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

（送审稿-修订中）

20118-03-09

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、北京奇安信科技有限公司、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、阿里云计算有限公司、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、华为技术有限公司、三六零科技股份有限公司。

本标准主要起草人：朱红儒、刘贤刚、李克鹏、叶润国、梅婧婷、胡影、叶晓俊、薛勇、谢安明、贾雪飞、孙明亮、潘亮、郑新华、郑斌、柯妍、徐雨晴、宋玲娓、杜跃进、苗光胜、刘玉岭、侯金刚、潘正泰、张锐卿、任卫红、金涛、任兰芳、常玲、赵蓓、张大江、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、王川、周薇茹、杜青峰、薛坤、程瑜琦、尤其、王伟、张屹、何军。

引　言

随着互联网、物联网、云计算等技术的快速发展，以及智能终端、网络社会、数字地球等信息体的普及和建设，全球数据量出现爆炸式增长，形成了大数据环境。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。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。各组织机构在大数据产业中提供或获取各种数据服务，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，定义数据安全保障的模型框架和方法论，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 AAAAA—AAAA信息安全技术　个人信息安全规范

GB/T BBBBB—BBBB信息安全技术 大数据服务安全能力要求

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

基本实践 base practices

是实现某一安全目标的数据安全相关的活动和过程，一个过程域由若干个基本实践组成。

3.1.8

通用实践 genericpractices

在评估中用于确定任何过程实施能力的评定准则。

3.1.9

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。

3.1.10

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。

3.1.11

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。

3.1.12

数据供应链 data supply chain

指为满足数据供应关系，通过资源和过程将需方、供方相互连接的网链结构，可用于供方将数据及其产品与服务提供给需方。

3.1.13

动态数据 active data

被存储在非持久性数字状态，通常指在计算机的随机存取存储器（RAM），CPU高速缓存，或CPU寄存器的活性数据。

3.1.14

合规 compliance

对数据安全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：

BP	基本实践（Base Practice）
CMM	能力成熟度模型（Capability Maturity Model）
DS-CMM	数据安全能力成熟度模型（Data Security Capability Maturity Model）
GP	通用实践（Generic Practice）
PA	过程域（Process Area）

4 数据安全能力成熟度模型架构

4.1 概述

本标准主要根据《信息安全技术 大数据服务安全能力要求》（以下简称为《要求》）中的数据安全要求对组织机构提供的数据安全能力提出评估的模型框架及方法论。《要求》中定义了大数据服务提供者应具有的组织相关基础安全能力和数据生命周期相关的数据服务安全能力，本标准针对《要求》中定义的每个安全要求定义基本实践，并根据本标准定义的成熟度等级的通用实践，对基本实践进行等级评估。

本标准阐述了数据安全能力评估的成熟度模型及方法论，在过程域层面与《要求》完全一致，在基本实践层面与《要求》进行映射，两标准可以相互支撑调用。《要求》中定义了大数据服务提供者提供大数据服务所需要满足的基线要求，本标准定义了组织机构持续实现安全过程、满足安全要求的能力等级的评估方法，来指导组织机构提升自身的数据安全能力水平。

4.2 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《要求》中的安全要求为基础，定义数据安全过程域和基本实践，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（DS-CMM）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，明确为组织建设、制度流程、技术工具和人员能力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五个级别的能力成熟度分级要求。

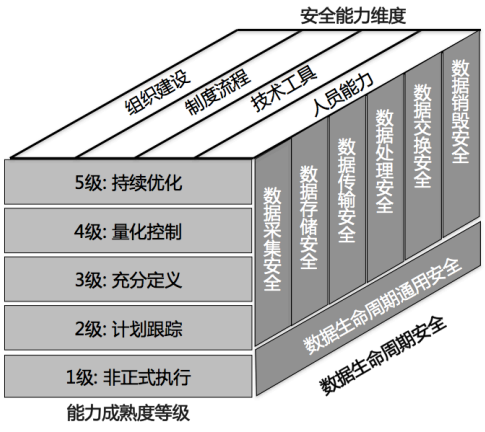

图1　数据安全能力成熟度模型架构

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，明确定义数据生命周期各阶段安全的过程域和数据生命周期通用安全的过程域。数据生命周期各阶段安全的过程域，包括数据采集、数据传输、数据存储、数据处理、数据交换和数据销毁这六个阶段中的过程域。数据生命周期通用安全的过程域，是与各个生命周期都相关的过程域，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，对数据生命周期各阶段安全的基本实践和数据生命周期通用安全的基本实践，进行能力成熟度等级评估。

对能力成熟度等级维和数据安全过程域维之间的映射关系，如图 2 所示。

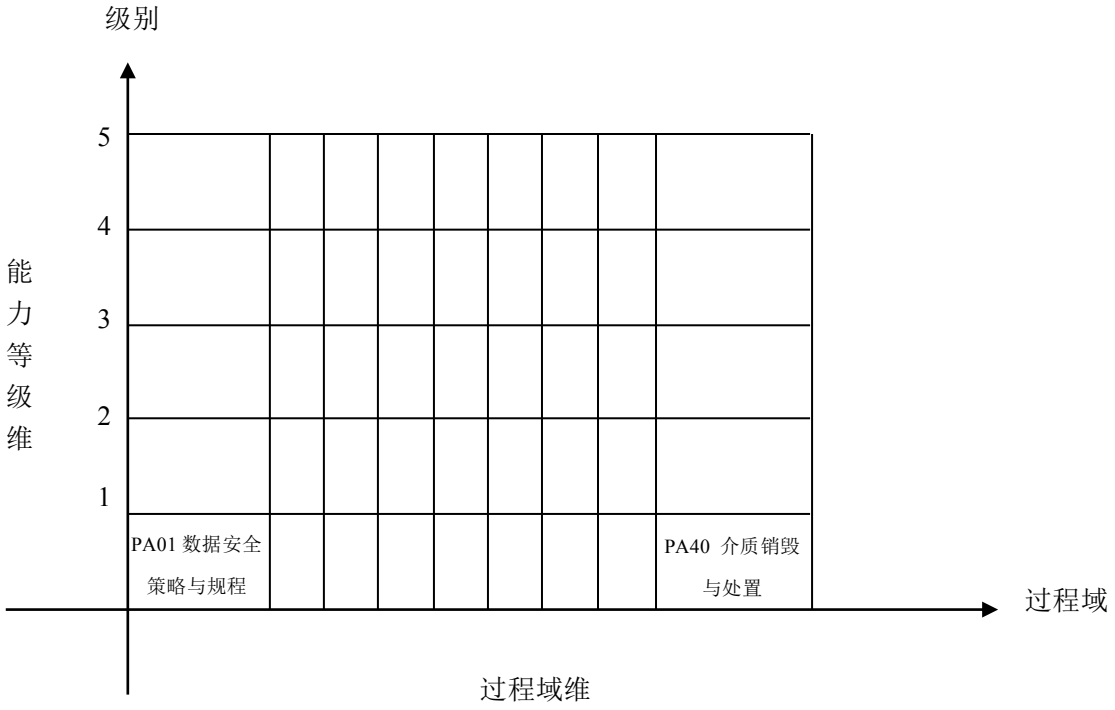

图2　能力等级维与过程域维的映射关系

其中，能力等级维由公共特征构成，公共特征由通用实践（GP）构成。对于某一级别的所有通用实施满足该级别的公共特征，从而形成这一级别的能力。通用实践在本标准的第 5 章中进行了详细介绍。通用实践用 GP 来进行编号，第一位数字表明等级，第二位数字表明公共特征的序号，第三位数字表明通用实践的序号。比如，GP 2.1.1 表明等级 2（计划跟踪级）的公共特征 1（规划执行）的第一个，关于组织建设的通用实践。

过程域维由数据生命周期通用安全的过程域和数据生命周期各阶段安全的过程域（PA）组成，每个过程域由基本实践（BP）组成。每个过程域的基本实施（BP）是构成该过程域的基本要素，是完成该过程活动的基本单元。基本实践在本标准的第 6 章和第 7 章中进行了详细介绍。基本实践用 BP 来进行编号，第一位数字表明过程域（PA）的序号，第二位数字表明基本实践的序号。比如，BP.01.01 表明，过程域 PA01（数据安全策略与规程）中的第一个，关于组织建设的实践。

4.3 数据生命周期安全

4.3.1 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：指在组织机构内部系统中新生成数据，以及从外部收集数据的阶段。

——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阶段。

——数据存储：指数据以任何数字格式进行物理存储或云存储的阶段。

——数据处理：指组织机构在内部针对数据进行计算、分析、可视化等操作的阶段。

——数据交换：指数据由组织机构与外部组织机构及个人交互的阶段。

——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，使数据彻底消除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。

4.3.2 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，包含数据生命周期通用安全的过程域和数据生命周期各阶段安全的过程域，如图3所示。

图3 数据安全过程域体系

4.4 安全能力维度

4.4.1 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。

4.4.2 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。

4.4.3 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，从以下方面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。

4.4.4 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，从以下方面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和持续支持能力，对数据安全制度流程的固化执行能力。

