数据安全能力建设实施指南 V1.0

（征求意见稿）

目　　录

前 言

本指南由阿里巴巴数据安全研究院发起，统筹规划和发布，最终解释归口。某些内容可能涉及专利，本指南的发布机构不承担识别这些专利的责任。

本指南参与起草单位：阿里巴巴（中国）有限公司（下文简称“阿里巴巴”），杭州数梦工场科技有限公司（下文简称“数梦工场”）、杭州安恒信息技术股份有限公司（下文简称“安恒信息”）、浙江蚂蚁小微金融服务集团（下文简称“蚂蚁金服”）、阿里云计算有限公司（下文简称“阿里云”）。

各章节参与单位及人员：

主要章节	起草单位	起草人员
第5章 数据安全能力建设框架	阿里巴巴数据安全研究院	张迅迪、薛勇
第6章 数据安全组织建设	阿里巴巴数据安全研究院	陈彩芳
	数梦工场	何维群
第7章 数据安全人员能力	阿里巴巴数据安全研究院	陈彩芳
	蚂蚁金服	陈树鹏
	安恒信息	周俊
第8章 数据安全制度流程	阿里巴巴数据安全研究院	薛勇
第9章 数据安全技术工具	阿里巴巴数据安全研究院	薛勇
第10章 PA01、PA02、PA03	数梦工场	何维群
第10章 PA14、PA15、PA16、PA17	数梦工场	毛昱
第10章 PA04、PA07、PA08、PA09、PA18、PA19、PA20、PA21、PA25	阿里巴巴数据安全研究院	薛勇
第10章 PA05、PA06	安恒信息	周俊、徐胜兵
第10章 PA10、PA11、PA12、PA13	安恒信息	周俊、徐胜兵
第10章 PA22、PA26、PA27	蚂蚁金服	陈树鹏
第10章 PA23、PA24	阿里云	张敏翀
第2章和第10章所有PA涉及的国家和行业标准，以及全文排版校对	阿里巴巴标准化部	白晓媛

本指南还得到以下单位相关领导和专家们的大力支持，参与了指南的评审并提出宝贵建议：

阿里巴巴（杜跃进、张玉东、朱红儒、张世长、潘亮、贾雪飞），电子四院（胡影、张宇光），数梦工场（孙晖），安恒信息（林明峰），蚂蚁金服（王心刚、王道奎），阿里云（岑欣伟、张大江）。

数据安全能力建设实施指南

1 范围

本指南依据《信息安全技术　数据安全能力成熟度模型》（简称DSMM）制定，以数据为核心，重点围绕数据生命周期，从组织建设、制度流程、技术工具和人员能力等四个方面，提供数据安全能力建设的具体实施指南，为组织数据安全能力建设提供参考。

规划输出系列版本，这次版本以数据安全能力成熟度三级为目标，即如何达到DSMM规定的充分定义级（三级），后续升级版再陆续补充其他级别的指南内容。

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 XXXX—XXXX 信息安全技术　数据安全能力成熟度模型(待发布)

GB/T 35273—2017 信息安全技术　个人信息安全规范

GB/T 35274—2017 信息安全技术　大数据服务安全能力要求

3 术语和定义

GB/T 25069—2010中界定的以及下列术语和定义适用于本文件。

数据安全　data security：保护数据的机密性、完整性和可用性。

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。

成熟度　maturity：对一个组织的有条理的持续改进能力以及实现特定过程的连续性、可持续性、有效性和可信度的度量。

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。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。

数据脱敏data desensitization：通过模糊化等方法对原始数据进行处理以屏蔽敏感信息的一种数据保护方法。

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。

数据处理 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等。

合规compliance：对数据安全所适用的法律法规的遵循。

4 缩略语

下列缩略语适用于本标准：

PA	过程域（Process Area）
BP	基本实践（Base Practice）
DSMM	数据安全能力成熟度模型（Data Security Capability Maturity Model）
IAM	身份识别与访问管理（Identity and Access Management）
BYOD	自带设备办公（Bring Your Own Device）
MDM	移动设备管理（Mobile Device Management）
MAM	移动应用管理(Mobile Application Management)
MCM	移动内容管理（Mobile Content Management）

5 数据安全能力建设框架

5.1 数据安全与现有安全体系融合

数据安全能力建设工作并非从零开始，大部分组织在此前或多或少已有一些安全体系，基本上是围绕信息系统和网络环境开展安全保护工作，主要聚焦在信息安全和网络安全；而数据安全是以数据为核心，围绕数据安全生命周期进行建设以提高数据安全保障能力，所以需要与当前安全体系进行融合。在决策层确定数据安全目标和愿景之后，再由数据安全管理层根据组织的业务发展实际情况讨论具体的融合方式。

