中心面临的安全风险，能够对数据中心安全事件进行及时响应。（《要求》6.3.1.1 b)）
2) 负责分布式数据存储安全策略制定的人员，熟悉数据存储安全管理的技术知识，并能够结合业务场景制定数据存储安全规则。（《要求》6.3.1.1 b)、d)）
3) 负责数据加密工作的人员熟悉各类数据加密算法的性能和瓶颈，并能够基于业务发展的需求、合规的需求制定有效的数据加密方案。（《要求》6.3.1.1 d)）
4) 面向数据开发人员、数据库管理人员开展数据加密管理的培训，使其了解了数据加密算法所适合的应用场景。（《要求》6.3.1.1 d)）

### 7.3.2 逻辑存储

#### 7.3.2.1 数据安全过程域描述

通过基于组织机构内部数据存储安全要求和大数据的业务特性建立针对数据逻辑存储环境的有效安全控制，以防止由于逻辑存储环境的安全风险而导致的存储数据的安全风险。

#### 7.3.2.2 数据安全能力基本实践

a) 组织建设
1) 组织机构内设立了统一负责数据存储系统安全管理的团队/岗位，负责明确整体的安全管理要求并推进相关要求的落地实施。（《要求》6.3.2.1 a)、b)、c)）
2) 组织机构内明确了各数据存储系统的安全管理员，负责执行数据存储系统的安全管理和运维工作。（《要求》6.3.2.1 a)、b)、c)）

b) 制度流程
1) 制定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、存储转移安全规则等，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。（《要求》6.3.2.1 b)）
2) 建立数据存储系统的安全管理规范，明确各类数据存储系统（如在线数据库、离线数据库、文件存储系统、办公终端系统、外部云存储系统等）的数据存储要求，如可存储的数据类型、安全级别、涉及业务范围等，以实现对不同数据类型、不同数据容量、不同也无需求和不同数据用户的存储安全管理。（《要求》6.3.2.1 a)）
3) 制定各类数据存储系统的安全配置规则，对存储系统的账号权限管理、访问控制、日志管理、加密管理、版本升级等方面进行要求。（《要求》6.3.2.1 a)）
4) 制定办公终端的安全管理办法，定义办公终端的安全管理要求，并明确终端数据防泄漏的相关要求。（《要求》6.3.2.1 a)）
5) 明确数据逻辑存储多租户隔离、授权管理规范，确保具备多租户数据存储安全隔离能力。

（《要求》6.3.2.1 c)）

6） 建立分层的逻辑存储授权管理规则和授权操作规范，具备对数据逻辑存储结构的分层和分级保护能力。（《要求》6.3.2.2 a)）

7） 各业务团队的数据存储系统的管理人员基于业务场景的需求，对所负责的存储系统的安全配置基线进行了定制化的管理，从而保证对业务的适应性和安全性的平衡。（《要求》6.3.2.1 b)）

c） 技术工具

1） 组织机构提供了针对主要数据存储系统的配置扫描的工具，定期对数据存储容器的安全配置进行扫描，以保证符合基线的一致性要求。（《要求》6.3.2.1 a)）

2） 组织机构提供了整体的终端安全解决方案，实现终端设备与组织机构内部员工的有效绑定，按照统一的部署标准在终端系统上安装各类防控软件（如防病毒、硬盘加密、终端入侵检测等软件），基于组织机构的数据防泄漏方案通过 DLP 产品对终端系统上的数据进行风险监控。（《要求》6.3.2.1 a)）

3） 内部的数据存储系统在上线前应通过安全配置流程以保证遵循了统一的安全配置，对使用的外部数据存储系统也应进行有效的安全配置。（《要求》6.3.2.1 a)）

4） 能利用技术工具监测存储系统的数据和从存储系统下载的数据，是否符合组织机构的相关安全要求。（《要求》6.3.2.2 a)）

5） 采用技术手段保护组织机构在外部公开云平台存储的数据，建立数据的机密性保护和完整性验证机制。（《要求》6.3.2.2 a)）

d） 人员能力

1） 负责该项工作的人员熟悉相关的数据存储系统的技术架构并能够基于安全管理的原则判断出相关的风险，从而能够保证对各类数据存储系统的有效安全防护。（《要求》6.3.2.1 a)、b)、c)）

2） 跟踪数据存储系统的技术发展现状和安全风险现状，及时调整组织机构整体的数据存储系统的安全规范，并通过部署和更新适当的技术手段提升对存储系统的安全保护能力。（《要求》6.3.2.2 a)、b)、c)）

### 7.3.3 访问控制

#### 7.3.3.1 数据安全过程域描述

通过基于组织机构数据存储安全需求和合规性要求建立数据访问控制机制，防止对存储数据的未授权访问风险。

#### 7.3.3.2 数据安全能力基本实践

a） 组织建设：组织机构内设立了统一负责数据权限管理的团队或岗位，明确了业务部门和安全部门的审批权限和审批人员。（《要求》6.3.3.1 a））

b） 制度流程：

1） 建立数据存储系统安全管理员的身份标识与鉴别策略、权限分配策略及相关操作规程。（《要求》6.3.3.1 a)）

2） 建立数据访问审计信息的存储保护机制和管控措施。（《要求》6.3.3.1 c)）

3） 在数据分类分级定义的基础上，明确各类各级数据的访问控制要求。（《要求》6.3.3.1 b））

c） 技术工具：

1） 建立了组织机构内部统一的数据权限管理平台，通过平台结合存储访问与控制模块对组织机构内部人员对各类数据存储系统的访问权限进行管理，实现对用户的身份标识与鉴别策

略、数据访问控制策略、数据扩容及复制策略。（《要求》6.3.3.1 b)）

2) 建立面向大数据应用的访问控制机制，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。（《要求》6.3.3.1 d)）

3) 利用技术工具对分布式数据存储访问进行安全审计，并保护对审计信息的有效保护。(《要求》6.3.3.1 c)）

4) 建立数据存储安全主动防御机制或措施，如基于用户行为或设备行为安全控制机制。(《要求》6.3.3.2 a)）

5) 对组织机构利用外部公开提供的云平台存储数据的情况，利用相关技术手段建立数据的机密性保护和完整性验证机制。（《要求》6.3.3.1 c)）

6) 跟踪数据访问控制的技术发展现状和安全风险现状，及时改进数据访问控制规则和工具性能，提高数据访问控制粒度。（《要求》6.3.3.1 a）、b）、c）、d）

d) 人员能力：负责该项工作的人员熟悉相关的数据访问控制的技术知识，并能够根据组织机构数据安全管理制度对数据权限进行审批管理。（《要求》6.3.3.1 c)）

### 7.3.4 数据副本

#### 7.3.4.1 数据安全过程域描述

通过执行定期的开展数据的复制、备份和恢复，实现对存储数据的冗余性管理，保护数据的有效性。

#### 7.3.4.2 数据安全能力基本实践

a) 组织建设：组织机构内设立了负责统一的的数据存储冗余性管理的团队或岗位，并将数据复制、备份和恢复的职责明确划分到相应的团队或岗位。（《要求》6.3.4.1 a））

b) 制度流程：

1) 建立数据存储冗余策略和管理制度，以满足大数据服务可靠性、可用性等数据安全保护目标。（《要求》6.3.4.1 a)）

2) 建立数据冗余强一致性、弱一致性等控制策略与规范，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。（《要求》6.3.4.1 b)）