4.4.5 人员能力

从组织机构承担数据安全工作的人员应具备的能力出发，从以下方面进行能力的级别区分：

——数据安全人员所具备的数据安全技能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。

4.5 成熟度等级定义

组织机构的数据安全能力成熟度模型分为五个成熟度等级，一级是非正式执行级，二级是计划跟踪级，三级是充分定义级，四级是量化控制级，五级是持续改进级。能力级别从一级至五级逐级提高，标志着组织机构的数据安全保障能力的成熟度不断提升。每个级别规定了对应的公共特征和通用实践。

对成熟度等级的描述如表 1 所示：

表 1. 成熟度等级描述

成熟度等级	详述	特征
等级 1: 非正式执行	• 执行基本实践：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”。	随机、无序、被动的执行安全过程，依赖于个人，经验无法复制。
等级 2: 计划跟踪	• 规划执行：对安全过程进行规划，提前分配资源和责任。 • 规范化执行：对安全过程进行控制，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。 • 验证执行：确认过程按照预定的方式执行，验证执行过程与	在项目级别主动实现了安全过程的计划与执行，没有形成体系

成熟度等级	详述	特征
	可应用的计划是一致的，对数据安全过程进行审计。 • 跟踪执行：控制数据安全项目的进展，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。	化。
等级 3: 充分定义	• 定义标准过程：组织机构对标准过程进行制度化，为组织机构定义标准化的过程文档，为满足特定用途对标准过程进行裁剪。 • 执行已定义的过程：充分定义的过程可重复执行，使用已定义的过程，针对有缺陷的过程结果和安全实践的核查，使用过程执行的结果数据。 • 协调安全实践：对业务系统和组织活动的协调，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。	在组织级别实现了安全过程的规范定义与执行。
等级 4: 量化控制	• 建立可测的安全目标：为组织机构的数据安全建立可测量目标。 • 客观地管理执行：确定过程能力的量化测量并使用量化测量来管理安全过程，以量化测量作为修正行动的基础。	建立了量化目标，安全过程可进行度量与预测。
等级 5: 持续优化	• 改进组织能力：在整个组织机构范围内标准过程的使用进行比较，寻找改进标准过程的机会，分析对标准过程的可能变更。 • 改进过程有效性：制定处于连续受控改进状态下的标准过程，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。	根据组织的整体目标，不断改进和优化安全过程。

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

在这一级别上，组织机构的数据安全管理过程域可被标识，相关基本实践通常在需要时被执行，但主要基于个人的的知识水平和经验判定，未经过严格的计划和跟踪。

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，仅在部分业务场景中/项目中根据临时的需求执行了相关实践，未形成成熟和稳定的机制保证实践持续有效进行,数据安全管理的一致性、有效性及质量可能波动很大,所执行的过程可称为“非正式过程”。

5.1.2.2 GP 1.1.1 组织建设

仅在部分业务场景/项目中根据临时的需求建立数据安全的岗位和人员，未形成成熟和稳定的专职/兼职的数据安全的岗位和人员。数据安全的组织建设未经严格的计划和跟踪。

5.1.2.3 GP 1.1.2 制度流程

仅在部分业务场景/项目中根据临时的需求建立数据安全的制度流程，未形成成熟和稳定的数据安全制度流程，多为对特定业务需求的响应而触发。数据安全的制度流程未经严格的计划和跟踪。

5.1.2.4 GP 1.1.3 技术工具

仅在部分业务场景/项目中根据临时的需求部署数据安全的技术工具，未形成成熟和稳定的技术工具来支撑数据安全工作，执行效果未经规范化的测量或验证。

5.1.2.5 GP 1.1.4 人员能力

从事数据安全工作的人员具备数据安全意识,但仅能支撑部分业务场景和项目工作，人员能力未得到有效的保障。

5.2 能力级别 2—计划跟踪

5.2.1 能力等级描述

在这一级别上，组织机构的数据安全过程域管理满足标准规范的规定，相关基本实践的执行是有计划和有跟踪的，并可对实践情况进行过程验证，与等级1“非正式执行”的主要区别是基本实践执行过程被规范的计划和管理。

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。

5.2.2 公共特征 2.1 —规划执行

5.2.2.1 公共特征描述

该公共特征的通用实践集中在过程域以及基本实践执行的规划方面，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指派，为规范化的过程执行提供了最根本的基础。

5.2.2.2 GP 2.1.1 组织建设

基于数据安全过程域的内容，应规划并设立数据安全管理岗位，该岗位人员负责制定和落实组织机构内部的数据安全管理规范。

5.2.2.3 GP 2.1.2 制度流程

建立以数据为中心的数据安全制度流程，将数据安全制度流程形成标准化文档，并按照规划方式执行。

5.2.2.4 GP 2.1.3 技术工具

为执行数据安全过程域基本实践提供合适的技术工具，确保数据安全过程的执行。

5.2.2.5 GP 2.1.4 人员能力

为执行数据安全过程域基本实践确定人员所需要具备的能力，规划和确保人员得到适当的培训。

5.2.3 公共特征 2.2 —规范化执行

5.2.3.1 公共特征描述

该公共特征的通用实践注重于对过程域的规范化管理，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。

5.2.3.2 GP 2.2.1 组织建设

建立规范化的数据安全管理的岗位，负责制定和落实数据安全过程域中的关键安全管理规则。

5.2.3.3 GP 2.2.2 制度流程

针对该数据安全过程域中的关键的风险点提出安全管理要求，实现制度流程文档化，在流程执行过程域中，使用文档化的计划、标准指导实践。

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。

5.2.3.4 GP 2.2.3 技术工具

采用技术工具执行可行度较高的自动化安全控制，技术工具的执行置于版本控制和配置管理下。

5.2.3.5 GP 2.2.4 人员能力

从事数据安全管理人员应具备对该数据安全风险管理知识，以及规范化执行数据安全过程的能力。

5.2.4 公共特征 2.3 —验证执行

5.2.4.1 公共特征描述

该公共特征的通用实践注重于验证和审计过程是否按预定计划执行,涉及执行过程与计划的一致性验证、数据安全过程的审计、验证和审计活动的计划。

5.2.4.2 GP 2.3.1 组织建设

应对组织机构的岗位设置与相关标准、需求及目标的一致性进行验证和审计。

5.2.4.3 GP 2.3.2 制度流程,

应对制度流程与相关标准、需求及目标的一致性进行验证和审计。

5.2.4.4 GP 2.3.3 技术工具

应对支撑数据安全过程的技术工具与相关标准、需求及测量目标的一致性进行验证和审计。

5.2.4.5 GP 2.3.4 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，并制定能力验证计划。

5.2.5 公共特征 2.4 —跟踪执行

5.2.5.1 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，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。

数据安全管理过程可能由于目标制定不精确、实践受外部因素影响、基础需求发生变化而与原有计划发生偏离，因此，当有重大差别时适当地采取修正措施，包括：计划、组织架构、制度流程、技术工具及人员能力等的变更和调整。

5.2.5.2 GP 2.4.1 组织建设

对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。

5.2.5.3 GP 2.4.2 制度流程

对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。

5.2.5.4 GP 2.4.3 技术工具

对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。

5.2.5.5 GP 2.4.4 人员能力

对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。

5.3 能力级别 3 —充分定义

5.3.1 能力等级描述

在这一级别上，组织机构根据已批准的过程、标准的剪裁版本和文档化过程执行基本实践，称为充分定义的过程。与等级2“计划跟踪”的主要区别在于，使用组织级的标准过程来策划和管理数据安全。

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。

5.3.2 公共特征 3.1—定义标准过程

5.3.2.1 公共特征描述

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。一个组织机构的标准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。组织机构的标准过程可能需要经过剪裁，来适用于特定用途，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。

5.3.2.2 GP 3.1.1 组织建设

组织机构设立了实体或虚拟的岗位和人员，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。

该岗位的人员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。

已明确了数据安全的岗位和人员，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。

5.3.2.3 GP 3.1.2 制度流程

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。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等。

同时，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，保证对与该数据安全过程域相关的人员在对制度流程的理解上的一致性。

5.3.2.4 GP 3.1.3 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。

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。

5.3.2.5 GP 3.1.4 人员能力

从事数据安全人员具备数据安全标准化和工程实践经验，充分理解组织机构在该数据安全过程域中面临的安全风险，并具备风险控制和改进方案的能力。

5.3.3 公共特征 3.2 —执行已定义过程

5.3.3.1 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安全实践的核查，对缺陷过程进行规避。该通用实践构成了协调安全实践的重要基础。

5.3.3.2 GP 3.2.1 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岗位和人员。

该岗位的人员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。

5.3.3.3 GP 3.2.2 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。使用充分定义的制度流程，并针对制度流程进行专门的缺陷复查和规避。

5.3.3.4 GP 3.2.3 技术工具

针对该数据安全过程域中的安全管理要求，建立相应的在线化平台固化并记录相关的流程，建设并部署相应的技术产品，强化相应的安全控制。使用成熟的技术工具，并对技术工具进行缺陷核查和规避。