5.2 数据安全能力建设框架

基于《信息安全技术　数据安全能力成熟度模型》标准能力成熟度等级3级要求，数据安全能力建设可参考以下实施框架：

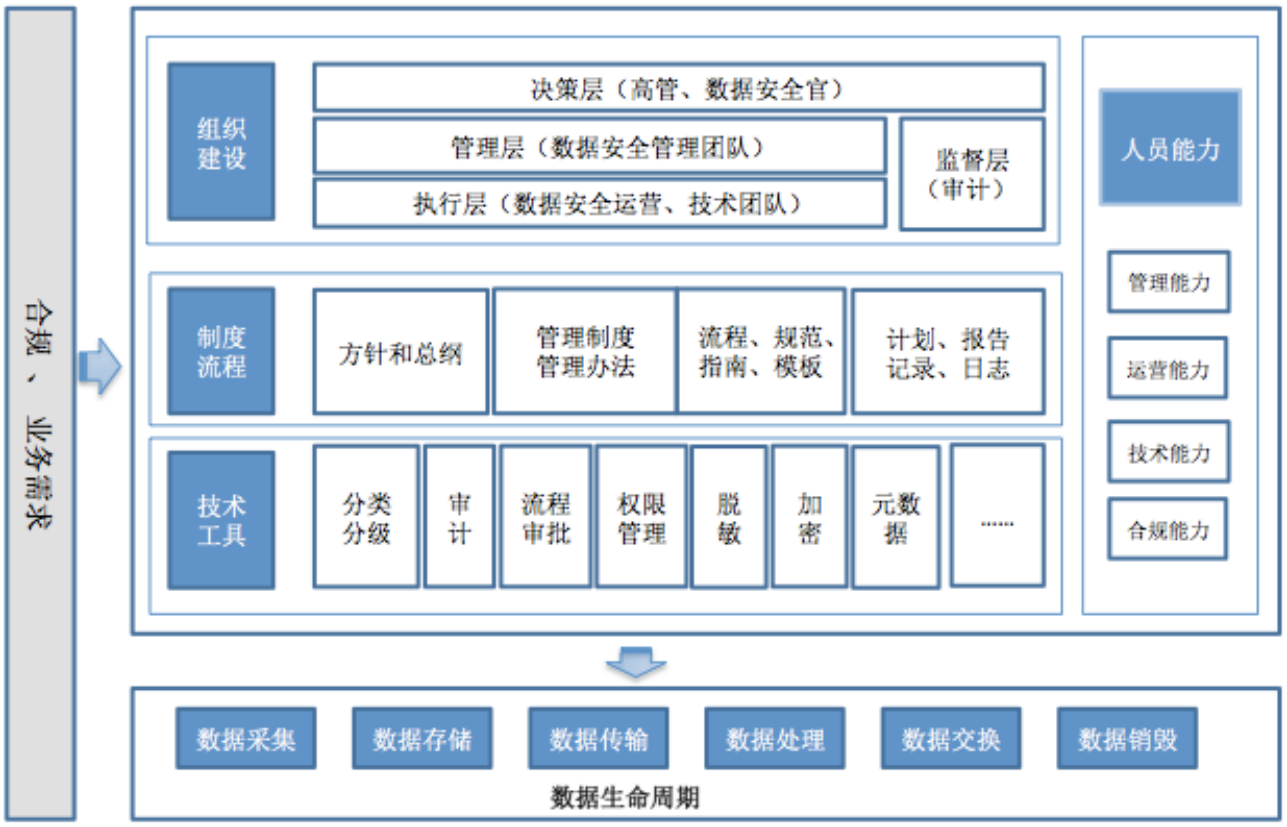

图1：数据安全能力建设框架

5.3 能力建设框架图说明

整体来看，数据安全能力建设是以法律法规监管要求和业务发展需要为输入，结合数据安全在组织建设、制度流程和技术工具的执行要求，匹配相应人员的具体能力，组织的数据安全能力建设结果最终以数据生命周期各个过程域来综合体现。下面对合规和业务需求及四个能力维度的框架设计进行概要说明：

合规和业务需求：数据安全最终是为组织的业务发展服务的，不能游离于业务之外或独立存在。在满足法律法规要求的前提下，数据安全能力建设须切合业务发展需要来开展。

组织建设：指数据安全组织的架构建立、职责分配和沟通协作。组织可分为决策层、管理层和执行层等三层结构。其中，决策层由参与业务发展决策的高管和数据安全官组成，制定数据安全的目标和愿景，在业务发展和数据安全之间做出良好的平衡；管理层是数据安全核心实体部门及业务部门管理层组成，负责制定数据安全策略和规划，及具体管理规范；执行层由数据安全相关运营、技术和各业务部门接口人组成，负责保证数据安全工作推进落地。

制度流程：指数据安全具体管理制度体系的建设和执行，包括数据安全方针和总纲、数据安全管理规范、数据安全操作指南和作业指导，以及相关模板和表单等。

技术工具：指与制度流程相配套并保证有效执行的技术和工具，可以是独立的系统平台、工具、功能或算法技术等。需要综合所有安全域进行整体规划和实现，且要和组织的业务系统和信息系统等进行衔接。包括适用于所有安全域的通用技术工具，和部分阶段或安全域试用的技术工具。

人员能力：指为实现以上组织、制度和技术工具的建设和执行其人员应具备的能力。核心能力包括数据安全管理能力、数据安全运营能力、数据安全技术能力及数据安全合规能力。根据不同数据安全能力建设维度匹配不同人员能力要求。

6 数据安全组织建设

数据安全能力建设是一个复合型、需多方联动型的工作，在开展组织架构建设时，需要考虑组织层面实体的管理团队及执行团队，同时也要考虑虚拟的联动小组，其中业务部门、研发部门、HR、IT、法务等部门均需要参与数据安全建设当中。成立数据安全组织其目的是明确数据安全的政策、落实和监督等工作，以确保数据安全能力建设的有效执行。

6.1 组织架构设计

设计数据安全的组织架构时，可按照决策层、管理层、执行层、员工和合作伙伴、监督层的组织架构设计。在具体执行过程中，组织也可赋予已有安全团队与其它相关部门数据安全的工作职能，或寻求第三方专业团队等形式开展工作，组织架构图如下：

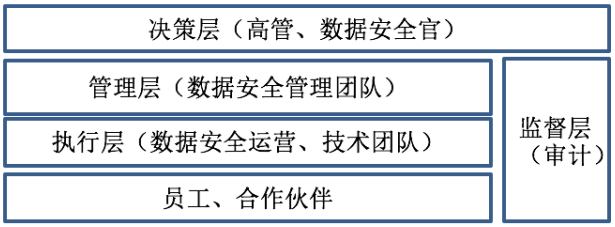

图2：数据安全组织架构图

6.1.1 决策层

决策层是数据安全管理工作的决策机构，建议由数据安全官及其它高层管理人员组成，数据安全官是组织内数据安全的最终负责人。数据安全官应能参与到组织的业务发展决策，因为业务的发展和数据安全是密不可分。除数据安全官外，其它高层管理人员对于数据安全的重视和决策是非常重要的，决策层也需要其它业务、法务、研发等高管共同组成，形成定期的沟通运作机制，其主要工作职责包括：

1) 制定组织的数据安全目标和愿景；
2) 对数据安全策略和规划，制度与规范等进行发布；
3) 为组织的数据安全建设的提供必要的资源；
4) 对公司的重大数据安全事件进行协调和决策；

6.1.2 管理层

管理层是数据安全组织机构的第二层，基于组织决策层给出的策略，对数据安全实际工作制定详细方案，做好业务发展与数据安全之间的平衡。在组织中承上启下，做好数据安全全面落地工作，是组织内开展数据安全工作最核心的部门或岗位，部分工作可能需要组织外部专业资源共同来履行。其主要工作职责包括：

1) 结合合规监管要求和业务发展需求，制订数据安全整体解决方案并组织实施；
2) 制定数据安全管理策略和规划，统一数据安全管理规范体系等；
3) 建立监控审计机制：数据安全工作和监督审计机制，推动并协助执行组织的建立，监督工作有效开展；
4) 对组织内人员能力开展数据安全技术培训和意识宣导，逐步提升数据安全工作人员的能力水平和组织内人员安全意识；
5) 制定数据安全决策层、管理层、执行层、监督层等的运作机制，保障数据安全工作在内部保持信息通畅、运作顺利；
6) 保持外部组织的沟通，包括国家及行业监管、第三方咨询服务商（安全咨询、安全厂商）以认证、测评机构（认证及认可、安全测评机构）等。

6.1.3 执行层

执行层与管理层是紧密配合的关系，其职责主要聚焦每一个数据安全场景，对设定的流程进行逐个实现。执行层主要包括数据安全专职人员和各业务部门的数据安全接口人员、风险管理人员、数据 owner 等，其主要工作职责主要包括：

1) 负责数据安全风险的评估和改进；
2) 负责数据安全运营工作，如：数据权限授权、数据共享、数据下载等审批；
3) 负责数据安全事件的跟进和处理；
4) 协助数据安全管理团队展开数据治理工作，如数据分类分级工作；
5) 负责数据安全专案项目管理和实施。

6.1.4 员工和合作伙伴

范围包括组织内部人员和有合作的第三方的人员，须遵守并执行组织内对数据安全的要求，特别是共享敏感数据的第三方，从协议、办公环境、技术工具方面等做好约束和管理。员工和合作伙伴主要职责是：

1) 履行组织对数据安全的要求，部署数据安全工具；
2) 通过培训、考试、案例学习等提升数据安全意识；
3) 提升数据安全风险识别的能力，能结合业务判断数据安全风险，并降低风险发生；
4) 对组织内风险及时申报，不断协助管理团队提升数据安全防护能力。

6.1.5 监督层

数据安全监督层负责定期监督审核管理小组、执行小组，员工和合作伙伴对数据安全政策和管理要求的执行情况，并且向决策层进行汇报，监督层人员必须具备独立性，不能与其它管理小组、执行小组等人员共同兼任，建议由组织内部的审计部门担任。其主要职责包括：