3) 建立数据复制、备份与恢复的操作规程，明确定义数据复制、备份和恢复的范围、频率、工具、过程、日志记录规范、数据保存时长等。（《要求》6.3.4.1 c)）

4) 建立数据复制、数据备份与恢复的定期检查和更新工作程序，包括数据副本更新频率、保存期限等，确保数据副本或备份数据的有效性。（《要求》6.3.4.1 d)）

5) 定期对组织机构内数据备份的场景、数量、频率进行统计，了解组织机构内部数据备份工作的开展情况。(《要求》6.3.4.1 c)、d)）

6) 具备数据副本或数据备份存储的多种压缩策略和实现机制，并确保压缩数据副本或数据备份的完整性和可用性。(《要求》6.3.4.2 a)）

c) 技术工具：

1) 建立用于数据复制备份、恢复的技术工具，并将具体的备份的策略固化到工具中，保证相关工作的自动化执行。（《要求》6.3.4.1 d)）

2) 定期地采取必要的技术手段和管控措施查验归档数据完整性和可用性。

d) 人员能力：

1) 执行数据备份和恢复测试的人员均经过了组织机构内部统一的培训，能够保证其执行数据备份和恢复测试时的操作具有一致性。（《要求》6.3.4.1 c)、d)）

2) 负责该项工作的人员了解数据备份介质的性能和相关数据的业务特性，从而能够确定有效

的数据备份、恢复工作开展的方式。（《要求》6.3.4.1 c)、d)）

### 7.3.5 数据归档

#### 7.3.5.1 数据安全过程域描述

通过建立数据归档存储的规范化流程和安全保护措施，实现对归档数据的有效保护。

#### 7.3.5.2 数据安全能力基本实践

a) 组织建设：组织机构内设立了负责统一的数据归档存储管理的团队或岗位，负责建立相应的制度流程并部署相应的安全控制措施。（《要求》6.3.5.1 a））

b) 制度流程：

1) 建立数据归档存储的制度规范,该制度规范中明确定义据生命周期和业务规范建立不同阶段数据归档存储相关的操作规程，并明确提出针对归档数据的相关安全策略。（《要求》6.3.5.1 a)）

2) 建立归档数据安全审计与恢复制度，并指定专人负责。（《要求》6.3.5.2 a））

c) 技术工具：

1) 建立在线/离线的多级数据归档架构，支持海量数据的有效归档、恢复和使用。（《要求》6.3.5.1 b)）

2) 建立归档数据的安全管理技术方案，包括但不限于针对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，确保对归档数据的安全性、存储空间的有效利用和安全访问。（《要求》6.3.5.1 c） 、d）、e））

d) 人员能力：

1) 负责该项工作的人员了解数据的业务特性，从而能够确定有效的数据存储归档工作开展的方式。（《要求》6.3.5.1 a)、b)、c)、d)、e)）

2) 定期对组织机构内数据归档存储的情况进行统计，了解组织机构内部数据归档存储工作的开展情况。（《要求》6.3.5.1 a)）

### 7.3.6 数据时效性

#### 7.3.6.1 数据安全过程域描述

通过执行对数据存储执行时效性管理对相关数据的及时清除和权限授予,实现对相关法律法规和合同协议中数据时效性要求的有效遵循。

#### 7.3.6.2 数据安全能力基本实践

a) 组织建设：组织机构设立了统一负责数据存储时效性管理的团队/岗位。(《要求》6.3.6.1 a))

b) 制度流程：

1) 基于数据存储时效性相关的合规性要求，制定了数据存储时效性管理的规范要求，明确数据分享、存储、使用和清除的有效期、有效期到期时对数据的处理流程、过期存储数据的安全管理策略。（《要求》6.3.6.1 a)、b)、c)）

2) 列出了使用的法律法规的条款清单以及相应的执行细则，明确存储数据分享、禁止使用和数据清除有效期。（《要求》6.3.6.1 a)）

3) 各团队根据业务场景的需求在组织机构整体规则的基础上基于团队所适用的合同条款的要求，对适用的条款清单进行了细化。（《要求》6.3.6.1 a））

c) 技术工具：

1) 建立组织机构统一的数据留存的合规要求在线库，以保证相关人员对相关监管合规要求的信息获取，具备数据存储时效性授权与控制能力。（《要求》6.3.6.1 a)）
2) 建立数据有效性管理的统一技术方案，实现对数据存储时效性的授权和控制、对过期存储数据的删除机制以保证删除有效性的验证和相关删除效果对数据控制着和大数据使用者的有效告知。（《要求》6.3.6.1 b)、c)、d)）
3) 为不同时效性的数据建立分层的数据存储方法，具备按照时效性自动迁移数据分层存储的能力，确保大数据用户能高效地获得有效数据。（《要求》6.3.6.2 b)）
4) 通过工具对需要符合数据存储合规要求的数据进行了标识。(《要求》6.3.6.1 b)）
5) 通过工具实现对数据的存储时效性进行阈值提醒，包括但不限于告警、自动清除和拒绝访问等，以保证数据的及时删除、更新和有效性。(《要求》6.3.6.1 b)、6.3.6.2 a)）

d) 人员能力：负责该项工作的人员充分了解数据存储时效性相关的合规性要求，并具备基于业务场景对留存合规性要求的解读能力和落地方案的制定和推进能力。（《要求》6.3.6.1 a)、b)、c)、d)