5.3.3.5 GP 3.2.4 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。能够对人员能力进行考核和复查，并对人员能力的不足开展培训。

5.3.4 公共特征 3.3—协调实践

5.3.4.1 公共特征描述

在大型组织机构或项目中缺乏数据安全管理协调机制将会造成延误或引发安全风险，此公共特征侧重于对不同业务系统和组织活动间的数据安全管理协调机制，包括业务系统内、组织机构的各业务系统之间、组织机构外部活动的协调机制。

5.3.4.2 GP 3.3.1 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。

5.3.4.3 GP 3.3.2 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。

5.3.4.4 GP 3.3.3 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。

5.3.4.5 GP 3.3.4 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

5.4.1 能力等级描述

在这一级别上，组织机构通过对基本实践执行情况的收集、分析和测量，获得过程执行能力和预测能力的量化表示。这个级别的数据安全管理和质量控制过程是客观，与等级3“充分定义”的主要区别在于执行过程的量化表示和控制。

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。

5.4.2 公共特征 4.1 —建立可测的安全目标

5.4.2.1 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，为客观地执行管理提供了必要的基础。

5.4.2.2 GP 4.1.1 组织建设

将安全目标分解落实到数据安全数据安全相关的岗位的职责中，以利于安全目标的量化可测量、可执行。

5.4.2.3 GP 4.1.2 制度流程

量化地确定已定义的制度流程，测量活动要被嵌入到过程定义中。

5.4.2.4 GP 4.1.3 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控制。

5.4.2.5 GP 4.1.4 人员能力

对数据安全人员能力建立量化的衡量指标，定期进行考核、培训等。

5.4.3 公共特征 4.2 —客观地管理执行

5.4.3.1 公共特征描述

该公共特征的提出对数据安全管理能力的测量方法，使用量化的方式来客观的管理和评价数据安全过程域。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。

5.4.3.2 GP 4.2.1 组织建设

组织机构应明确定量的工作管理要求，在工作岗位中设置负责数据收集、存储和分析的角色和人员，并提供相应的资源。

5.4.3.3 GP 4.2.2 制度流程

在制度流程中制定收集和测量数据的方法，对各项工作的执行情况及其效果进行客观的度量。当制度流程未按定义执行时，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，从而反馈到相关制度流程的内容修订上。

5.4.3.4 GP 4.2.3 技术工具

技术工具支持在数据的采集、传输、存储、处理、交换和销毁过程中自动化采集数据和测量，并对度量结果进行展示。当技术工具未按定义执行时，识别出现偏差的原因，从安全要求、工具执行的有效性方面进行持续的跟踪和效果度量，从而反馈到相关技术工具的完善和更新上。

5.4.3.5 GP 4.2.4 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，具备能采用相关方法和工具开展安全度量工作的能力。

5.5 能力级别 5 —持续优化

5.5.1 能力等级描述

在这个级别上，组织机构的数据安全管理过程域是可持续优化的，在业务目标的基础上制定量化的有效性和效率指标，通过执行已定义过程、组织定期评估、运用新思想与技术等进行持续性的改进，以

更好适应业务发展，数据安全最佳实践可为行业供借鉴和参考。这一级与等级4“量化控制”的主要区别在于对已定义和标准过程变化效果进行量化表示，并进行连续调整和改进。

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。

5.5.2 公共特征 5.1 —改进组织能力

5.5.2.1 公共特征描述

该公共特征关注标准过程在整个组织机构范围内的使用情况，分析和标识产生的缺陷的原因，寻求对组织架构的变更和能力提升，以更好地适应业务目标和规划。

5.5.2.2 GP 5.1.1 组织建设

能够分析组织架构的设置上的不足，与国内外领先的数据安全管理理念的差距，提出对组织架构的可能改进目标。

5.5.2.3 GP 5.1.2 制度流程

持续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，从而提高过程有效性。

5.5.2.4 GP 5.1.3 技术工具

能够分析技术工具执行效果上的不足，建立改进目标，标识出对技术工具的改进点，分析对技术工具的可能变更。

5.5.2.5 GP 5.1.4 人员能力

能够分析人员能力上的不足，标识出对人员能力的改进点，建立改进目标，开展人员培训等。

5.5.3 公共特征 5.2 —改进过程有效性

5.5.3.1 公共特征描述

该公共特征注重于对标准过程的持续监控和有效性评价，提出消除产生缺陷的因素，和提出持续改进的标准过程。

5.5.3.2 GP 5.2.1 组织建设

能够消除组织架构设置上的不足，并持续改进组织架构的设置，具备及时调整的以促进业务发展的能力。

5.5.3.3 GP 5.2.2 制度流程

对制度流程进行持续监控，并对制度流程的执行效果进行有效性评价，分析并消除制度流程上的缺陷，并提出持续改进的制度流程。

5.5.3.4 GP 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。

5.5.3.5 GP 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。

6 数据生命周期通用安全的基本实践

6.1 策略与规程

6.1.1 PA01 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与规程，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：
- BP.01.01:设立数据安全的岗位和人员，负责组织机构的数据安全策略与规程的制定、修订和实施。（《要求》5.1.1 a）b)）

b) 制度流程：
- BP.01.02:建立数据安全的策略与规程，明确管理的目的、范围、岗位、责任、管理层承诺、内外部协调及合规性方面的要求。（《要求》5.1.1 a）b））
- BP.01.03:建立数据安全策略与规程的分发流程，确保其能被组织机构各部门、岗位和人员获取。（《要求》5.1.1 c））
- BP.01.04:建立策略与规程的评审、发布和更新流程，确保其连续性和有效性。（《要求》5.1.1 e））

c) 技术工具：
- BP.01.05: 通过信息平台面向组织机构全体员工发布相关材料，以便于获取和执行。（《要求》5.1.1 c） d））

d) 人员能力：
- BP.01.06: 应掌握信息安全管理体系相关的知识。（《要求》5.1.1 a））
- BP.01.07: 应能够及时评估策略与规程的实施效果，制定改进计划，并进行修订。（《要求》5.1.2 a）b））

6.2 组织和人员管理

6.2.1 PA04 组织管理

6.2.1.1 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，明确数据安全责任，防范人员管理过程中存在的安全风险。

6.2.1.2 数据安全能力基本实践

a) 组织建设：
- BP.04.01：基于组织机构的数据安全方针及策略，建立数据安全职能部门和岗位，相关职能包括于：数据安全规范及标准编制、数据安全技术及产品开发、数据安全监控及审计、数据安全宣传与促进、数据安全合作与交流等。（《要求》5.3.1.1 a）、c））
- BP.04.02：建立组织机构层面的数据安全领导小组，最高管理者或授权代表人担任组长，

并明确组长责任与权力，小组应配备必要的管理人员和技术人员。（《要求》5.3.1.1 b）、《要求》5.3.1.2 a））

- BP.04.03：设置专职的数据安全岗位，建立规范化的数据安全保护、评估及考核队伍。（《要求》5.3.1.2 b））
- BP.04.04：职能岗位设计时考虑职责分离的原则，建立内部监督管理职能部门，对数据安全管理活动进行监督。（《要求》5.3.1.1 d））

b) 制度流程：

- BP.04.06：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，明确各职能岗位的运行配合机制。（《要求》5.3.1.1 a））
- BP.04.07：制定数据安全追责制度，定期对责任部门和安全岗位开展安全检查，形成检查报告。（《要求》5.3.1.1 e））

c) 技术工具：

- BP.04.08：通过信息化平台面向全员发布数据安全职能部门组织架构和相关联络人。（《要求》5.3.1.1 a，5.3.1.2 a））

d) 人员能力：

- BP.04.09：数据安全职能和岗位规划人员应能够明确组织机构的数据安全工作目标，充分了解数据安全职能现状，有效的调整职能设置。（《要求》5.3.1.2 a）、b））

6.2.2 PA05 人员管理

6.2.2.1 数据安全过程域描述

通过规范人力资源管理过程中的数据安全要求，降低人员管理过程中的安全风险。

6.2.2.2 数据安全能力基本实践

a) 组织建设：

- BP.05.01：设立人力资源管理过程中的数据安全管理岗位和职责，负责对人员相关的数据安全分析、方案制定和实施。（《要求》5.3.2.1 a）、b）、c）、d）、e）、f）、g））

b) 制度流程：

- BP.05.02：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工作范畴和安全管理措施。（《要求》5.3.2.1 b）、c）、d）、e）、f)、g））
- BP.05.03：制定数据服务相关人员招聘、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，应包括：
  1) 数据服务岗位人员或候选人的背景调查要求；
  2) 数据服务岗位人员安全责任和保密协议要求；
  3) 数据服务重要岗位的兼职和轮岗、权限分离、多人共管等安全要求；
  4) 数据安全责任和奖惩管理机制；
  5) 人员调离或终止劳动合同时的要求；
  6) 第三方人员的数据安全管理制度。

c) 技术工具：

- BP.05.04：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：

- BP.05.05：人力资源数据安全管理人员应充分理解人力资源管理过程中的安全控制措施，并通过培训、考试等手段提其数据安全意识。（《要求》5.3.2.1 a）、b）、c）、d）、

e）、f)、g））

- BP.05.06：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））

6.2.3 PA06 角色管理

6.2.3.1 数据安全过程域描述

通过对数据安全管理过程中各角色的安全控制，降低角色和权限管理相关的安全风险。

6.2.3.2 数据安全能力基本实践

a) 组织建设：

- BP.06.01：设立人力资源管理过程中的数据安全管理岗位和职责,负责对角色和权限相关的数据安全分析、管理和审查。（《要求》5.3.3.1 a）、b)、c)）

b) 制度流程：

- BP.06.02：依照数据业务需求和数据系统架构建立分层的角色体系、职责分离的数据业务安全角色管理机制。（《要求》5.3.3.2 a））
- BP.06.03：明确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））
- BP.06.04：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））

c) 技术工具：

- BP.06.05：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，实现自动化的安全控制。（《要求》5.3.3.1 a）、b)、c)）

d) 人员能力：

- BP.06.07：角色管理的人员应充分理解角色管理流程中的安全控制措施,通过培训、考试等手段提升其数据安全意识水平。（《要求》5.3.3.1 a）、b)、c)）