1) 对数据安全制度落地执行情况监督；
2) 对数据安全工具执行有效性监督；
3) 对数据安全风险开展监控与审计；

6.2 协同部门数据安全职能

数据安全组织和组织内多个部门之间有非常紧密的关系，在组织架构的顶层设计层面，业务部、IT部、法务部、HR、研发部、风控部、公关部等部门需要参与到策略方向及重大事件的决策中；在实际数据安全业务开展层面，从平台底层设计到流程制定实施、安全工具部署、人员安全管控、数据安全合规、对外披露等方面均需要深度介入和协作。

同时，需要数据安全管理层制定与各部门之间的数据安全工作机制，目的是为了保障数据安全工作顺利开展，过程中的争议得到解决，如数据安全安全团队与业务方、法务以及合作伙伴之间的日常工作交流、争议与问题解决等事项。

这些职能部门所涉及的数据安全工作在第十章节会有更详细的描述，这里主要列举了一部分组织部门在数据安全能力建设上可能会涉及的协同工作，具体部门名称在不同组织内可能会有差异，具体以实际情况为主。

6.2.1 业务部门数据安全职能

业务部门在组织内主要职能是拓展业务，保障业务持续发展，但是同时需要兼顾数据安全风险问题。在业务开展过程中，主要会涉及以下几方面的数据安全联动工作，对于较为复杂大型的组织，考虑业务内部有一名数据安全接口人经过培训、赋能等工作（兼职）开展以下相关工作：

1）业务新增：大部分场景主要涉及数据采集合规，需要由数据安全组织及法务合规部门，联合开展新增业务的数据安全风险评估。

2）业务运营：可能涉及数据批量查询、下载、分析和处理，过程中做好岗位权限管理，保障数据最小化使用的原则。

3）业务外部合作：当与外部产生合作，可能涉及数据共享、交换等场景，需要数据安全组织或数据安全接口人开展数据共享、数据披露的风险评估，避免敏感数据外泄等风险；同时接收外部合作的数据时，与合规部门联合做好数据来源合法的控制等措施。

4）数据安全事件：当业务部门内部发生数据安全事件时，业务负责人需要联合数据安全组织及时调查和处理，降低事件影响面及影响程度。并举一反三，改进业务流程机制，降低数据安全风险。

5）其他数据安全执行工作，风险上报等职能。

6.2.2 人力资源部门数据安全职能

人员资源部门主要负责企业内部人员招聘、管理等工作，在人员入职、调岗、离职等过程中，做好人员完整链路的数据安全协同工作，同时需要对数据安全违规人员进行处罚设置及处理。具体数据安全工作职能详见10.x的PA21的详细解读。

6.2.3 IT 部门数据安全职能

IT部门主要实现组织内信息化的工作，过程中涉及到多个数据安全相关的管理工作，一般由数据安全组织制定策略制度，由IT部门开展执行落地。主要数据安全职能包括：

1）服务器、硬盘、PC等介质的安全管理；

2）终端安全的防护措施部署；

3）高风险软件、云盘、通信工具等软件的管理策略执行。

6.2.4 法务部门数据安全职能

法务部门主要负责政策法律、合作协议等相关事项，其中数据安全 / 个人隐私的政策法规逐步出台和完善，结合实际业务组织开展内部的数据安全合规工作至关重要。具体开展时，可利用外部专业机构，作为职能补充。主要会涉及到联动的数据安全工作职能包括：

1）组织内部开展数据安全 / 个人隐私保护合规专项，并联合多部门完成合规。

2）对数据供应链的合作伙伴，在合作协议中拟定数据安全相关管理要求。

3）对组织内部开展数据安全合规政策的解读和培训。

6.2.5 风险管理部门数据安全职能

风险管理部门主要统筹负责组织内所有风险的安全管控，数据安全应是其中的一个模块，一定意义上，可以与数据安全组织架构中的数据安全管理部门开展分工协作。其主要职能包括：

1）设置内部数据安全风险举报机制，收集风险并及时开展处理；

2）设置数据安全风险应急相应机制，联动数据安全组织、业务部门等开展风险评估和及时处理；

3）对数据安全风险定期分析和总结，反馈给数据安全部门，促进数据安全在流程上、机制上、产品上做优化和更新；

6.2.6 公共关系部门数据安全职能

公关部门即公共关系部门，通过良好的公共关系活动的策划来实施和实现组织内外有良好的科学关系，涉及和管理组织内部较多信息对外发声以及外部声音的内部回应，在过程中其主要职能包括：

1） 当对媒体发布信息时，在数据披露流程中，可以考虑结合内容敏感程度，增加公关的审批节点，将数据披露的风险控制到最低。

2）当涉及较大数据安全风险事件时，对外及时的响应应考虑由公关统筹发声，保障回应内容和方式被公众所接受 。

7 数据安全人员能力

数据安全治理不是简单技术形的工种，在现在大数据背景下，是一个复合型的工作，所需要配备的人员也需要具有多方面的能力。数据安全领域较新，在国内这方面培养的人员较少，也是当前逐步需要提升的关键任务。

数据安全的人员能力主要包括几个维度，数据安全管理能力、数据安全运营能力、数据安全技术能力和数据安全合规能力。通用能力在本章节中不再具体描述。

7.1 数据安全管理能力

目前大部分组织尚未正式开展数据安全体系建设，也较少有数据安全的专职职能岗位，对人员能力的培养也在起步阶段。但是随着组织对数据安全的重视度逐步提高，体系建设的诉求也越来越强，所以如何建设完整的数据安全体系，做好数据安全管理是企业面临的第一大问题。

数据安全管理包含以下能力：

M1 熟悉国家网络安全法律法规及组织所属行业的政策和监管要求，了解行业内数据安全建设的最佳实践路线；

M2 具备良好的业务发展战略判断能力，能够通过平衡业务需求和法律风险进行战略思考并提供实用建议；

M3 熟悉组织的业务特性，能根据业务的发展变化，制定或调整组织的数据安全策略；

M4 能够基于组织的数据安全策略，编制相关的制度体系文件，对业务过程进行规范指导；

M5 在隐私保护、数据安全、风险管理、审计合规等相关领域至少 3 年以上的管理经验；

M6 具备组织内跨部门的管理协调能力，能够调动其他部门资源配合落地相关的数据安全控制机制。

M7 具备数据安全管理团队的组建及人才梯队建设的能力；

M8 具备数据安全应急指挥能力，对业务过程中发生的数据安全问题，能够准确判断快速组织相关人员进行应急处置；

M9 了解组织业务及数据特性，在各业务部门有针对性的落实数据安全策略和控制措施；

M10 具备与国家单位、行业监管机构及合作伙伴之间的沟通协调能力，能利用外部资源协助组织数据安全体系的建设；

M11 具备良好的数据安全风险意识。

7.2 数据安全运营能力

数据安全建设是一个长期持续的过程，需要在组织内持续性的落实数据安全的相关制度和流程，并基于组织的业务变化和技术发展不断的调整和优化，安全也是一个不断螺旋上升的过程，因此需要做好数据安全运营工作。数据安全运营包含以下能力：

O1 具备数据安全策略、制度规程及技术工具在组织内部的推广落地能力;

O2 具备利用相关技术工具，对组织业务运营过程中的数据安全风险进行监测、识别、预警和处置的能力;