## 7.4 数据处理安全

### 7.4.1 分布式处理安全

#### 7.4.1.1 数据安全过程域描述

通过针对组织机构内部使用相关计算、开发平台/系统建立分布式处理的安全保护机制，防止分布式处理过程中数据泄漏、未授权访问等安全风险。

#### 7.4.1.2 数据安全能力基本实践

a) 组织建设：设立团队/岗位负责组织机构统一分布式处理的安全管理规则的制定，并由各分布式处理平台/ 系统团队配合从而实现相关管理规则在系统/平台上的落地。(《要求》6.4.1.1 a）)
b) 制度流程：
   1) 制定了分布式处理安全管理规范，在分布式处理的节点间可信连接认证、节点和用户安全属性周期性确认、数据文件鉴别和访问用户身份认证、数据副本节点更新检测、以及防止数据泄露等方面进提出明确的安全管理要求。（《要求》6.4.1.1 a)、b)、c)、d)、e)）
   2) 利用分布式处理节点及访问用户操作日志，开展定期的操作审计，确定用户在大数据加工平台上的计算分析未超出前期数据申请的目的。（《要求》6.4.1.1 e））
c) 技术工具：
   1) 对分布式处理节点间进的可信连接进行认证，以确保节点接入的真实性；以及外部服务组件注册与使用审核机制。（《要求》6.4.1.1 a)，6.4.1.2 a)）
   2) 对分布式处理节点和用户安全属性进行周期性确认,确保预定义分布式安全策略一致性。（《要求》6.4.1.1 b)）
   3) 对分布式处理过程中数据文件鉴别和访问用户身份认证进行验证,确保分布式处理数据文件的可访问性。（《要求》6.4.1.1 c)）
   4) 对分布式处理过程中不同数据副本节点的更新进行定期检测,确保这些节点数据拷贝的完整性、 一致性和真实性。 （《要求》6.4.1.1 d)）
   5) 对分布式处理过程中的调试信息和日志记录等实施监控,确保这些信息不受控制输出泄露受保护的个人信息、重要数据等敏感信息。 （《要求》6.4.1.1 e)）
   6) 建立对数据分布式处理节点的服务组件自动维护策略和管控措施,如各工作节点的功能稳

定、实现对工作节点的伪装风险监测、故障用户节点确认和自动修复的技术机制,避免云环境或虚拟环境下潜在的安全攻击等。（《要求》6.4.1.2 b））

d) 人员能力：负责该项工作的人员了解在的分布式处理系统/平台的主要安全风险，并能够在相关的系统设计、开发阶段通过合理的设计以及运维阶段的有效配置规避相关风险。（《要求》6.4.1.1 a)、b)、c)、d)、e) ，6.4.1.2 a)）

### 7.4.2 数据分析安全

#### 7.4.2.1 数据安全过程域描述

通过在数据分析过程中对国家安全、业务价值、个人数据保护的安全需求分析，采取适当的安全控制措施以防止由于数据分析而可能带来的数据价值泄漏风险。

#### 7.4.2.2 数据安全能力等级描述

a) 组织建设：组织机构设立统一负责数据分析安全的岗位，负责整体的原则制定并提供相应的支持能力，并由业务团队指定相关的人员在数据分析过程中负责具体的安全保护管理。（《要求》6.4.2.1 a）、b）、c）、d）、e））

b) 制度流程：

1) 制定了数据分析中获取数据和使用数据的安全保护规范,主要从数据获取方式、访问接口、授权机制、分析逻辑、分析结果及数据使用等方面分别展开。（《要求》6.4.2.1 a)）
2) 制定多源数据派生、聚合、关联分析等数据分析过程中的数据资源操作规范和实施指南，整体保证大数据分析的预期不会超过相关分析团队对数据的权限范围。（《要求》6.4.2.1 b)）
3) 建立大数据分析结果输出和使用的安全审查、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。（《要求》6.4.2.1 c)、d)、e)）
4) 持续跟进国内外的隐私保护法律法规的变化和技术发展变化,基于法律法规的要求调整组织机构在数据分析过程中的隐私保护方案。（《要求》6.4.2.1 c）、d）、e））

c) 技术工具：

1) 提供对数据分析中的个人数据执行了匿名化处理的技术工具，即对任何个人识别信息（Personally Identifiable Information, 如姓名、地址、身份证号等）从数据中进行了去标识化处理。（《要求》6.4.2.1 c)、d)、e)）
2) 对数据分析过程的个人身份信息、重要或敏感数据的操作行为进行日志记录,以备对分析结果质量和真实性进行数据溯源。（《要求》6.4.2.1 e)）
3) 采用多种技术手段结合以降低数据分析过程中安全风险,比如基于机器学习的重要数据自动识别、数据安全分析算法设计、差分隐私保护、K 匿名（K-Anonymity）等。（《要求》6.4.2.1 c)、d)、e)、6.4.2.2 a)）
4) 对数据分析的结果数据进行扫描并采取必要的阻断措施,以保证大数据分析的结果不会构成对个人隐私、公司商业价值、以及国家安全的侵犯。（《要求》6.4.2.1 c)、d)、e)）
5) 建立了大数据分析过程的安全风险监控平台,对数据分析可能涉及的安全风险进行批量的分析和跟进。（《要求》6.4.2.1 c）、d）、e））

d) 人员能力：

1) 能够基于合规性要求、业界标准对大数据安全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。（《要求》6.4.2.1 a)、b)、c)、d)、e)）