6.2.4 PA07 人员培训

6.2.4.1 数据安全过程域描述

通过面向员工开展数据安全培训,提升组织机构内部员工和第三方员工的数据安全意识和数据安全能力水平。

6.2.4.2 数据安全能力基本实践

a) 组织建设：

- BP.07.01：设立数据安全培训管理的岗位和人员，负责对数据安全培训需求分析，及培训方案的制订和培训实施。（《要求》5.3.4.1 a）、 b）、c））

b) 制度流程：

- BP.07.02：制定数据安全岗位人员的安全培训计划,以及关键岗位转岗、升级的数据安全培训计划，并定期审核和更新。（《要求》5.3.4.1 a）《要求》5.3.4.1 b））
- BP.07.03：根据不同岗位的安全要求,开展数据安全培训，包括政策、法律、法规、标准等要求，并对结果进行评价、记录和归档。（《要求》5.3.4.1 c）、《要求》5.3.4.2 a））

c) 技术工具：

- BP.07.04：建立数据安全培训平台，并对人员培训的效果进行评价、记录和归档。（《要求》5.3.4.1 a）、 b）、c）、5.3.4.2 a））

d) 人员能力：

- BP.07.08：固化针对员工、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））

6.3 数据与系统资产

6.3.1 PA02 数据资产

6.3.1.1 数据安全过程域描述

通过建立组织机构数据资产管理手段，实现资产类型、管理模式方面的统一管理要求。

6.3.1.2 数据安全能力基本实践

a) 组织建设：
- BP.02.01: 设立数据安全的岗位和人员，负责数据资产安全管理规范的制定和实施。(《要求》5.2.1.1 a）、b)、c)、d)、e))

b) 制度流程：
- BP.02.02: 制定数据资产的安全管理规范，明确数据资产安全管理目标和原则、资产登记制度、角色及职责等要求，并定期审核和更新。（《要求》5.2.1.1 a）c））
- BP.02.03: 制定数据资产的分类管理要求，包括：分类分级规定、操作指南、变更审批机制。根据分类管理要求，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》5.2.1.1 b）、《要求》5.2.1.2 a） ）
- BP.02.04: 建立数据资产清单，明确数据资产管理范围和属性。基于业务场景，建立内外部数据资源整合规范（《要求》5.2.1.1 d）、《要求》5.2.1.2 b） ）。

c) 技术工具：
- BP.02.05:建立组织机构统一的数据资产管理平台，标识数据管理者、分类分级、数据量等信息，以及对数据资产的分布和使用情况等进行统计。（《要求》5.2.1.2 c） ）

d) 人员能力：
- BP.02.06: 应理解组织机构内部数据资产所涉及业务范围和相应的安全管理需求，能够建立数据资产管理制度。（《要求》5.2.1.1 a））

6.3.2 PA03 系统资产

6.3.2.1 数据安全过程域描述

通过建立组织机构信息系统资产管理手段，实现资产类型、管理模式方面的统一管理要求。

6.3.2.2 数据安全能力基本实践

a) 组织建设：
- BP.03.01: 设置专门的岗位和人员，负责信息系统资产安全管理规范的制定和实施。(《要求》5.2.2.1 a））

b) 制度流程：
- BP.03.02：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原则、生命周期管理、资产登记和分类标记等要求，并定期审核和更新。(《要求》5.2.2.1 a)、e））
- BP.03.03：制定信息系统资产建设和运营管理制度，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））
- BP.03.04：建立组织机构内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。（《要求》5.2.2.1 c））

- BP.03.05：制定信息系统资产更新、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：

- BP.03.06：通过技术工具执行资产登记和分类标记，实现自动化的属性标识。（《要求》5.2.2.1 d））
- BP.03.07：组织机构建立统一的信息系统资产管理平台，具备系统资产统一注册、管理和使用监控、资产现状统计等功能。（《要求》5.2.2.2 a））

d) 人员能力：

- BP.03.09：应理解组织机构内部信息系统资产所涉及业务范围和相应的安全管理需求，能够建立信息系统资产管理制度。（《要求》5.2.2.1 a）、b））

6.4 业务规划与管理

6.4.1 PA08 战略规划

6.4.1.1 数据安全过程域描述

通过建立组织层面数据安全战略规划体系，保证数据安全战略规划与组织机构的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：

- BP.08.01：设立专门的数据安全战略规划岗位和人员，负责制定组织机构整体的数据安全战略规划，并推进规划执行。（《要求》5.4.1.1 a）、b）、 c））
- BP.08.02：设立数据安全战略规划评估小组，负责机构安全规划评估，确保数据安全策略、安全目标和战略规划内容的合规性。（《要求》5.4.1.1 a）、b）、 c））

b) 制度流程：

- BP.08.02：建立组织机构数据安全战略规划目标，制定各阶段目标、任务和工作重点，以及调整、监督与控制措施等。（《要求》5.4.1.1 b））
- BP.08.03：建立数据安全管理总则，包括数据治理、数据质量、元数据等管理要求，以及数据所有权、数据开放与共享等安全策略。（《要求》5.4.1.2 b））

c) 技术工具：

- BP.08.04：通过信息化平台面向全员发布数据安全战略规划，及执行和调整情况。（《要求》5.4.1.1 a）、b)、c)）《要求》5.4.1.2 a）

d) 人员能力：

- BP.08.05：负责人员均具有战略规划经验，对组织机构的数据安全管理需求有充分的理解。（《要求》5.4.1.1 a）、b)、c））
- BP.08.06：通过培训和宣传等手段实现全体人员对数据安全战略规划的一致性理解。(《要求》5.4.1.1 a）、b)、c））

6.4.2 PA09 需求分析

6.4.2.1 数据安全过程域描述

建立面向组织机构业务的数据安全需求分析体系，开展数据安全需求分析活动。

6.4.2.2 数据安全能力基本实践

a) 组织建设：

- BP.09.01：数据业务团队应设立安全需求分析的岗位和人员，在数据业务规划阶段开展安全需求分析工作。（《要求》5.4.2.1 a）、b）、c）、d）、e））

b) 制度流程：

- BP.09.02：建立数据业务的安全需求分析的指南，包括：
  1）依据的国家法律、法规、标准及相关政策要求，分析等合规性需求；
  2）识别数据业务面临的威胁和自身脆弱性，分析数据业务的安全风险和应对措施需求；
  3）依据组织机构的业务战略规划，明确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））
- BP.09.03：利用数据驱动分析方法或安全需求工程等方法开展数据安全需求分析，确保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：

- BP.09.04：建立承载数据业务的安全需求分析的平台，该平台记录所有的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：

- BP.09.05：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 PA10 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：

- BP.10.01：设立固定的岗位和人员，负责组织机构的统一元数据管理工作。（《要求》5.4.3.1 a）、b）、c）、d））

b) 制度流程：

- BP.10.02：建立元数据管理规范，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等。（《要求》5.4.3.1 a））
- BP.10.03：建立元数据安全管理和访问控制策略，明确元数据管理角色及其授权控制机制。建立元数据操作审计机制，确保操作可追溯。（《要求》5.4.3.1 b））（《要求》5.4.3.1 c））（《要求》5.4.3.1 d））
- BP.10.04：依据资产分类分级策略，建立元数据安全属性分级机制，以及安全属性的标记策略和标记定义。（《要求》5.4.3.2 b））（《要求》5.4.3.2 c））

c) 技术工具：

- BP.10.05：建立组织机构统一的元数据管理平台，实现对数据的存储、访问、所属业务情况，以及字段级、表级、应用级的数据上下游关系等信息的可视化展现和统一管理。（《要求》5.4.3.2 a））
- BP.10.06：根据元数据安全管理规范和访问控制策略，实现元数据管理角色及其授权控制的技术手段；根据审计制度要求，采集元数据操作日志，实现元数据操作的追溯技术。（《要求》5.4.3.1 a），5.4.3.1 b）c）d））

d) 人员能力：

- BP.10.10：负责人员应了解元数据管理的基础理论，充分理解组织机构元数据管理业务需求。（《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 PA11 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：