O3 具备对组织现有数据安全控制措施的有效性进行识别和判断的能力;

O4 具备对员工进行数据安全培训和安全意识教育的能力。

7.3 数据安全技术能力

数据安全的实现，需要技术和工具平台的支撑，来完成安全管控措施的构建，从而实现数据安全能力的建设。数据安全技术目前正在逐步更新和迭代，在大数据环境下，要求组织内从事数据安全领域的技术人员具备以下能力：

T1 熟悉国内外主流的数据安全产品和工具，如数据防泄漏（DLP）、脱敏工具、数据溯源、加密平台等，能准确判断当前组织所需的最佳实践，并深入和落地应用；

T2 在数据安全全生命周期中，能评估潜在数据安全风险，如数据业务风险、数据风控风险、隐私保护风险等，并能制定有效、合理降低数据风险的解决方案或者措施；

T3 在数据安全架构设计时，能够贴合业务和合规场景，覆盖数据在全生命周期中的保护；

T4　能对敏感数据流动做好审计工作，具备风险排查能力，快速处置数据的篡改和泄露等风险；

T5　能对当前数据安全体系进行技术验证，如白盒、灰盒和黑盒等安全测试和对抗，从而让数据安全防御形成一个持续迭代更新的良性循环系统；

T6　需要自研或平台型的组织，应熟悉数据安全技术发展，了解国内外前沿的数据安全和隐私保护技术，如加密技术、差分隐私和 UEBA 等，能在恰当时期引入组织需要的技术，从而降低数据安全和隐私保护的风险。

7.4　数据安全合规能力

在数据安全领域，国内外越来越多的法律法规、标准逐步出台，如《网络安全法》、《个人信息保护法（草案）》、欧盟《一般数据保护条例（GDPR）》等，合规工作成了数据安全领域建设的底线。如何保障合规要求准确识别，并形成内部规章指导合规落地工作，主要具备的能力包括：

C1　熟悉国内外数据安全和隐私保护的法律、政策和行业标准，并精通适用于本组织业务开展所必须遵守的法律、政策和标准内容；

C2　能够依据外部合规要求，建立覆盖组织的数据安全和隐私保护的管理体系和机制，并推动多方参与，落地执行；

C3　能够与组织内采购、供应商管理以及法律等部门合作，确保合作伙伴执行统一的标准，使得合同和操作层面的协议、数据安全和隐私保护管理计划，符合国内外数据安全政策与法规要求；

C4　能够与业务、法务和风险等部门协作，发现的隐私合规问题，并制定纠正措施和计划，定期进行评审。

7.5　人员能力与组织架构的映射

考虑到数据安全组织架构中各个层级能力要求会有侧重和交叉，用下图来表示他们之间映射关系：

表1：人员能力与组织架构映射关系

组织架构	管理能力	运营能力	技术能力	合规能力
策略层	M1、M2、M3、M6、M7、M10	O1	T2、T3	C1、C2、

管理层	M1、M2、M3、M4、M5、M6、M7、M8、M9、M11	O1、O4	T1、T3	C1、C2、C3、C4
执行层（运营）	M1、M6、M8、M9、M11	O1、O2、O3、O4	T1、T2、T3、T4	C1、C4
执行层（技术）	M1、M6、M8、M9、M11	O2、O3	T1、T2、T3、T4、T5、T6	C1、C4
监督层	M1、M2、M3、M4、M5、M6、M7、M8、M9、M11	O3、O4	T1、T4、T5	C1、C4
员工、合作伙伴	M11	/	/	/

8 数据安全制度流程

8.1 制度体系架构设计

制度流程需要从组织层面整体考虑和设计，并形成体系框架。制度体系需要分层，层与层之间，同一层不同模块之间需要有关联逻辑，在内容上不能重复或矛盾。一般按照分为四级：

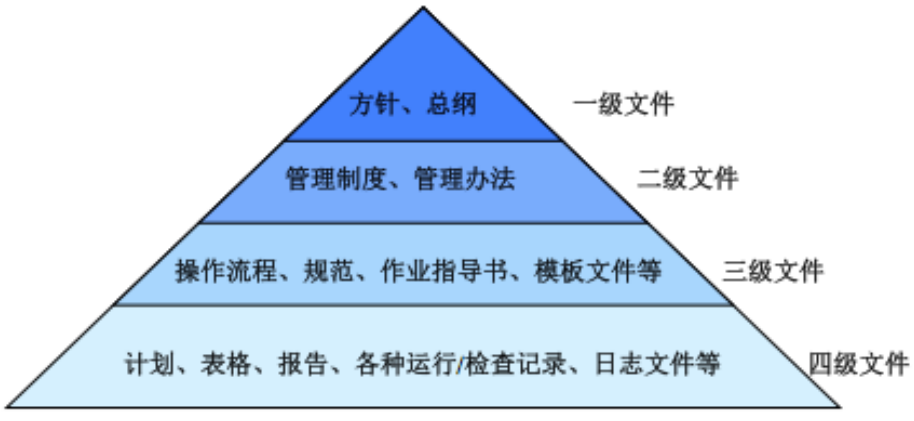

图 3 数据安全制度体系层级

可以形成一份单独的文档，以图或表形式描述数据安全制度体系结构，对每一份制度文件给予编号和层级标识，具体编号和层级定义方式根据实际情况自定义，以便于索引和维护。

常见格式如下：

表 2：数据安全制度体系列表示意

编号	名称	层级	相关文件	版本	最新修订日期
DS-01-001	数据安全总纲	1			
DS-02-001	数据资产管理	2			
DS-02-002	系统资产管理	2			
DS-02-003	数据质量管理	2			
DS-02-004	数据安全人才管理	2			
DS-02-005	……	2			
DS-02-006	……	2			
DS-03-001	数据采集管理规范	3			
DS-03-002	数据传输管理规范	3			
DS-04-001	数据脱敏规范	3			
DS-04-002	日志管理规范	3			
……		……			
	硬盘销毁操作指南	3			
	XXX 作业指导书	3			
	公共硬盘借用记录表	4			
	XXXX 模板	4			
……		……			