2) 具备对大数据分析技术的深刻理解能力，能够及时跟进先进的最佳实践以保证对相关技术的合理应用。（《要求》6.4.2.1 c)、d)、e)）

### 7.4.3 数据正当使用

#### 7.4.3.1 数据安全过程域描述

基于国家相关法律法规对数据使用和分析处理的相关要求，通过对数据使用过程中的相关责任、机制的建立保证数据的正当使用。

#### 7.4.3.2 数据安全能力基本实践

a) 组织建设：
   1) 设置了明确的团队/岗位负责对数据的使用管理，该团队/岗位负责建立明确组织机构内部信息系统相关的用户身份管理和数据权限管理的原则及要求，并推进相关要求在各信息系统上的落地执行。（《要求》6.4.3.1 a)、b)）
   2) 组织机构内设立了统一的团队/岗位负责整体的身份及访问管理的原则并提供相关技术能力，并由各信息系统的管理人员负责对相关信息系统的具体的身份及访问管理。（《要求》6.4.3.1 a）、b）、c））
b) 制度流程：
   1) 制定了组织机构整体的数据权限管理制度，该制度对数据使用和分析处理的目的和范围符合网络安全法等国家相关法律法规要求，以及组织机构内身份及访问权限的授予、变更、撤销提出了的全生命周期的管理要求和责任制。（《要求》6.4.3.1 a)、b)）
   2) 组织机构定义了统一的身份及访问管理流程，各系统均遵循规范的身份及访问管理流程对用户访问数据资源进行管理，并定期审核当前的数据资源访问权限是否符合身份及访问管理的规范要求，身份及访问管理应遵循最小够用和职责分离的原则。（《要求》6.4.3.1 c)）
   3) 建立数据使用正当性的内部责任制度，保证在数据使用声明的目的和范围内对受保护的个人信息、重要数据等数据进行使用和分析处理。（《要求》6.4.3.1 b））
c) 技术工具：
   1) 建立组织机构内部统一的身份及访问管理平台，组织机构内部所有信息系统接入了组织机构的统一身份及访问管理系统（因特殊原因而无需接入同一身份及访问管理的信息系统除外，如基于国家合规需求必须与其它网络物理隔离的信息系统），实现唯一的用户身份标识，能够通过账号追溯到组织机构内部唯一的人员，并能识别内部人员身份的冒用、转借风险。（《要求》6.4.3.1 c)）
   2) 针对关键的系统采用多因素认证的方式进行身份认证，如可信的数字证书、生物识别方式等。（《要求》6.4.3.1 c)）
   3) 通过身份及访问管理平台对各系统的用户和数据资源进行权限管理，遵循最小够用的原则，并依据数据使用目的建立相应强度或粒度的访问控制机制（《要求》6.4.3.1 c)）
   4) 完整记录数据使用过程的操作日志，以备潜在违约使用者责任的识别和追责。（《要求》6.4.3.1 d)）
   5) 集中身份及访问管理平台对权限的授予均设置了时间期限，通过合理的到期提醒督促、管理权限的回收工作。（《要求》6.4.3.1 c)）
   6) 根据组织机构内部的数据权限管理需求，对数据权限执行细粒度的访问控制，如实现列级别的访问控制管理，并对数据滥用行为进行有效的识别、监控和预警，并能够结合数据使用的场景分析与违约、缔约过失和侵权相关的风险。（《要求》6.4.3.2 a)、b)）

7) 研究并利用新的技术对用户的身份及访问管理能力进行提升，并通过风险监控与审计实现对数据正当使用相关的风险的自动化分析和处理。（《要求》6.4.3.2 a）、b））

d) 人员能力：

1) 负责该项工作的人员了解身份及访问管理的基本原理，并能够在不同的业务场景中识别出组织机构内部身份及访问管理的需求并建立有效的身份及访问管理方案。(《要求》6.4.3.1 c))

2) 负责该项工作的人员具备对数据正当使用的相关风险的分析和跟进能力。(《要求》6.4.3.2 a)、b))

### 7.4.4 密文数据处理

#### 7.4.4.1 数据安全过程域描述

通过建立适合组织机构内数据服务特点的数据加密和解密处理策略和密钥管理规范，以防止重要或敏感数据在加工处理过程的泄漏风险。

#### 7.4.4.2 数据安全能力基本实践

a) 组织建设：组织机构内明确了团队/岗位对组织机构的数据加密处理负责。（《要求》6.4.4.1 a））

b) 制度流程：

1) 基于组织机构内部的数据处理所面临的合规性要求，在数据分类分级定义的基础上明确提出对各类各级别数据的加密要求，针对数据的加密要求应包含对数据加密算法的要求和数据加密密钥的管理要求，如对密钥使用时长的要求。（《要求》6.4.4.1 a)）

2) 密切关注国内外最新的数据加密技术发展情况，适当的采纳并用于组织机构内部的数据加密管理。（《要求》6.4.4.1 a））

c) 技术工具：

1) 建立有效的数据加密工具，并提供有效的密钥管理机制已实现对密钥的全生命周期（存储、使用、分发、更新和销毁）的安全管理。（《要求》6.4.4.1 a)）

2) 组织机构提供固定的数据加密模块供处理功能的开发人员调用，该模块可自动识别数据的类型和级别进行数据加密处理，从而保证数据的加密功能的统一性。(《要求》6.4.4.1 a)）

3) 具备对密文数据进行搜索、排序、计算等透明处理的能力。（《要求》6.4.4.2 a））

d) 人员能力：

1) 负责该项工作的人员熟悉各类数据加密算法的性能和瓶颈，并能够基于业务发展的需求、合规的需求制定有效的数据加密方案。（《要求》6.4.4.1 a)）

2) 面向数据开发人员、数据库管理人员及数据加工人员开展数据加密管理的培训，使其了解了数据加密算法所适合的应用场景。（《要求》6.4.4.1 a)）

### 7.4.5 数据脱敏处理

#### 7.4.5.1 数据安全过程域描述

遵守法律法规及相关标准的要求，根据数据使用过程中的安全和业务需求，明确敏感数据的脱敏需求，制定相应脱敏规则，对敏感数据进行脱敏处理以保证数据的可用性和安全性的平衡。

#### 7.4.5.2 数据安全能力基本实践

a) 组织建设：组织机构内设立了统一的团队/岗位，明确数据脱敏的原则、方法并提供相关技术

能力，并由数据的管理/安全管理团队/岗位负责实际场景下的数据的脱敏管理。（《要求》6.4.5.1 a）、b）、c））

b) 制度流程：

1) 建立组织机构的数据脱敏规范，在规范中明确需要脱敏的数据资产脱敏场景，给出不同分类分级数据的脱敏处理流程，以及数据脱敏的需求、规则和方式。（《要求》6.4.5.1 a)、b)）

2) 数据权限申请阶段由该数据的管理/安全管理团队/岗位判断申请人员对数据的使用场景是否要求对真实数据进行访问，若可采用数据脱敏则进一步判断该场景下适用的数据脱敏规则及方法。（《要求》6.4.5.1 b)）

3) 明确脱敏数据治理原则和规范，在脱敏策略、评估指标、评估分析和评估方法等方面反映脱敏治理效果。（《要求》6.4.5.1 a)、6.4.5.2 c)）

4) 针对组织机构内部的数据分类分级要求，明确定义数据资产需要脱敏的业务场景，并对各类型各级别的数据建立相应的脱敏处理流程。（《要求》6.4.5.2 a））

c) 技术工具：

1) 组织机构提供统一的数据脱敏工具，配置数据脱敏服务组件或技术手段,支持如泛化、抑制、干扰等数据脱敏技术，实现数据脱敏工具与数据权限管理平台的联动，以实现数据使用前的静态脱敏。（《要求》6.4.5.1 c)）

2) 数据脱敏的工具开放面向使用者的定制化功能,可以基于脱敏场景的需求实现对原有定制规则的改动。（《要求》6.4.5.1 c)）

3) 能够在屏蔽信息时保留其原始数据格式和特定属性,以满足基于脱敏数据的开发与测试要求。（《要求》6.4.5.1 d)）

4) 对数据脱敏处理过程相应的操作日志进行记录,以满足数据脱敏处理安全审计要求。(《要求》6.4.5.1 e)）

5) 配置基于策略的数据脱敏支持服务组件或技术手段,针对特定的数据使用场景和数据脱敏的策略，部署数据的动态脱敏方案，并保证数据脱敏的有效性和合规性。(《要求》6.4.5.2 b)、d)）