- BP.11.01：设立数据供应链安全管理岗位和人员，负责数据供应链管理要求和解决方案的制定。（《要求》5.5.1.1 a）、b）、c）、d）、e）、f））

b) 制度流程：

- BP.11.02：建立数据供应链安全管理规范，定义数据供应链管理要求和适用范围，明确供应链相关方的责任、义务和保密要求，确保数据交换、使用和利用符合法律法规。（《要求》5.5.1.1 a）、b）、c）、d））
- BP.11.03：针对数据供应链上下游的数据服务者和数据使用者，建立安全能力评估、合规审核、风险监测等的规范或流程。（《要求》5.5.1.1 f））、（《要求》5.5.1.2 a））
- BP.11.04：针对组织机构的外包服务商和人员，建立数据安全能力审核和准入机制，开展安全监控和合格评审。外包服务商应达到相应的数据安全能力成熟度等级（如适用）。（《要求》5.5.1.2 a））

c) 技术工具：

- BP.11.06：组织机构应建立统一的数据供应链目录和数据链路清单。（《要求》5.5.1.1 e））
- BP.11.07：基于对数据供应链的相关记录，利用技术工具对数据供应链上下游的相关方的开展合规性审核和分析。（《要求》5.5.1.1 e）、f））

d) 人员能力:

- BP.11.08：负责人员应了解组织机构上下游数据供应链的整体情况，并熟悉供应链安全方面的法规和标准。（《要求》5.5.1.1 a）、b）、c）、d）、e）、f）、5.5.1.2 a））

6.5.2 PA12 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：

- BP.12.01：设立数据服务接口安全管理岗位和人员，负责制定安全规则和方案，开展安全管理。（《要求》5.5.2.1 a）、b）、c）、d））

b) 制度流程：

- BP.12.02：制定数据服务接口规范（包括接口名称、接口参数、接口安全要求等）和安全控制策略。（《要求》 5.5.2.1 a））（《要求》 5.5.2.1 b））

c) 技术工具：

- BP.12.04：提供数据服务接口安全控制措施，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，建立异常告警机制。（《要求》5.5.2.1 a）、b））
- BP.12.05：统一收集数据服务接口的日志记录，并提供服务接口服务审计功能。（《要求》5.5.2.1 c））
- BP.12.06：对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））
- BP.12.07：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））

d) 人员能力:
- BP.12.08：负责人员应理解数据服务接口的业务场景，具备安全风险评估能力。（《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 PA13 个人信息保护

6.6.1.1 数据安全过程域描述

组织机构应根据其业务所适用的法律法规和标准要求,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。

6.6.1.2 数据安全能力基本实践

a) 组织建设：
- BP.13.01：设立统一负责个人信息保护的岗位和人员，为组织机构提供统一的个人信息保护的规范要求和安全解决方案，并组织实施。（《要求》5.6.1.1 a）、b）、c）、d）、5.6.1.2 a））

b) 制度流程：
- BP.13.02：依据《GB/T GB/T 35273-2017 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））
- BP.13.03：针对组织机构职能、业务、服务和设备等的调整变化，建立相应的个人信息保护机制，确保个人信息的妥善转移、转存或销毁。（《要求》5.6.1.2 a））
- BP.13.04：针对个人信息保护的技术手段，建立有效性评价和风险评估机制。（《要求》5.6.1.2 d））

c) 技术工具：
- BP.13.05：建立组织机构个人信息保护安全技术方案，实现对个人信息处理过程中的匿名化、去标识化、差分隐私保护等，并提供在线保护和控制措施。(《要求》5.6.1.2 b)、c））

d) 人员能力：
- BP.13.06：相关人员应了解个人信息保护的标准和法规，具备基于标准要求制定解决方案的能力。
- BP.13.07：应在组织机构内部开展个人信息保护培训工作，以保证全体人员体对合规要求理解的一致性。（《要求》5.6.1.1 a）、5.6.1.2 a）、b）、c）、d））

6.6.2 PA14 重要数据保护

6.6.2.1 数据安全过程域描述

组织机构应根据其业务所适用法律法规和标准的要求，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。

6.6.2.2 数据安全能力基本实践

a) 组织建设：
   - BP.14.01：设立统一负责重要数据保护的岗位和人员，为组织机构提供统一的重要数据保护的规范要求和安全解决方案，并组织实施。（《要求》5.6.2.1 a）、b）、c）、d）、e），5.6.2.2 a）、b）、c））

b) 制度流程：
   - BP.14.02：依据网络安全法等法律法规及相关标准中对重要数据的保护要求，建立组织机构统一的重要数据全生命周期保护的制度规范。（《要求》5.6.2.1 a）、b））
   - BP.14.03：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。（《要求》5.6.2.1 c））
   - BP.14.04：定期对重要数据保护的制度规范执行情况执行进行跟进，以及时更新相关规程保证其可落地性。（《要求》5.6.2.1 e））
   - BP.14.05：建立对重要数据相关风险的管理要求，定期审核重要数据相关的操作记录，监控通过沉淀数据获取重要数据的风险。（《要求》5.6.2.2 b）、c））

c) 技术工具：
   - BP.14.06：建立重要数据的全生命周期操作日志，并进行安全分析，获取组织机构安全合规整体情况。（《要求》5.6.2.1 d））
   - BP.14.07：具备对重要数据的脱敏机制，支持如匿名、泛化、随机和加密等脱敏技术手段，并建立相应的有效性评价机制。（《要求》5.6.2.2 a））

d) 人员能力：
   - BP.14.08：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 PA15 数据跨境传输

6.6.3.1 数据安全过程域描述

组织机构根据其业务所适用的境外法律法规和标准的要求，在相关业务环节和内部运营流程中开展数据跨境传输安全控制，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：
   - BP.15.01：设立统一负责数据跨境传输的岗位和人员，为组织机构提供统一的数据跨境传输的规范要求和安全解决方案，并组织实施。（《要求》5.6.3.1 a）、b）、c），5.6.3.2 a））

b) 制度流程：
   - BP.15.02：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和控制措施，以及处理和审批流程。（《要求》5.6.3.1 a））
   - BP.15.03：定期或发生重大安全事件后，对数据跨境传输有关制度、流程和技术进行审查和检验。（《要求》 5.6.3.2 a））

c) 技术工具：
   - BP.15.04：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。（《要求》5.6.3.1 a）、b）、c））

d) 人员能力：

- BP.15.07：相关人员应充分理解数据跨境传输的合规性要求，并具备合规性分析和解决方案制定的能力。（《要求》5.6.3.1 a）、b）、c），5.6.3.2 a））

6.6.4 PA16 密码支持

6.6.4.1 数据安全过程域描述

组织机构根据其业务所适用法律法规和标准的要求,在相关业务环节和内部运营流程中应用相应的密码技术。

6.6.4.2 数据安全能力基本实践

a) 组织建设：

- BP.16.01：设立统一负责加密技术的岗位和人员，为组织机构提供统一的加密管理的规范要求和安全解决方案,并组织实施。（《要求》5.6.4.1 a），5.6.4.2 a）、b））

b) 制度流程：

- BP.16.02：按照国家密码管理的相关规定，使用和管理有关密码技术和设施，建立组织机构整体的密码技术管理规范，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））

c) 技术工具：

- BP.16.03：建立统一的密钥管理平台，通过该平台执行对密钥的全生命周期的安全管理。（《要求》5.6.4.1 a））
- BP.16.04：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））
- BP.16.05：宜具备密文数据透明处理的技术能力，在不解密数据的情况下进行检索、计算等。（《要求》5.6.4.2 b））

d) 人员能力：

- BP.16.06：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安全的基本实践

7.1.1 PA17 数据分类分级

7.1.1.1 数据安全过程域描述

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。

7.1.1.2 数据安全能力基本实践

a) 组织建设：

- BP.17.01：设立负责数据安全分类分级工作的管理岗位和人员，负责定义组织机构数据安全分类分级原则并提供技术支持。（《要求》6.1.1.1 a）、b）、c））

b) 制度流程：

- BP.17.02：建立组织机构整体的数据分类分级总则和具体业务场景的分类分级细则，并制定相应的安全管理策略和保障措施。（《要求》6.1.1.1 a）、b））
- BP.17.03：建立数据分类分级的变更审核机制和流程。（《要求》6.1.1.1 c））

c) 技术工具：
- BP.17.04：建立数据的安全分类分级标识工具，能够支持人工/自动标识和安全规则检查。（《要求》6.1.1.1 a）、b）、c））
- BP.17.05：建立数据分类分级的创建、操作和变更的日志和分析机制，确保相关操作的可追溯性，支持异常告警和风险分析。（《要求》6.1.1.2 a））

d) 人员能力：
- BP.17.07：相关人员应理解数据相关的业务场景以及面临风险，具备制定数据分类分级要求和解决方案的能力。（《要求》6.1.1.1 a）、b）、c））