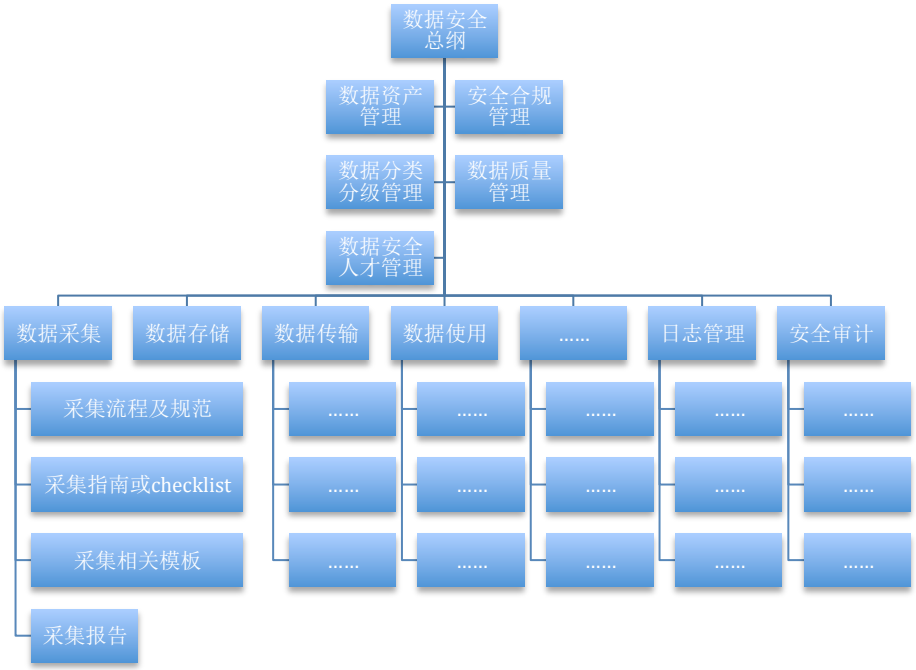

图 4：数据安全制度体系架构

8.2 制度体系架构说明

8.2.1 一级文件

方针和总纲是面向组织层面数据安全管理的顶层方针、策略、基本原则和总的管理要求等，主要内容包括但不限于：

1) 数据安全管理的目标、愿景、方针等；
2) 数据及数据资产定义：比如定义组织内数据包含哪些内容和类别，信息系统载体等；
3) 数据安全管理基本原则：比如数据分类分级原则、数据安全和业务发展匹配原则、数据安全管理方针和政策等；
4) 数据生命周期阶段划分和整体策略，比如：数据产生、数据存储、数据传输、数据交换、数据使用、数据销毁等。
5) 数据安全违规处理：比如违规事件及其等级定义，相应处罚规定等；

8.2.2 二级文件

数据安全管理制度和办法，是指数据安全通用和各生命周期阶段中某个安全域或多个安全域的规章制度要求，比如：

通用安全域：数据资产管理、数据质量管理、数据安全合规管理、系统资产管理，等等。

数据生命周期各阶段：数据采集安全管理、数据存安全管理、数据传输安全管理、数据交换安全管理、数据使用安全管理、数据销毁安全管理，以及某个安全域的安全管理要求，等等。

8.2.3 三级文件

数据安全各生命周期及具体某个安全域的操作流程、规范，及相应的作业指导书或指南，配套模板文件等。

在保证生命周期和安全域覆盖完整的前提下，可以根据实际情况整合流程和规范的文档数量，不一定每个安全域或者每个生命周期阶段都单独建立流程和规范。数据安全操作指导书或指南，是对数据安全管理流程和规范的解释和补充，以及案例说明等文档，以方便执行者深入理解和执行；并非强制执行的制度规范，仅供参考。

数据安全模板文件是与管理流程、规范和指南相配套的固定格式文档，以确保执行一致性，以及数据或信息的汇总统计等。比如，权限申请和审批表模板，日志存储格式模板，等等。有条件的情况下，一般都通过技术工具实现。

8.2.4 四级文件

指执行数据安全管理制度产生的相应计划、表格、报告、各种运行/检查记录、日志文件等，如果实现自动化，大部分可通过技术工具收集到，形成相应的量化分析结果，也是数据的一部分。

9 数据安全技术工具

9.1 技术工具架构设计

数据生命周期中所有安全域涉及到的技术工具，可以是独立的系统平台、工具、功能或算法技术等，在规划设计时不用单独针对某个安全域，需要整体考虑。尤其涉及到通用的技术工具，需要整合，且和组织的业务系统和信息系统等进行衔接。

围绕组织业务系统和数据流，技术工具整体设计框架参考如下图：

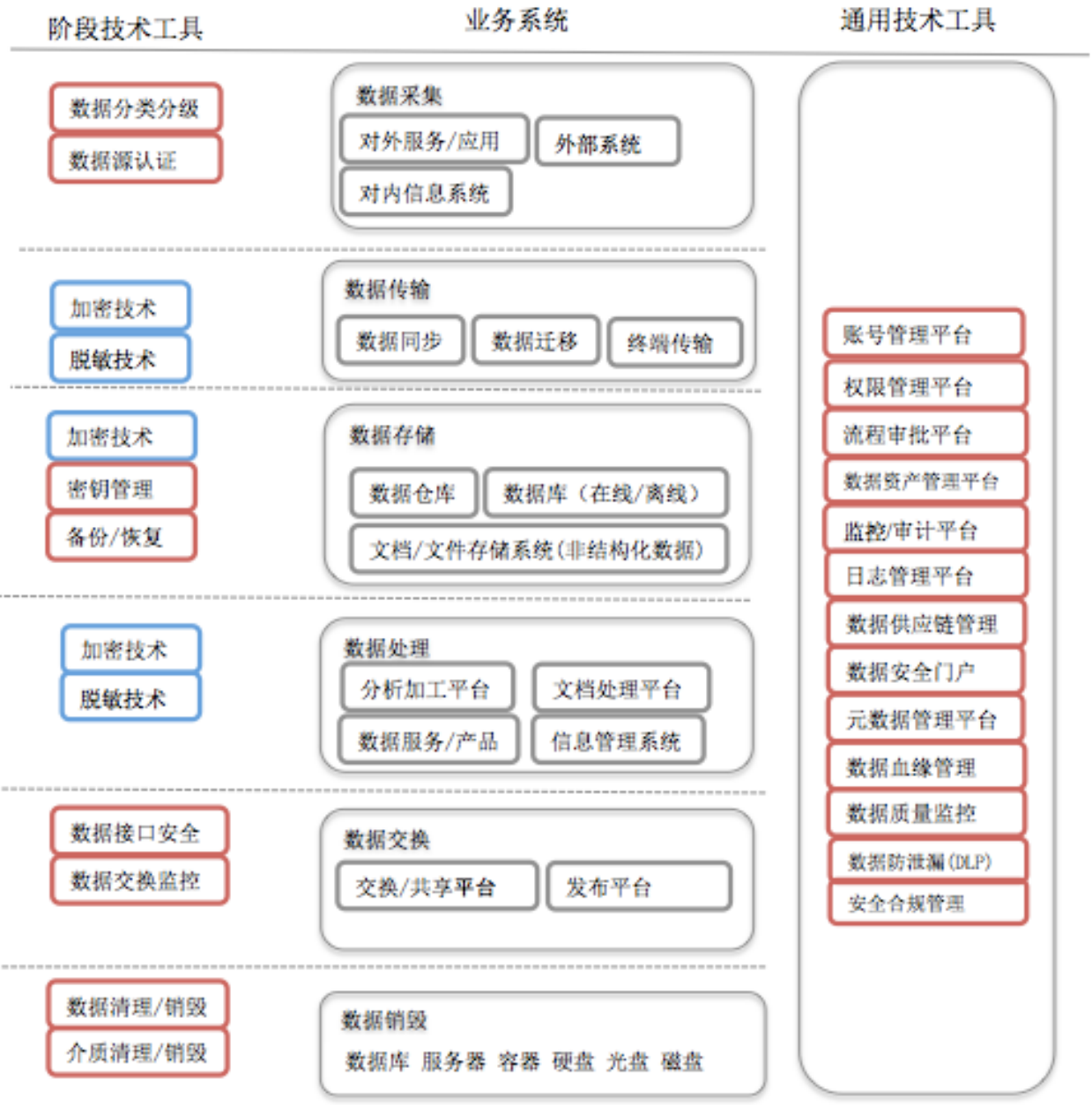
阶段技术工具
业务系统
通用技术工具
数据分类分级
数据源认证
数据采集
对外服务/应用
外部系统
对内信息系统
加密技术
脱敏技术
数据传输
数据同步
数据迁移
终端传输
加密技术
密钥管理
备份/恢复
数据存储
数据仓库
数据库（在线/离线）
文档/文件存储系统(非结构化数据)
加密技术
脱敏技术
数据处理
分析加工平台
文档处理平台
数据服务/产品
信息管理系统
数据接口安全
数据交换监控
数据交换
交换/共享平台
发布平台
数据清理/销毁
介质清理/销毁
数据销毁
数据库 服务器 容器 硬盘 光盘 磁盘
账号管理平台
权限管理平台
流程审批平台
数据资产管理平台
监控/审计平台
日志管理平台
数据供应链管理
数据安全门户
元数据管理平台
数据血缘管理
数据质量监控
数据防泄漏(DLP)
安全合规管理