6) 密切关注行业内在数据脱敏领域的最新实践和技术发展,建立适用于组织机构内各类电子数据的数据脱敏技术方案。（《要求》6.4.5.2 b）、d））

d) 人员能力：

1) 熟悉常规的数据脱敏技术，能够分析数据脱敏过程中存在的安全风险，并能够基于数据脱敏的具体场景保证业务和安全之间的有效平衡。（《要求》6.4.5.1 a)、b)、c)、d)）

2) 通过培训宣贯保证在各类场景下负责数据脱敏功能实现的人员对脱敏规则理解的一致性。（《要求》6.4.5.1 a)、b)）

3) 具备对数据脱敏的技术方案定制化的能力,能够基于组织机构内部各级别的数据建立有效的数据脱敏方案降低相应的风险。（《要求》6.4.5.2 a)）

### 7.4.6 数据溯源

#### 7.4.6.1 数据安全过程域描述

通过针对数据处理过程中产生的数据的溯源机制的建立,以实现对数据处理过程中涉及数据源的可追溯性。

#### 7.4.6.2 数据安全能力基本实践

a) 组织建设：组织机构设立了负责数据源追溯性管理的团队，提供统一的数据源管理的有效方案和策略。（《要求》6.4.6.1 a））

b) 制度流程：

1) 制定数据源管理的制度规范，明确定义数据溯源策略和溯源机制，溯源数据表达方式和格式规范，以及溯源数据安全存储与使用的管理制度，以规范化组织、存储和管理溯源数据。（《要求》6.4.6.1 a)、b)）

2) 建立基于溯源数据的数据业务与法律法规合规性审核机制,并依据审核结果增强或改进数据服务相关的访问控制与合规性保障机制和策略。(《要求》6.4.6.2 b)）

3) 基于业务的发展变化以及行业最佳实践，提升采集数据源可追溯性管理的有效性。(《要求》6.4.6.1 a))

c) 技术工具：

1) 提供了有效的技术工具针对分布式处理环境下，或离线分析过程中数据生成相关的数据源及其类型进行识别和记录，即通过数据溯源的机制能够保证数据分析团队能够明确追踪其加工计算生成数据相关的数据源，如追溯操作发起者及发起时间等。(《要求》6.4.6.1 c)）

2) 提供工具对关键溯源数据进行备份，并采取技术手段对溯源数据进行安全保护。（《要求》6.4.6.1 d)）

3) 关键的数据管理平台 / 系统中提供了管控措施，执行对溯源数据的授权访问、备份和校验，保证溯源数据的完整性和保密性。（《要求》6.4.6.1 d）、6.4.6.2 a））

d) 人员能力：负责该项工作的人员能够理解组织机构内部数据采集的业务场景，从而能够结合实际情况执行落地执行的方案。（《要求》6.4.6.1 a)、b)、c)、d)）

## 7.5 数据交换安全

### 7.5.1 数据导入导出安全

#### 7.5.1.1 数据安全过程域描述

通过对数据导入、导出过程中对数据的安全性的管理，防止相关过程中可能对数据自身的可用性和完整性构成的危害、以及可能会存在的数据泄漏风险。

#### 7.5.1.2 数据安全能力基本实践

a) 组织建设：设立了统一的数据导入导出过程的安全管理的团队负责相关原则和技术能力的提供，并推广相关要求在组织机构内的相关业务场景的落地执行。（《要求》6.5.1.1 a））

b) 制度流程：

1) 建立数据导入导出的安全制度规范，基于组织机构的数据分类分级要求定义数据导入导出相关的安全策略（如访问控制策略、不一致处理策略、流程控制策略、审计策略、日志管理策略）。（《要求》6.5.1.1 b）、f））

2) 建立规范的数据导入导出的安全审核和授权流程，流程中包括但不限于数据导入导出的业务方、数据在组织机构内部的管理方、相应的安全管理团队，以及根据组织机构数据导入导出的规范要求所需参与具体风险判定的相关方，如法律团队、对外公关团队、财务数据对外管理团队等其他重要的与数据价值保护相关的团队。（《要求》6.5.1.1 c））

3) 建立针对导出数据介质的标识规范，明确介质的命名规则、标识属性等重要信息，定期验证导出数据的完整性和可用性。（《要求》6.5.1.1 e)）

4) 及时跟进业务相关的法律法规的更新和产业内的优秀做法，定期评估数据导入机制、服务组件和共享通道的安全性，对数据导入导出的风险控制方案进行持续的优化调整。(《要求》6.5.1.1 a)、b)、c))

c) 技术工具：

1) 建立数据导入导出审核流程的在线平台，组织机构内部的对数据导入导出可通过平台进行审核并详细记录，确保没有超出大数据服务提供者的数据授权使用范围。(《要求》6.5.1.1 c))

2) 建立针对数据导入导出过程的安全技术方案，对数据导入导出终端、用户或服务组件执行有效的访问控制，实现对其身份的真实性和合法性的保证；对关键的敏感数据在导入导出的过程采用数据加密的手段，以保证数据在导入导出过程中的保密性、完整性和可用性；对数据导出导出通道进行有效的缓存数据清除，以保证导入导出过程中涉及的数据不会被恶意恢复。（《要求》6.5.1.1 d)、g)、h)）

3) 针对数据导入导出的日志建立相应的管理和审计方案，以保证对对导入导出过程中的相关日志信息的有效记录，并通过定期的审计工作开展发现其中存在的安全风险。（《要求》6.5.1.1 f)）

4) 在组织机构统一的对数据导入导出的原则和规范要求下，采取多因素鉴别技术对数据导入导出操作员进行身份鉴别，为数据导入导出通道提供冗余备份能力，确保数据安全可靠导入导出要求；对数据导入导出接口进行流量过载监控，确保海量数据导入过程安全可控。（《要求》6.5.1.2 a)、b)、c)）

5) 组织机构在数据导入导出审核平台上对各类审核流程中应关注的安全风险进行提示，以辅助审核人员进行风险的评估，提升审核的准确度和效率；配置专业数据导入机制或服务组件，明确数据导入导出最低安全防护基线要求。（《要求》6.5.1.1 c））

d) 人员能力：

1) 负责该项工作的人员能够充分理解组织机构的数据导入导出策略，并根据数据导入导出的业务场景执行相应的风险评估，从而提出实际的解决方案。（《要求》6.5.1.1 f））