7.2 数据采集安全

7.2.1 PA18 数据收集和获取

7.2.1.1 数据安全过程域描述

对数据的收集和获取过程建立安全控制措施，保证对各类数据采集活动的合规性和安全性。

7.2.1.2 数据安全能力基本实践

a) 组织建设：
- BP.18.01：设立负责数据采集安全的岗位和人员，负责制定相关的数据收集和获取的安全要求，并组织实施。（《要求》 6.1.2.1 a）、b）、c）、d）、e）、f））
- BP.18.02：设立相应的数据采集风险评估小组，负责数据收集和获取过程的风险评估与改进。（《要求》 6.1.2.1 a）、b）、c）、d）、e）、f））

b) 制度流程：
- BP.18.03：组织机构应基于法律法规要求制定数据采集规范,应包括:
  1）数据采集的原则、目的和用途；
  2）数据源的真实性和有效性要求；
  3）数据采集范围和数据量的最小够用原则要求；
  4）数据采集的渠道、数据的格式以及相关的流程和方式规范要求。

  （《要求》 6.1.2.1 a）、c）、d））
- BP.18.04：组织机构应针对数据采集建立风险评估要求和规范，防止可能引发的数据泄漏风险，评估内容包括：数据采集源、采集范围和频度、采集通道和方式、数据类型、涉及个人信息和重要数据的合规要求等。（《要求》 6.1.2.1 b）、c））

c) 技术工具：
- BP.18.05：数据采集的业务系统中应具备必要的传输加密和访问授权机制。（《要求》6.1.2.1 e））
- BP.18.06：对采集数据进行校验，保证结果的完整性和一致性。建立数据采集日志，实现对数据采集过程的可追溯。（《要求》 6.1.2.2 a）、b）

d) 人员能力：
- BP.18.09：负责人员应理解数据采集的合规需求、安全需求和业务需求，并能提出解决方案。（《要求》 6.1.2.1 a）、b）、c）、d）、e）、f））
-

7.2.2 PA19 数据清洗、转换与加载

7.2.2.1 数据安全过程域描述

在数据执行清洗、转换与加载的过程中执行保护措施，确保数据的完整性、一致性和可用性。

7.2.2.2 数据安全能力基本实践

a) 组织建设：

- BP.19.01：组织机构内设立相关岗位和人员，负责业务场景下的数据清洗、转换和加载的安全管理。（《要求》 6.1.3.1 a）、b）、c））

b) 制度流程：

- BP.19.02：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，明确执行的规则和方法、相关人员权限、准确性和一致性要求等。（《要求》 6.1.3.1 a）、b）、c））
- BP.19.03：针对个人信息和重要数据等数据，建立数据清洗、转换与加载过程中分类分级要求，及还原和恢复要求。（《要求》 6.1.3.2 a））

c) 技术工具：

BP.19.04：数据清理、转换和加载工具平台应支持不同数据源、不同安全域之间数据访问控制；能够记录并保存个人敏感信息、重要数据等的处理过程；具备一致性检测的能力，支持清洗与转换前后的映射关系展现。《要求》 6.1.3.2a）、b））、（《要求》 6.1.3.1 a））

d) 人员能力：

- BP.19.05：通过培训确保相关人员对清洗、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），6.1.3.2a）、b））

7.2.3 PA20 质量监控

7.2.3.1 数据安全过程域描述

建立组织机构的统一的数据质量监控和评价体系，保障数据采集处理过程中的质量要求。

7.2.3.2 数据安全能力基本实践

a) 组织建设：

- BP.20.01：组织机构内设立相关岗位和人员，负责制定统一的数据质量管理规范，支持业务部门的数据处理质量评价需求。（《要求》 6.1.4.1 a）、b）、c））

b) 制度流程：

- BP.20.02：制定数据采集质量管理控制策略和规范，包括：数据的格式规范和完整性要求、数据质量评价指标、质量监控范围及监控方式、对异常数据处理的流程和时限要求等。（《要求》 6.1.4.1 c））

c) 技术工具：

- BP.20.03：建立数据质量的指标体系，结合元数据管理平台等实现数据质量的策略发布、等级划分和质量评估，利用技术工具实现在线数据质量监控，并对异常数据及时更正。（《要求》 6.1.4.1 a）、b）、c））

d) 人员能力：

- BP.20.04：负责人员应具有数据质量管理的相关理论基础，能够根据数据质量管理需求开展相关工作。（《要求》 6.1.4.1 a）、b）、c，6.1.4.2 a）、b））

7.3 数据传输安全

7.3.1 PA21 数据传输安全管理

7.3.1.1 数据安全过程域描述

利用加密、签名、鉴别和认证等机制对数据传输进行安全管理，防止数据遭泄漏和篡改。

7.3.1.2 数据安全能力基本实践

a) 组织建设：
- BP.21.01：组织机构内设立相关岗位和人员，负责数据传输安全的解决方案制定和技术方案实施。（《要求》6.2.1 a） ）

b) 制度流程：
- BP.21.02：应区分安全域内、安全域间等的数据传输场景，制定相应的数据传输安全策略和审批流程；
- BP.21.03：针对不同类型、级别的数据的数据传输场景，提出加密传输、签名验签、鉴别和验证的安全管理要求；
- BP.21.04：建立对数据传输安全策略变更进行审核和监控的制度，建立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》6.2.1a）、b）、c）、d）、e）、f），6.2.2 a））

c) 技术工具：
- BP.21.03：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，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））
- BP.21.04：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））
- BP.21.05：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》6.2.1e））
- BP.21.06：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；并综合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》6.2.1f））
- BP.21.07：在关键的业务网络架构汇总考虑数据传输可靠性和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：
- BP.21.08：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》6.2.1a）、b）、c）、d）、e）、f），6.2.2 a））

7.4 数据存储安全

7.4.1 PA22 存储架构

7.4.1.1 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。

7.4.1.2 数据安全能力基本实践

a) 组织建设：
- BP.22.01：组织机构内设立统一负责数据存储安全管理的岗位和人员，负责制定数据存储安全管理规范，并推进相关要求的落地实施。（《要求》6.3.1.1 a)、b)、c)、d)、e)，6.3.1.2a)、b)）

b) 制度流程
- BP.22.02：制定数据存储架构相关安全策略，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））
- BP.22.03：制定数据存储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，确保数据存储架构安全管理规则的实施。（《要求》6.3.1.1 b）、c））
- BP.22.04：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》6.3.1.1d)）

c) 技术工具
- BP.22.05：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，具备对高等级的核心数据进行网络层面的物理隔离的能力。（《要求》6.3.1.1a））
- BP.22.06：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））
- BP.22.07：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》6.3.1.1d））
- BP.22.08：确保存储架构具备数据存储跨地域的容灾能力。（《要求》6.3.1.2e））
- BP.22.09：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》6.3.1.1d)、6.3.1.2 b)）

d) 人员能力
- BP.22.10：负责数据存储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存储面临的安全风险，能够对数据中心安全事件进行及时响应。（《要求》6.3.1.1 b））
- BP.22.11：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））
- BP.22.12：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））
- BP.22.13：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，使其了解数据加密算法所适合的应用场景。（《要求》6.3.1.1 d））

7.4.2 PA23 逻辑存储

7.4.2.1 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数据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。

7.4.2.2 数据安全能力基本实践

a) 组织建设

- BP.23.01：设立统一负责数据逻辑存储系统安全管理的岗位和人员，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；明确各数据逻辑存储系统的安全管理员，负责执行数据逻辑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

- BP.23.02：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））
- BP.23.03：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、不同需求和不同数据用户的存储安全管理。（《要求》6.3.2.1 a））
- BP.23.04：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；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））
- BP.23.05：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））
- BP.23.06：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》6.3.2.2a））

c) 技术工具

- BP.23.07：提供针对主要数据存储系统的配置扫描的工具，定期对数据存储系统的安全配置进行扫描，以保证符合基线的一致性要求。（《要求》6.3.2.1a））
- BP.23.08：提供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对终端系统上的数据进行风险监控。（《要求》6.3.2.1a））
- BP.23.09：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；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》6.3.2.2a））

d) 人员能力：

- BP.23.10：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》6.3.2.1a）、b）、c））

7.4.3 PA24 访问控制

7.4.3.1 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。

7.4.3.2 数据安全能力基本实践

a) 组织建设：

- BP.24.01：建立统一负责数据权限管理的岗位和人员，明确业务部门和安全部门的审批

权限和审批人员。（《要求》6.3.3.1a））

b) 制度流程：

- BP.24.02：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》6.3.3.1a））
- BP.24.03：建立数据访问审计信息的存储保护机制和管控措施。（《要求》6.3.3.1c））

c) 技术工具：

- BP.24.04：建立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》6.3.3.1b））
- BP.24.05：建立面向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））
- BP.24.06：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））
- BP.24.07：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））

d) 人员能力：

- BP.24.08：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））

7.4.4 PA25 数据副本

7.4.4.1 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。

7.4.4.2 数据安全能力基本实践

a) 组织建设：

- BP.25.01：建立统一的数据存储冗余性管理的岗位和人员，并将数据复制、备份和恢复的职责明确划分到相应的岗位和人员。（《要求》6.3.4.1 a）、b）、c）、d））

b) 制度流程：

- BP.25.02：建立数据存储冗余策略和管理制度，以满足数据服务可靠性、可用性等数据安全保护目标。（《要求》6.3.4.1 a））
- BP.25.03：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））
- BP.25.04：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））
- BP.25.05：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））
- BP.25.06：定期对数据备份的场景、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)）

c) 技术工具：

- BP.25.07：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））
- BP.25.08：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以及技术，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））

d) 人员能力：

- BP.25.09：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））
- BP.25.10：执行数据备份和恢复测试的人员均经过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））