图5：技术工具架构图

数据安全技术工具和各个安全域对应关系如下表：

表3：技术工具和PA对照表

阶段	技术工具	涉及 PA	安全域
通用	账号管理平台	PA1-PA27	编号 安全域 PA01 数据分类分级 PA02 数据采集安全管理 PA03 数据源鉴别及记录 PA04 数据质量管理 PA05 数据传输加密 PA06 网络可用性管理 PA07 存储介质安全 PA08 逻辑存储安全 PA09 数据备份和恢复 PA10 数据脱敏 PA11 数据分析安全 PA12 数据正当使用 PA13 数据处理环境安全 PA14 数据导入导出安全 PA15 数据共享安全 PA16 数据发布安全 PA17 数据接口安全 PA18 数据销毁处置 PA19 介质销毁处置 PA20 数据安全策略 PA21 人力资源安全 PA22 合规管理 PA23 数据资产管理 PA24 数据供应链安全 PA25 元数据安全 PA26 终端数据安全 PA27 监控与审计
	权限管理平台	PA1-PA27	
	流程审批平台	PA1-PA27	
	数据资产管理平台	PA1-PA27	
	监控/审计平台	PA1-PA27	
	日志管理平台	PA1-PA27	
	数据供应链管理平台	PA1-PA05，PA14-PA19	
	数据安全门户	PA1-PA27	
	元数据管理平台	PA1-PA27	
	数据血缘管理	PA1-PA27	
	数据质量监控	PA1-PA17，PA23-PA25	
	安全合规管理	PA02、PA16、PA22	
数据采集	数据分类分级	PA01	
	数据源认证	PA02、PA03	
数据传输	加密技术	PA05	
	脱敏技术		
数据存储	加密技术	PA07、PA08、P09	
	密钥管理	PA07、PA08	
	备份/恢复	PA09	
数据处理	加密技术	PA10-PA14	
	脱敏技术		
数据交换	数据接口管理	PA17	
	数据交换监控	PA14-PA16	
数据销毁	数据清理/销毁	PA18	
	介质清理/销毁	PA19	

9.2 技术工具架构说明

9.2.1 业务系统

业务系统是组织业务运行的信息系统，包括前台应用、后台数据库和管理平台等等，支撑数据从采集、存储、传输、处理、交换到销毁整个生命周期过程，几乎所有数据安全的技术工具都要对接并运用在这些信息系统上。

9.2.2 通用技术工具

通用技术工具是指所有或绝大部分生命周期阶段（或安全域）都要用到的技术工具，或者是数据安全管理的基础平台，或者是整合数据安全管理信息和入口的门户网站等。比如身份和权限控制平台，所有业务系统和管理平台要接入进行统一控制；日志管理平台，需要从所有业务系统和管理平台采集系统和访问者操作日志，并统一日志规范以方便后续监控和审计。

9.2.3 各阶段技术工具

各阶段技术工具，仅部分生命周期阶段（或安全域）适用的技术工具，或者是一些单独的算法技术和功能模块，只对接或应用到部分信息系统和管理平台。比如数据分分级打标工具，对数据资产进行打标；比如数据安全接口管理，对数据库接口调用安全进行管理；比如加密技术，脱敏技术，应用在数据存储和传输等过程。

10 数据安全域实施指南

该章节将结合制度流程和技术工具整体规划设计和实施要求，对数据生命周期每一个安全域充分定义级（三级）的背景目标和实践要求进行解读，并给出一些实施指南和案例参考。

10.1 数据采集安全

10.1.1 PA01 数据分类分级

10.1.1.1 过程域设定背景和目标

大数据应用在不断发展创新的同时，由于数据违规收集、数据开放与隐私保护相矛盾以及粗放式“一刀切”管理方式等给大数据应用的发展带来严峻的安全挑战。大数据资源的过度保护不利于大数据应用的健康发展，数据分类分级的安全管控方式能够避免“一刀切”带来的问题，通过对数据进行分类分级，实现数据资源的精细化管理和保护，确保数据应用和数据保护的有效平衡。

10.1.1.2 过程域具体标准要求解读

- **制度流程：**

——数据资产的分类分级管理包括两个层面：首先需要先制定组织机构层面的数据分类分级原则和要求，如按照数据的重要程度进行分类，在数据分类基础上根据数据损坏、丢失、泄漏等对组织造成形象损害或利益损失程度进行数据分级等；其次在组织机构总体分类分级的原则下，可针对具体关键业务场景制定数据分类分级的实施细则，这里的数据分类分级应包含有业务属性；

——数据分类分级目的是为了对数据采取更合理安全管理和保护，需要对分类分级的数据进一步制订具体的保护细则，包括对不同级别的数据进行标记区分、明确不同数据的访问人员和访问方式、采取的安全保护措施（如加密、脱敏等）；

——数据分类分级的建立及变更审核流程，是指在具体数据分类分级应用场景中对数据分类分级的执行过程、结果确认及分类分级的变更等过程需要明确详细的操作流程及相关的审核机制，避免出现与分类分级原则和制度不符合的情况发生。

- **技术工具：**

数据分类分级工具：通过对识别的数据资产进行分类分级，针对不同级别的数据进行策略设置，以实现敏感数据的识别和跟踪管理。数据分类分级一般包括主要功能：

——支持多种敏感数据识别模式，包括预定义模式、自定义模式、相似数据发现模式等；

——支持常见的敏感数据类型发现能力，包括姓名、电话号码、邮箱、身份证号码、银行卡号、住址等；

——支持对数据进行自定义分类和分级，用户可通过编写不同的识别规则如正则表达、关键字匹配等来识别自定义的敏感数据；

——支持相似性敏感数据发现功能，通过对已指定的部分样本数据进行机器学习，从而对其它类似数据进行分类分级；

——支持对识别数据进行标记的管理，包括标记自定义、标记设置、标记变更等功能；

——应包括数据分类分级的操作、变更过程进行日志的记录和分析功能；

10.1.1.3 过程域充分定义级实施指南

- 制度流程参考：

  数据分类分级实施建议：

  - 数据分类分级在具体执行过程中，应综合考虑数据分类分级粒度对数据生命周期各阶段的实现过程的影响，包括人员能力、工具实现等情况，建议多次逐步递进的惯例，不要求一步到位；过度复杂的分类分级方案可能对使用来说不方便和不经济，或许是不实际的；
  - 在数据分类时应防止出现分类重复或交叉的情况，可以根据业务数据特点分成几个大类，对于较复杂的数据场景还可以对大类进一步细化二级分类；
  - 数据分级可根据数据的保密性、完整性和可用性这三个安全目标进行分级，也可依据数据受到破坏后产生的潜在影响进行分级；