2) 针对数据导入导出的原则在全组织范围内进行了培训和推广，以保证组织机构的人员在数据导入导出方面具有一定的安全意识水平。（《要求》6.5.1.1 f)）

### 7.5.2 数据共享安全

#### 7.5.2.1 数据安全过程域描述

通过在业务系统、产品对外部客户提供数据时，以及通过合作的方式与第三方合作伙伴交换数据时，执行对数据交换过程的安全风险控制，以实现对数据价值保护的有效性、对法律法规的符合性。

#### 7.5.2.2 数据安全能力基本实践

a) 组织建设：组织机构设立了统一的数据共享过程的安全管理的团队负责相关原则和技术能力的提供，并推广相关要求在组织机构内的相关业务场景的落地执行。（《要求》6.5.2.1 a)、d)、e)）

b) 制度流程：

1) 制定了数据共享的原则及数据保护措施，该要求从国家安全、组织机构的核心价值保护、个人信息保护等方面的数据共享的风险控制提出了要求，明确数据共享涉及机构或部门相关职责和权限，明确共享数据相关的使用者的数据保护责任，确保数据使用的相关方具有对共享数据的足够的保护能力；对数据共享涉及的数据类型、数据内容、数据格式、以及对数据共享的常见场景制定了细化的规范要求从而保障数据共享安全策略的有效性。(《要求》6.5.2.1 a)、d)、e)、i)）

2) 建立了规范的数据共享的审核流程，审核流程中包括但不限于数据共享的业务方、共享数据在组织机构内部的管理方、数据共享的安全管理团队，以及根据组织机构数据共享的规范要求所需参与具体风险判定的相关方，如法律团队、对外公关团队、财务数据对外管理

团队等其他重要的与数据价值保护相关的团队，确保共享的数据未超出授权范围。（《要求》6.5.2.1 a)、d)、e)）

3) 制定了数据共享审计策略和审计日志管理规范，明确审计记录要求，为数据共享安全事件的处置、应急响应和事后调查提供帮助。（《要求》6.5.2.1 g)）

4) 在组织机构统一的对数据共享的原则和规范要求下，针对关键的数据共享场景制定了细则，如对外的数据产品/服务的安全细则、对政府机构的数据共享安全细则等。(《要求》6.5.2.1 a)、d)、e)）

5) 建立对数据共享机制、相关共享组件和共享通道的安全性评估机制，以保证对相关安全风险的持续可控。（《要求》6.5.2.2 a)）

6) 及时跟进业务相关的法律法规的更新和产业内的优秀做法，定期评估数据共享机制、服务组件和共享通道的安全性，对数据共享的风险控制方案进行持续的优化调整。(《要求》6.5.2.2 a) ）

c) 技术工具：

1) 建立了数据共享审核流程的在线平台，组织机构内部的对外数据共享可通过平台进行审核并详细记录，确保没有超出大数据服务提供者的数据所有权和授权使用范围。（《要求》6.5.2.1 a)、d)、e)）

2) 利用数据加密、安全通道等措施保护数据共享过程中的个人信息、重要数据等敏感信息。（《要求》6.5.2.1 f））

3) 建立数据共享过程的监控工具，对共享数据及数据共享服务过程进行监控，确保共享的数据未超出授权范围。（《要求》6.5.2.1 h））

4) 建立数据共享审计和审计日志管理规的工具，明确审计记录要求，为数据共享安全事件的处置、应急响应和事后调查提供帮助。（《要求》6.5.2.1 g））

5) 在数据共享审核平台上对各类审核流程中应关注的安全风险进行提示，以辅助审核人员进行风险的评估，提升审核的准确度和效率；配置专业数据共享机制或服务组件，明确数据共享最低安全防护基线要求。(《要求》6.5.2.1 a)、d)、e)、6.5.2.2 b))

d) 人员能力：

1) 具备对数据共享业务场景的理解能力，能够结合合规性要求给出适当的安全解决方案，确保共享数据使用者具备与大数据服务提供者具有足够或相当的数据安全防护能力。(《要求》6.5.2.1 a)、d)、e))

2) 能够充分理解组织机构的数据共享策略，并根据数据共享的业务场景执行相应的风险评估，从而提出实际的解决方案。（《要求》6.5.2.1 a)、d)、e)）

3) 针对数据共享的原则在全组织范围内进行了培训和推广，以保证组织机构的人员在数据共享方面具有一定的安全意识水平。（《要求》6.5.2.1 a)、b)、c)、d)、e)、g)）

### 7.5.3 数据发布安全

#### 7.5.3.1 数据安全过程域描述

通过在数据发布的过程中对发布数据的格式、适应范围、发布者与使用者权利和义务执行的必要控制，以实现数据发布过程中数据的安全可控与合规。

#### 7.5.3.2 数据安全能力等级描述

a) 组织建设：

1) 组织机构设立负责数据发布安全管理的团队，由该团队负责制定整体的规则并推广相关流程的推行。（《要求》6.5.3.1 a) ）

2) 指定专人负责数据发布信息的披露，并且对数据披露人员进行安全培训。(《要求》6.5.3.1

f））

b） 制度流程：

1） 依据相关法律法规，制定数据资源公开发布的审核制度与流程，确保数据发布有审核记录；针对每一次发布，明确数据资源公开内容、适用范围及规范，发布者与使用者权利和义务。（《要求》6.5.3.1 a）、b）、c））

2） 建立数据资源公开事件应急处理流程，包括必要措施使处理流程快速有效。(《要求》6.5.3.1 d））

3） 建立对公开发布的数据资源的定期审查机制，定期审查其中是否含有非公开信息，并采取相关措施确保发布数据使用的合规性。（《要求》6.5.3.1 g））

4） 细化制定了各类数据发布的审核流程，从审核的有效性和审核的效率层面充分考虑流程节点的制定。（《要求》6.5.3.1 a）、b））

c） 技术工具：

1） 建立数据资源公开数据库，通过大数据发布平台服务实现公开数据资源登记、用户注册等共享数据和共享组件的验证互认机制。（《要求》6.5.3.1 e））

2） 依法通过大数据发布平台服务实现大数据服务相关数据资源公告、资格审查、成交信息、履约信息等数据发布信息。（《要求》6.5.3.1 c））

3） 建立数据资源公开事件应急处理平台，支持采取必要措施使应急处理流程快速有效。(《要求》6.5.3.1 d））

4） 在数据发布平台上对各类审核流程中应关注的安全风险进行提示，以辅助审核人员进行风险的评估，提升审核的准确度和效率。（《要求》6.5.3.1 a）、b）、c)、g））