7.4.5 PA26 数据归档

7.4.5.1 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。

7.4.5.2 数据安全能力基本实践

a) 组织建设：

- BP.26.01：设立统一的数据归档存储管理的岗位和人员，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)、c)、d)、e)）

b) 制度流程：

- BP.26.02：建立数据归档存储的制度规范，该制度规范中明确定义根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））
- BP.26.03：建立归档数据安全审计与恢复制度，并指定专人负责。并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》6.3.5.2 a））

c) 技术工具：

- BP.26.04：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））
- BP.26.05：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：

- BP.26.06：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））

7.4.6 PA27 数据时效性

7.4.6.1 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。

7.4.6.2 数据安全能力基本实践

a) 组织建设：

- BP.27.01：组织机构设立统一负责数据存储时效性管理的岗位和人员。（《要求》6.3.6.1 a）、b）、c）、d））

b) 制度流程：

- BP.27.02：制定数据存储时效性管理的规范，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））

c) 技术工具：

- BP.27.03：建立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））
- BP.27.04：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数据使用者的有效告知。（《要求》6.3.6.1 b）、c）、d））
- BP.27.05：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，确保数据用户能高效地获得有效数据。（《要求》6.3.6.2 b））
- BP.27.06：通过工具对需要符合数据存储合规要求的数据进行标识。（《要求》6.3.6.1 b））
- BP.27.07：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））
- BP.27.08：通过风险提示和技术手段避免非过期数据的误删除，确保在一定的时间窗口内的误删除数据可以手动恢复。（《要求》6.3.6.1 d））

d) 人员能力：

- BP.27.09：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)

7.5 数据处理安全

7.5.1 PA28 分布式处理安全

7.5.1.1 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。

7.5.1.2 数据安全能力基本实践

a) 组织建设：

- BP.28.01：设立岗位和人员负责组织机构统一分布式处理的安全管理规则的制定，并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：

- BP.28.02：制定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））
- BP.28.03：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：

- BP.28.04：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））

- BP.28.05：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））
- BP.28.06：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））
- BP.28.07：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，确保这些节点数据副本的完整性、一致性和真实性。 （《要求》6.4.1.1 d））
- BP.28.08：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））
- BP.28.09：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：

- BP.28.10：负责该项工作的人员了解分布式处理系统/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））

7.5.2 PA29 数据分析安全

7.5.2.1 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。

7.5.2.2 数据安全能力等级描述

a) 组织建设：

- BP.29.01：设立统一负责数据分析安全的岗位和人员，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) 制度流程：

- BP.29.02：制定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））
- BP.29.03：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，整体保证数据分析的预期不会超过相关分析人员对数据的权限范围。（《要求》6.4.2.1 b））
- BP.29.04：建立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)）

c) 技术工具：

- BP.29.05：提供对数据分析中的个人数据执行去标识化处理的技术工具，即对任何个人识别信息（如姓名、地址、身份证号等）从数据中进行去标识化处理。（《要求》6.4.2.1 c）、d）、e））
- BP.29.06：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））

- BP.29.07：采用多种技术手段结合以降低数据分析过程中安全风险，包括但不限于常用技术手段，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等。（《要求》6.4.2.1 c）、d）、e）、6.4.2.2 a））
- BP.29.08：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））
- BP.29.09：建立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：

- BP.29.10：能够基于合规性要求、业界标准对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））
- BP.29.11：具备对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））

7.5.3 PA30 数据正当使用

7.5.3.1 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。

7.5.3.2 数据安全能力基本实践

a) 组织建设：

- BP.30.01：设立明确的岗位和人员负责对数据的使用管理，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））
- BP.30.02：设立统一的岗位和人员，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：

- BP.30.03：制定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、撤销提出全生命周期的管理要求和责任制。（《要求》6.4.3.1 a）、b））
- BP.30.04：统一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))
- BP.30.05：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：

- BP.30.06：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））

- BP.30.07：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））
- BP.30.08：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））
- BP.30.09：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））
- BP.30.10：集中身份及访问管理平台对权限的授予均设置时间期限，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））
- BP.30.11：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)）

d) 人员能力：

- BP.30.12：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））
- BP.30.13：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））

7.5.4 PA31 密文数据处理

7.5.4.1 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。

7.5.4.2 数据安全能力基本实践

a) 组织建设：

- BP.31.01：明确组织机构的岗位和人员，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：

- BP.31.02：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)）

c) 技术工具：

- BP.31.03：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））
- BP.31.04：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。（《要求》6.4.4.2 a））

d) 人员能力：

- BP.31.05：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））

- BP.31.06：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，使其了解数据加密算法所适合的应用场景。（《要求》6.4.4.1 a））

7.5.5 PA32 数据脱敏处理

7.5.5.1 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。

7.5.5.2 数据安全能力基本实践

a) 组织建设：

- BP.32.01：设立统一的数据安全岗位和人员，明确数据脱敏的原则、方法并提供相关技术能力，并由数据的安全管理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：

- BP.32.02：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））
- BP.32.03：数据权限申请阶段由该数据的安全管理岗位人员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））
- BP.32.04：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)）

c) 技术工具：

- BP.32.05：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））
- BP.32.06：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））
- BP.32.07：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））
- BP.32.08：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））
- BP.32.09：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)）

d) 人员能力：

- BP.32.10：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））
- BP.32.11：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））

- BP.32.12：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））

7.5.6 PA33 数据溯源

7.5.6.1 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。

7.5.6.2 数据安全能力基本实践

a) 组织建设：
- BP.33.01：组织机构设立负责数据源追溯性管理的岗位和人员，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：
- BP.33.02：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））
- BP.33.03：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)）

c) 技术工具：
- BP.33.04：提供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人员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））
- BP.33.05：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））
- BP.33.06：关键的数据管理平台 / 系统中提供管控措施，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：
- BP.33.07：负责该项工作的人员能够理解组织机构内部数据溯源的业务场景，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)）

7.6 数据交换安全

7.6.1 PA34 数据导入导出安全

7.6.1.1 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。

7.6.1.2 数据安全能力基本实践

a) 组织建设：
- BP.34.01：设立统一的数据导入导出过程的安全管理的岗位和人员，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：

- BP.34.02：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））
- BP.34.03：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、相应的安全管理岗位人员，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））
- BP.34.04：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)）

c) 技术工具：

- BP.34.05：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，确保没有超出数据服务提供者的数据授权使用范围。(《要求》6.5.1.1 c））
- BP.34.06：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））
- BP.34.07：针对数据导入导出的日志建立相应的管理和审计方案，并保存出错数据处理记录，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））
- BP.34.08：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））
- BP.34.09：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：

- BP.34.10：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））
- BP.34.11：针对数据导入导出的原则在全组织范围内进行培训和推广，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））

7.6.2 PA35 数据共享安全

7.6.2.1 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。

7.6.2.2 数据安全能力基本实践

a) 组织建设：

- BP.35.01：设立统一的数据共享过程的安全管理的岗位和人员，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：

- BP.35.02：制定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））
- BP.35.03：建立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岗位人员，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））
- BP.35.04：制定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））
- BP.35.05：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））
- BP.35.06：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））
- BP.35.07：在共享数据时，应对数据接收方的组织机构的安全防护能力进行评估，确保数据接收方有能力保证数据安全。

c) 技术工具：

- BP.35.08：建立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））
- BP.35.09：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））
- BP.35.10：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））
- BP.35.11：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））
- BP.35.12：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：

- BP.35.13：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。（《要求》6.5.2.1 a）、d）、e））
- BP.35.14：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））

- BP.35.15：针对数据共享的原则在全组织范围内进行培训和推广，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））

7.6.3 PA36 数据发布安全

7.6.3.1 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。

7.6.3.2 数据安全能力等级描述

a) 组织建设：
- BP.36.01：组织机构设立负责数据发布安全管理的岗位和人员，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））
- BP.36.02：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：
- BP.36.03：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））
- BP.36.04：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））
- BP.36.05：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））
- BP.36.06：细化制定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：
- BP.36.07：建立数据资源公开数据库，通过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））
- BP.36.08：依法通过数据发布平台服务实现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））
- BP.36.09：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））
- BP.36.10：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））
- BP.36.11：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：
- BP.36.12：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））