  案例：《xx组织数据分类分级实施指引》关键内容：

  - 数据范围
  - 数据分类分级角色和职责
  - 数据分类的原则
  - 数据分类分级方法
  - 数据分类、数据分级
  - 建立数据分类分级清单
  - 数据生命周期的保护机制
  - 数据分类分级的关键问题处理

- 技术工具参考：

  - 标签库：根据分类分级规则，建立标签库；可以单独成一个静态库，也可以直接在打标工具/系统后台进行配置；
  - 结构化数据打标：用户在建表时对字段标签直接进行设置，基于数据库的权限模型对底层数据表的列权限控制；
  - 非机构化数据打标：引入自然语言处理、数据挖掘和机器学习进行等技术，对内容识别并实现数据分类分级。比如文本识别的机器学习过程：
  - 标注：利用人工对一批文档进行了准确分类，以作为训练集（进行机器学习的材料）；
  - 训练：计算机从这些文档中挖掘出一些能够有效分类的规则，生成分类器（总结出的规则集合）；
  - 分类：将生成的分类器应用在有待分类的文档集合中，获取文档的分类结果。由于机器学习方法在文本分类领域有着良好的实际表现，已经成为了该领域的主流。

- 标准参考：

——DB 52/T 1123—2016《政府数据 数据分类分级指南》

10.1.2 PA02 数据采集安全管理

10.1.2.1 过程域设定背景和目标

数据采集过程中涉及包括个人信息及商业数据在内的海量数据，现今社会对于个人信息和商业秘密的保护提出了很高的需求，需要防止个人信息和商业数据的滥用，采集过程需要信息主体授权，并应当依照法律、行政法规的规定和与用户的约定，处理其相关数据；另外还应在满足相关法定的规则的前提下，在数据应用和数据安全保护间寻找适度的平衡。

10.1.2.2 过程域具体标准要求解读

- 制度流程：

——建立数据采集安全合规管理规范：明确数据采集的目的、用途、方式、范围、采集源、采集渠道等内容，对外部数据提供方及被采集者提供的数据进行合法性和正当性的确认，必须满足相关法律法规要求；

——建立数据采集的风险评估流程：明确数据采集的风险评估方法、评估周期、评估对象，识别相关的法律法规并纳入合规评估，如是否符合《网络安全法》、《个人信息安全规范》等国家法律法规及行业规范；

——数据采集过程的数据保护：明确数据采集过程中的个人信息和重要数据的安全控制措施，如采取数据脱敏、数据加密、链路加密等，确保数据在采集过程中的个人信息和重要数据不被泄漏。

- 技术工具：

——部署数据采集系统或相关工具，设置统一的数据采集策略（如采集周期、频率、采集内容等）对数据进行采集，保证数据采集流程实现的一致性；并且在采集过程中对被采集方授权同意采集的过程和信息进行日志记录；

——实施数据采集过程的数据防泄漏安全技术措施：如采集数据的加密、采集链路加密、敏感信息和字段的脱敏、权限的访问控制等，这些措施一般是指在采集后传输、存储等过程中的安全保护，可参考其它安全相关安全域的工具实现；

10.1.2.3 过程域充分定义级实施指南

- 制度流程参考：

案例：《xx组织数据采集安全合规管理规定》关键内容：

- 数据采集规则：采集目的、采集用途、采集方式、采集范围
- 采集岗位职责：负责采集相关工作的岗位和职责
- 数据采集评估：风险评估方法、评估周期、评估对象、整改要求等
- 采集过程保护：防护数据类型、安全措施、审计要求等
- 合规性说明：相关法律法规和监管要求

- 标准参考：

  暂无

10.1.3 PA03 数据源鉴别及记录

10.1.3.1 过程域设定背景和目标

数据源鉴别是指对收集或产生数据的来源进行身份识别的一种安全机制，防止采集到其它不被认可的或非法数据源（如机器人信息注册等）产生的数据，避免采集到错误的或失真的数据；数据源记录是指对采集的数据需要进行数据来源的标识，以便在必要时对数据源进行追踪和溯源。

10.1.3.2 过程域具体标准要求解读

- 制度流程：

  ——数据源管理制度规范需要包含两个方面的内容：一是要对数据采集来源的管理，包括采集源识别和管理、采集源的安全认证机制、采集源安全管理要求等内容；二是对针对采集的数据在数据生命周期过程中进行数据溯源的管理，把数据流路径上的每次变化情况保留日志记录，保证结果的可追溯，以及数据的恢复、重播、审计和评估等功能；

- 技术工具：

  ——针对采集的数据识别和记录工具：如元数据管理、数据血缘管理等工具对采集数据进行数据采集来源的标识

  ——针对数据采集源(人员、终端、数据库等)识别和记录的工具：如身份鉴别机制、指纹识别等技术防止数据采集点的仿冒或伪造。

10.1.3.3 过程域充分定义级实施指南

- 制度流程参考：

本安全域的制度流程可与其它安全域的制度相整合，如数据源的鉴别认证相关要求可与数据采集安全管理相关制度进行整合编写；溯源数据存储可以在数据存储管理制度中。

- 技术工具实施参考：

数据血缘管理工具：数据从源到目的地， 经过大量的功能模块的处理和传递，呈现在业务用户面前，很多时候需要对数据的来龙去脉进行分析 。 例如两个数据报表进行对比，结果差异很大，需要人工核对分析指标的维度信息，分析数据指标从哪里来，处理条件是什么，最后才能分析出问题原因。 又如基础数据表因某种原因需要修改字段时 ，需要评估其对数仓的影响。 通过元数据管理以历史事实的方式记录每项数据的来源，处理过程，应用对接情况等，记录了数据表在治理过程中的全链血缘关系，基于这些血缘关系信息，可以进行影响分析，以数据流向为主线的血缘追溯等功能。 血缘关系图示例：