5） 建立数据资源发布接口及发布数据格式规范，如提供机器可读的可扩展标记语言格式，确保用户能高效获取开放数据资源。(《要求》6.5.3.2 a)）

d） 人员能力：负责该项工作的人员充分理解数据安全发布的制度和流程，通过了岗位能力测试，并能够根据实际发布要求建立相应的应急方案。（《要求》6.5.3.1 a）、b）、c））

### 7.5.4 数据交换监控

#### 7.5.4.1 数据安全过程域描述

通过建立组织机构和外部组织机构/个人之间数据交换监控机制，以实现对数据交换过程中可能存在的数据滥用、数据泄漏等安全风险的防控。

#### 7.5.4.2 数据安全能力基本实践

a） 组织建设：组织机构设立负责数据交换监控审计岗位，由该岗位负责数据交换监控审计工作。（《要求》6.5.4.1 a)、b））

b） 制度流程：

1) 制定数据交换风险行为识别和评估规则，并不断进行完善和优化。(《要求》6.5.4.1 a)、b))

2) 定期对数据交换行为进行人工审计。(《要求》6.5.4.1 a)、b))

c） 技术工具：

1) 建立数据交换监控平台，监控高风险数据交换操作；数据交换监控平台提供的功能包括但不限于：实时记录及报告个人信息、重要数据等的外发行为；记录交换服务流量数据；建立数据处理平台对被监控的数据交换服务流量数据进行数据安全分析。(《要求》6.5.4.1 a)、c)、d))

2) 基于数据交换监控平台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，且实现对异常或高风险数据交换操作的自动化识别和实时预警能

力。（《要求》6.5.4.2 a)、b)）

3) 参与行业内对数据交换监控的解决方案的交流，实施跟进国内外的最佳实践，结合组织机构的业务现状不断优化监控方案。（《要求》6.5.4.1 a)、b)）

d) 人员能力：负责该项工作的人员充分理解数据监控审计要求，能够识别数据泄露风险。（《要求》6.5.4.1 a)、b)）

## 7.6 数据销毁安全

### 7.6.1 介质使用管理

#### 7.6.1.1 数据安全过程域描述

针对组织机构内需要对大数据存储介质进行访问和使用的场景，提供有效的制度流程和技术工具保证，防止对介质的不当使用而可能引发的数据泄露风险。

#### 7.6.1.2 数据安全能力基本实践

a) 组织建设：组织机构设立统一的负责介质使用管理的团队/岗位，该团队整体把控组织机构内部介质使用的原则，并明确各类介质使用的规范做法。由介质使用管理、维护团队依据相关要求负责执行落地。（《要求》6.6.1.1 a））

b) 制度流程：

1) 基于组织机构的数据分类分级要求以及介质使用的要求，建立大数据服务存储介质访问和使用安全策略和管理规范，并制定了介质使用的审批和记录流程。（《要求》6.6.1.1 a)）

2) 建立购买或获取存储介质的规范流程，要求通过可信渠道购买或获获取存储介质，并针对各类存储介质建立标准的存储介质净化规程。（《要求》6.6.1.1 b)）

3) 建立存储介质的标记规程，明确介质存储的数据对象，并对介质访问和使用行为进行记录和审计。（《要求》6.6.1.1 c)）

4) 建立对存储介质使用的常规和随机检查流程，确保存储介质的使用遵守机构公布的关于介质的使用规范。（《要求》6.6.1.1 d)）

c) 技术工具：

1) 组织机构采取有效的介质净化工具对存储介质进行净化处理。（《要求》6.6.1.1 b)）

2) 建立介质管理系统，确保存储介质的使用和传递过程得到跟踪。（《要求》6.6.1.2 a)）

3) 持续更新优化组织机构介质管理系统和净化工具，以保证介质的安全使用。（《要求》6.6.1.1 b)、c)、d)、6.6.1.2 a)）

d) 人员能力：负责该项工作的人员熟悉介质使用的相关合规要求，熟悉不同存储介质访问和使用的差异性，能够主动根据政策变化更新管理要求。（《要求》6.6.1.1 a)、b)、c)、d)）

### 7.6.2 数据销毁处置

#### 7.6.2.1 数据安全过程域描述

通过建立针对数据内容的清除、净化机制，实现对数据的有效销毁，防止因对存储介质上的数据内容的恶意恢复而导致的数据泄漏风险。

#### 7.6.2.2 数据安全能力基本实践

a) 组织建设：组织机构设立统一的负责数据安全销毁管理的团队/岗位，该团队整体把控组织机构内部数据销毁的原则，并明确各类数据销毁的规范做法。由各业务团队的数据管理人员和数据介质的管理、维护团队依据相关要求负责执行落地。（《要求》6.6.2.1 a）、b））

b) 制度流程：

1) 基于组织机构的数据安全分类分级的要求以及各类数据销毁手段的特点，按照国家相关法律和标准对个人信息、重要数据等敏感信息的销毁要求，并结合组织机构的财务成本考虑，

组织机构制定了数据的销毁指引，明确了符合组织机构业务需求和法律合规需求的各类数据销毁的场景以及销毁的手段，并制定了数据销毁执行时的审批和记录流程。（《要求》6.6.2.1 a)、c)、g)）

2) 建立相应的数据销毁机制，明确销毁方式和销毁要求，设置销毁相关监督角色，监督操作过程，并对审批和销毁过程进行记录控制。（《要求》6.6.2.1 b)、c)）

3) 制定详细的数据销毁指引，明确提出针对主要介质所存储数据的销毁方法和技术，如针对网络存储数据以及针对闪存、硬盘、磁带、光盘等存储数据所应采用的硬销毁和软销毁的方法和技术，采用基于安全策略、分布式杂凑算法等网络数据分布式存储的销毁策略与机制。（《要求》6.6.2.1 d)、e)）

4) 建立数据销毁效果评估机制，对已经完成数据销毁的存储介质进行抽样的销毁效果进行认定，以保证对数据销毁工具的持续改进和销毁方案的整体优化；同时，建立已共享或者已被其他用户使用的数据销毁管控措施（《要求》6.6.2.2 a)、b)、c)）

5) 定期审核数据存储时长的情况，考虑数据存储成本的需求、法律法规和更新合同的需求，以及相关数据销毁技术的发展现状，对数据销毁的整体方案进行及时更新。(《要求》6.6.2.1 c)）

c) 技术工具：

1) 提供了与数据销毁指引相配套的各类数据销毁的技术工具（如针对网络存储数据、针对闪存、硬盘、磁带、光盘等存储数据），从而供数据销毁的执行人员利用规范的工具产品执行数据的销毁，确保以不可逆方式销毁数据及其副本内容，从而保证对同类场景下的数据销毁效果的一致性。(《要求》6.6.2.1 f)）