7.6.4 PA37 数据交换监控

7.6.4.1 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。

7.6.4.2 数据安全能力基本实践

a) 组织建设：
   - BP.37.01：组织机构设立负责数据交换监控审计岗位和人员，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：
   - BP.37.02：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））
   - BP.37.03：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：
   - BP.37.04：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））
   - BP.37.05：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））

d) 人员能力：
   - BP.37.06：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)）

7.7 数据销毁安全

7.7.1 PA38 介质使用管理

7.7.1.1 数据安全过程域描述

针对组织机构内需要对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。

7.7.1.2 数据安全能力基本实践

a) 组织建设：
   - BP.38.01：组织机构设立统一的负责介质使用管理的岗位和人员，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：
   - BP.38.02：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，并制定介质使用的审批和记录流程。（《要求》6.6.1.1 a））
   - BP.38.03：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））
   - BP.38.04：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））
   - BP.38.05：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：

- BP.38.06: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））
- BP.38.07：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））
- BP.38.08：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：

- BP.38.09：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））

7.7.2 PA39 数据销毁处置

7.7.2.1 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。

7.7.2.2 数据安全能力基本实践

a) 组织建设：

- BP.39.01：组织机构设立统一的负责数据安全销毁管理的岗位和人员，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：

- BP.39.02：制定数据的销毁指引，明确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，并制定数据销毁执行时的审批和记录流程。（《要求》6.6.2.1 a）、c）、g））
- BP.39.03：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））
- BP.39.04：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））
- BP.39.05：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））
- BP.39.06：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：

- BP.39.07：提供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））

- BP.39.08：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：

- BP.39.09：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））

7.7.3 PA40 介质销毁处置

7.7.3.1 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。

7.7.3.2 数据安全能力基本实践

a) 组织建设：

- BP.40.01：设立统一的负责数据安全销毁管理的岗位和人员，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。（《要求》6.6.3.1 a））

b) 制度流程：

- BP.40.02：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））
- BP.40.03：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））
- BP.40.04：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：

- BP.40.05：提供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））
- BP.40.06：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））
- BP.40.07：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：

- BP.40.08：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）
成熟度等级的评估方法

A.1 基本实践与通用实践的配套

各个过程域中，四个能力维度（组织建设、制度流程、技术工具和人员能力）的基本实践，只需要根据通用实践中每个成熟度等级的公共特征中的对应的能力维度进行评估，比如，组织制度下的基本实践基于通用实践中公共特征的组织制度的要求进行评估。

通用实践与基本实践的配套关系如表 2 所示：

表 2. 通用实践与基本实践的配套评估关系示例

			过程域	PA01 数据安全策略与规程			
			能力维度	组织建设	制度流程	技术工具	人员能力
能力等级	公共特征	能力维度	基本实践	BP.01.01	BP.01.02, BP.01.03, BP.01.04 BP.01.05	BP.01.06	BP.01.07, BP.01.08
能力等级 2： 计划跟踪	公共特征 2.1 规划执行	GP 2.1.1 组织建设		○			
		GP 2.1.2 制度流程			○		
		GP 2.1.3 技术工具				○	
		GP 2.1.4 人员能力					○
	公共特征 2.2 规范化执行	GP 2.2.1 组织建设		○			
		GP 2.2.2 制度流程			○		
		GP 2.2.3 技术工具				○	
		GP 2.2.4 人员能力					○
	公共特征 2.3 验证执行	GP 2.3.1 组织建设		○			
		GP 2.3.2 制度流程			○		
		GP 2.3.3 技术工具				○	
		GP 2.3.4 人员能力					○
	公共特征 2.4 跟踪执行	GP 2.4.1 组织建设		○			
		GP 2.4.2 制度流程			○		
		GP 2.4.3 技术工具				○	
		GP 2.4.4 人员能力					○

说明：图中圆框框（○）表示，在这个交叉点是需要进行评估的，否则不需要进行评估。

A.2 成熟度等级评级说明

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。过程域的等级取决于该过程域中的基本实践对于目标等级的满足情况。

本标准不对评级方法做任何限定。比如，可以基于“木桶效应”的评级方法，也可以基于权重等其他的评级方法。

附 录 B
（资料性附录）
成熟度等级评估流程和模型使用方法

B.1 成熟度等级评估流程

数据安全能力从组织建设、制度流程、技术工具和人员能力四个维度展开。通过对各项安全过程所需具备安全能力的量化评估，可评估组织在每项安全过程的实现能力属于哪一级别。。

数据安全能力成熟度等级评估可以通过四个阶段来实现：

- 选取安全过程域：针对组织机构的数据相关的业务现状，选取适当的数据安全过程域纳入评估范围。例如，对于有的组织机构而言，不存在数据对外共享的加工处理，则无需选择共享加工环境安全的过程域。
- 过程域安全评估：基于选择的安全过程域范畴，针对各项安全过程域对组织机构的数据安全实践情况进行现状的调研和分析。
- 确定过程域安全级别：针对该过程域的评估分析的内容，结合过程域的等级评估标准，确定该过程域的级别。
- 确定组织机构整体级别：结合所有过程域的级别，确定组织机构整体的数据安全能力成熟度等级。

其中，4个评估维度如下：

- 组织建设：评估是否具有开展工作的专职/兼职岗位、团队或人员，其工作职责是否通过规范要求或其他手段得到确认和保障。
- 制度流程：检查关键数据安全领域的制度规范和流程在组织内的落地执行情况。
- 技术工具：检查组织内的各项安全技术手段、通过产品工具固化安全要求或自动化的安全作业的实施运作情况。
- 人员能力：执行数据安全工作的人员是否经过专业的技能和安全意识教育培训。

数据安全能力成熟度模型的评估所采用的方式与基线风险评估的方式类似，可以采取以下几种手段：

- 人员访谈：通过访谈的方式与被评估方进行交流、讨论等活动，获取相关证据，了解有关信息。
- 文档审核：由被评估方输入与数据安全相关的文档材料（如数据安全的方针政策、制度规范流程、培训教育材料、以及与产品技术相关的设计实施方案、配置说明、运行记录和其他配套表单），评估小组审核相关的文档材料是否已涵盖完整数据生命周期的过程域和控制项。
- 配置检查：根据被评估方提供的技术材料，登录相关的系统工具平台，检查配置是否与材料保持一致，对文档审核内容进行核实。
- 工具测试：利用技术工具对系统工具平台进行测试，验证是否符合数据安全成熟度模型特定级别的技术能力要求。
- 旁站式验证：评估人员在现场通过实地观察人员行为、技术设施和环境状况判断人员的安全意识、业务操作、管理程序等方面的安全情况。

B.2 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”。

组织机构使用数据安全能力成熟度模型的闭环如图 4 所示。

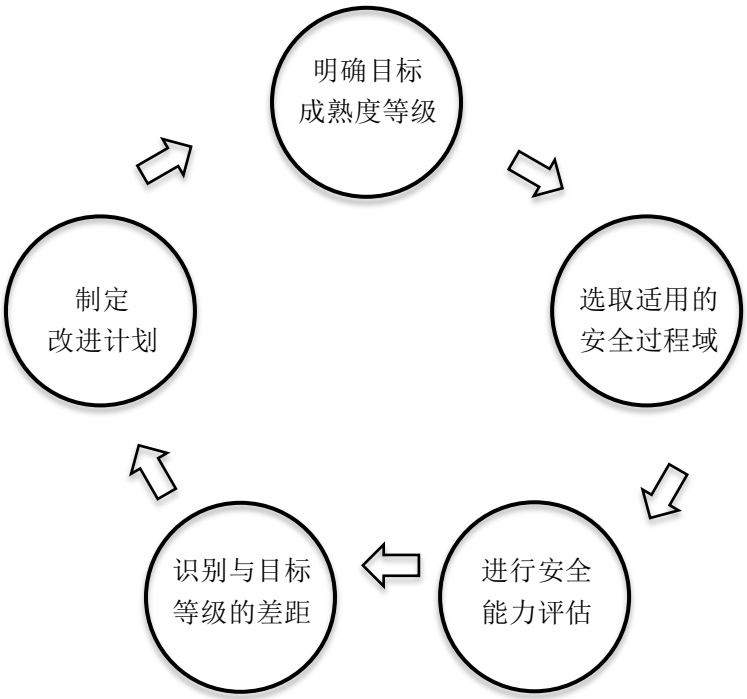

图4　推荐的成熟度模型使用步骤

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 成熟度等级定义”），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 不存在数据跨境传输的情况，因此“数据跨境传输”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。

参考文献

【1】GB/T 20261—2006信息安全技术 系统安全工程-能力成熟度模型
【2】GB/T 30271-2013 信息安全技术 信息安全服务能力评估准则
【3】GB/T AAAAA—AAAA 信息技术大数据术语
【4】GB/T BBBBB—BBBB 信息技术大数据参考框架
【5】GB/T CCCCC—CCCC信息技术 数据管理能力成熟度模型
【6】ISO/IEC 27002 信息技术安全技术信息安全控制规则
【7】ISO/IEC 27004 信息技术安全技术信息安全管理测量
【8】ISO/IEC 21827:2002 信息技术 系统安全工程成熟度模型
【9】ISO/IEC 29190:2013 信息技术安全技术隐私能力评估模型
【10】ISO/IEC 33063:2015 信息技术 过程评估 软件测试的过程评估模型