2) 数据资产管理平台能够对数据的销毁需求进行明确的标识，并可通过该系统提醒数据管理者及时发起对数据的销毁。(《要求》6.6.2.1 c)）

d) 人员能力：负责该项工作的人员熟悉数据销毁的相关合规要求，熟悉不同业务对数据销毁需求的差异性，能够主动根据政策变化和技术发展更新相关知识和技能。（《要求》6.6.2.1 a)、b)、c)、d)、e)、f)、g)）

### 7.6.3 介质销毁处置

#### 7.6.3.1 数据安全过程域描述

通过建立对介质的安全销毁的规程和技术手段，防止因介质丢失、被窃或未授权的物理访问而导致的介质中的数据面临泄漏的安全风险。

#### 7.6.3.2 数据安全能力基本实践

a) 组织建设：组织机构设立统一的负责数据安全销毁管理的团队/岗位，该团队整体把控组织机构内部数据销毁的原则，并明确各类数据销毁的规范做法，以及在数据销毁的前提下执行介质销毁的要求。由各业务团队的数据管理人员和数据介质的管理、维护团队依据相关要求负责执行落地。（《要求》6.6.3.1 a））

b) 制度流程：

1) 制定介质销毁的管理制度，明确介质销毁处理策略、管理制度和机制，明确销毁对象和流程，同时依据介质存储内容的重要性明确磁介质、光介质和半导体介质销毁方法和机制。（《要求》6.6.3.1 a)、b)）

2) 制定对存储介质进行销毁的监管机制，确保对销毁介质登记、审批、交接等介质销毁过程监控，并按照国家相关法律和标准销毁存储介质、加强对介质销毁人员监管。（《要求》6.6.3.1 c)、d)）

3) 建立对销毁过程的监控机制，实现对介质销毁效果进行认定；同时定期执行介质销毁记录

的检查，以保证相关记录工作的规范性执行。（《要求》6.6.3.1 c）、6.6.3.2 b））

c) 技术工具：

1) 组织机构提供了统一的介质销毁工具，包括但不限于物理摧毁、消磁设备等工具，实现基于各类介质（如针对磁介质、光介质和半导体介质）的有效销毁。（《要求》6.6.3.1 b））

2) 使用国家权威机构认证的机构或设备对存储介质设备进行物理销毁或联系国家认定资质的销毁服务提供商执行存储介质的销毁工作。（《要求》6.6.3.2 a)、c)）

3) 持续更新组织机构的介质销毁的技术工具，以保证介质销毁的效果。(《要求》6.6.3.1 b))

d) 人员能力：负责该项工作的人员能够依据数据销毁的整体需求明确使用的介质销毁工具。(《要求》6.6.3.1 a）、b））

# 附 录 A
# （资料性附录）
# 等级评定方法

组织机构的数据安全能力成熟度等级取决于各项数据安全过程域的能力成熟度等级。本标准采用“木桶效应”的等级评定方法，组织机构整体的能力成熟度取决于各项数据安全规程域的能力成熟度级别中的最低级别。

比如，当所有的数据安全过程域的能力成熟度都达到2级及以上时，组织机构的大数据安全能力成熟度级别方可为2级。

# 附 录 B
（资料性附录）
模型使用方法

由于各组织机构在业务规模、业务对数据的依赖性、以及组织机构对数据安全工作定位等方向的差异，组织机构对模型的使用需要“因地制宜”。

使用模型时，组织机构应首先明确其数据安全能力的目标成熟度级别。根据对组织机构整体的数据安全能力成熟度级别的定义（见“4.4.1 等级定义”），组织机构可以选择适合自己业务实际情况的短期目标和长期目标。本标准定义的数据安全能力成熟度级别中，3 级目标适用于所有具备数据安全管理需求的组织机构作为自己的短期目标/长期目标，具备了 3 级的数据安全能力则意味着组织机构能够针对数据安全的各方面风险进行有效的控制。然而，对于业务中尚未大量依赖于大数据技术的组织机构而言，数据仍然倾向于在固有的业务环节中流动，其数据安全管理的需求整体弱于强依赖于大数据技术的组织机构，因此其短期目标可先定位为 2 级，待达到 2 级的目标之后再进一步提升到 3 级的能力。

在确定目标成熟度级别的前提下，组织机构根据数据生命周期所覆盖的业务场景挑选适用于组织机构的数据安全过程域。例如组织机构 A 不存在与外部组织机构之间交换数据加工的平台或并未与外部组织机构之间在某个大数据加工平台上交换数据并混合加工，因此“大数据交换加工平台” 就可以从评估范围中剔除掉。

接着，组织机构基于对成熟度模型内容的理解，识别数据安全能力现状并分析与目标能力等级之间的差异，在此基础上进行数据安全能力的整改提升计划。而伴随着组织机构业务的发展变化，组织机构也需要定期复核、明确自己的目标成熟度等级，然后开始新一轮目标达成的工作。组织机构使用模型的闭环如图 5 所示。

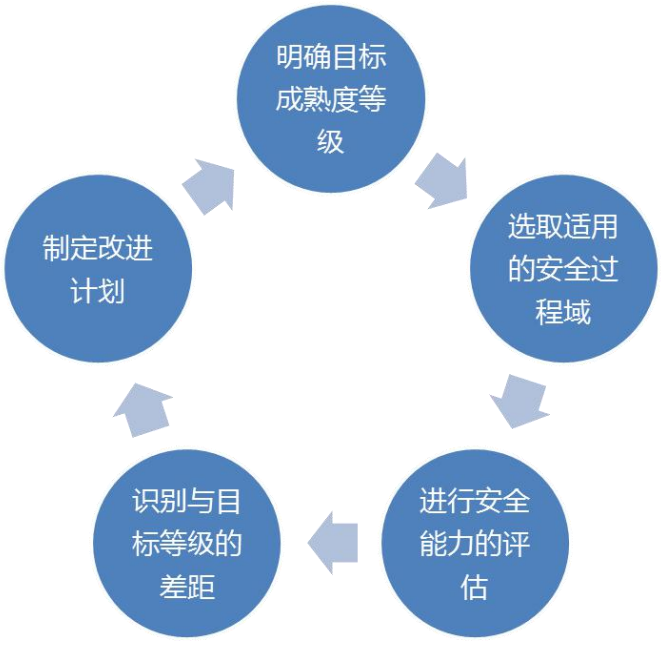


图 3 推荐的成熟度模型使用步骤