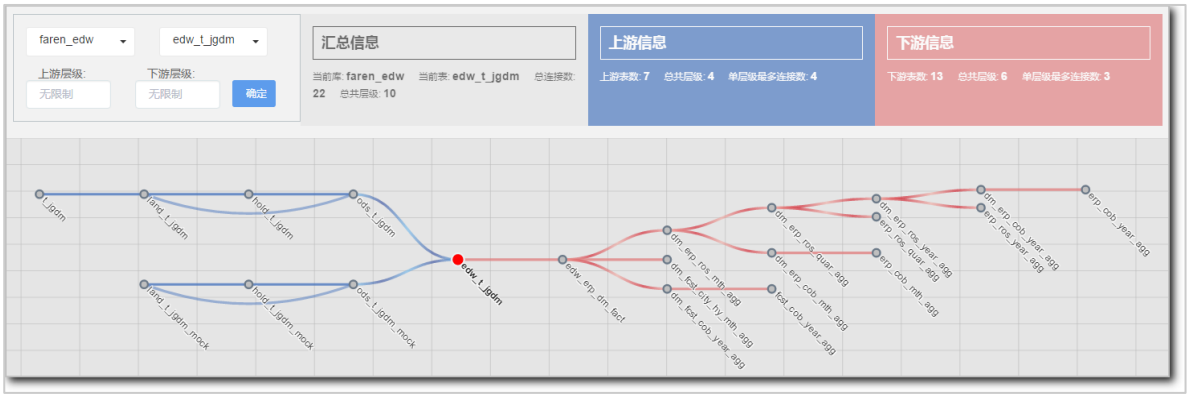

图6：数据血缘中表级上下游关系图

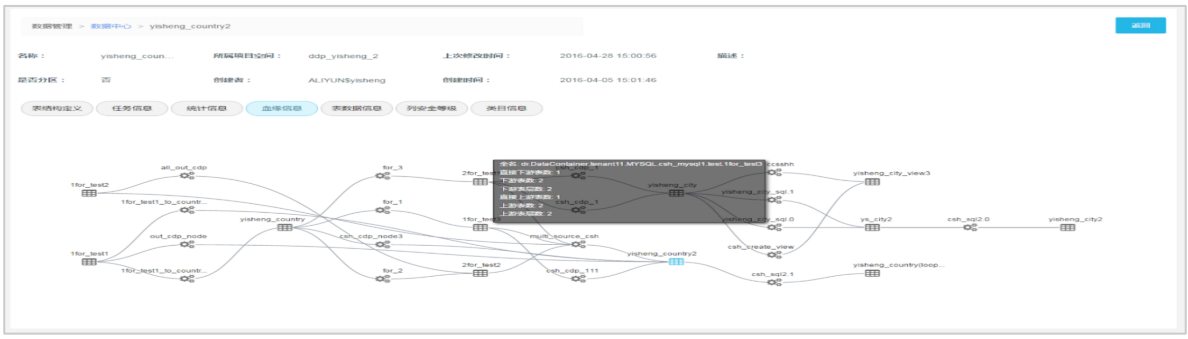

图7：数据血缘中作业级上下游关系图

10.1.4 PA04 数据质量管理

10.1.4.1 过程域设定背景和目标

数据安全保护的对象是有价值的数据，而有价值的前提是数据质量要有保证，所以必须要有数据质量相关的管理体系。本安全域设置目是保证对数据采集过程中收集和产生的数据的准确性、一致性和完整性。

10.1.4.2 过程域具体标准要求解读

- 制度流程：

——定义什么是“数据质量”，数据质量的属性一般包括一致性、完整性、准确性和失效性等；

——数据质量校验方法，比如校验的层次（人工比对/程序比对/统计分析等）和校验方法（时效性/完整性/原则性/逻辑性等）

——数据质量管理实施流程，比如在产品研流中植入数据质量控制手段，涉及需求、系统设计、开发、测试、发布及运维；

——数据采集质量管理规范，包含数据格式要求、数据完整性要求、数据质量要素、数据源质量评价标准；

- 技术工具：

——对数据资产进行等级划分，具体打标规则和方法等见数据分类分级和元数据管理等安全域有更详细介绍；

——在线数据质量监控，比如针对业务数据库实时产生的数据；

——离线数据质量监控，比如针对数据仓库或数据开发平台的离线数据；

——数据质量事件处理流程，根据监控结果一旦发现数据质量异常进行及时告警和上报，并及时采取更正等处理措施。

10.1.4.3 过程域充分定义级实施指南

- 制度流程参考：

案例1：《XX集团数据质量管理规范》关键内容：

- 术语定义：数据/元数据/数据质量/数据质量问题
- 数据质量管理规范：职责要求/度量与标准/控制流程（需求-设计-开发-测试-发布）
- 数据订正规范：需求-方案-审批-执行-验证
- 数据质量事件处理：定级和分类/原因分类/产生环节/处理流程
- 数据质量审计：审计流程/审计内容
- 违规责任：违规分级/责任和处罚

案例2：《xxx组织数据质量管理讲座》关键内容：

- 数据质量问题分析
- 数据质量方法论
- 数据质量保证成功因素
- 数据质量案例分析

- 技术工具实施参考：

离线数据质量监控：对离线数据库数据表进行校验,比如表行数/主键监控/波动检测/业务逻辑等。可以考虑基于数据库单表的记录生命周期时效性态监控，或全量表间记录同步核对监控：如上游系统A表数据应在下游系统有B表数据对应。

案例1：XXX离线数据监控：

- 监控粒度：针对表的分区进行配置，分区是依附于表；监控可以设定在任务粒度或SQL粒度，任务粒度表示只有当整个任务的脚本都运行结束后监控规则才会运行；SQL粒度则是一段SQL执行完毕若生成的表配有监控，则运行；
- 监控规则：配置的规则是数据的正向期望，即希望数据是什么样的就怎么配置规则，如希望数据的分组不能超过2，所以配置<=2；
- 运行时间：将直接反映在任务的总运行时间中，监控可以在表创建15分钟后配置。
- 触发机制：监控的分区生成或更新时；

目前离线数据质量主要有**波动值检测**和**固定值比较**两种校验方式。

表 4：离线数据质量校验方式

校验方法	**校验逻辑**
波动值校验	1. 如果校验值的绝对值小于或等于橙色阈值，则返回正常。 2. 如果校验值的绝对值不满足第一种情况，且小于或等于红色阈值，则返回橙色报警。 3. 如果校验值不满足第二种情况，则返回红色报警。 4. 如果没有橙色阈值，则只有红色报警和正常两种情况。 5. 如果没有红色阈值，则只有橙色报警和正常两种情况。 6. 两个都不填，则红色报警（前端会禁止两个阈值不填的情况）。
固定值比较	1. 根据校验的表达式，计算 s opt expe c t，返回布尔值，opt 支持大于、小于、等于、大于等于、小于等于、不等于。 2. 根据上式的计算结果，如果为 true，返回正常，否则返回红色报警。

常见的监控规则说明：

表5：离线数据质量常见监控规则设置示例

模板级别	模板名称	说明
1	字段平均值，相比 1 天、1 周、1 个月前波动率	取该字段的平均值，同 1 天，7 天，一个月周期比较，计算波动率，然后与阈值比较，只要有一个报警就报警出来。
2	字段汇总值，相比 1 天、1 周、1 个月前波动率	取该字段的 sum 值，同 1 天，7 天，一个月周期比较，计算波动率，然后与阈值比较，只要有一个报警就报警出来。
3	字段最小值，相比 1 天、1 周、1 个月前波动率	取该字段的最小值，同 1 天，7 天，一个月周期比较，计算波动率，然后与阈值比较，只要有一个报警就报警出来。
4	字段最大值，相比 1 天、1 周、1 个月前波动率	取该字段的最大值，同 1 天，7 天，一个月周期比较，计算波动率，然后与阈值比较，只要有一个报警就报警出来。
5	字段唯一值个数	去重之后的 count 数与一个期望数字进行比较，即固定值校验。
6	字段唯一值个数,相比 1 天、1 周、1 个月前波动率	去重之后的 count 数，同 1 天，1 周，1 个月作比较，即固定值校验
7	表行数，相比 1 天、1 周、1 个月前波动率	同 1 天、一周、一月前采集的表行数作比较，对比波动率。
8	字段空值个数	去该字段的空值数与固定值比较。
9	字段空值个数 / 总行数	空值个数与行总数，计算得到一个比率，与一个固定值做比较，注意：该固定值是一个小数。
10	字段重复值个数 / 总行数	重复值个数与总行数的比率与一个固定值做比较。

在线数据监控：首先根据线上业务逻辑制定产生数据的监控规则，通过接收实时消息进行相关的规则校验，抓取线上脏数据并进行报警，并及时处理。下图为某在线业务数据质量监控平台实现流程：

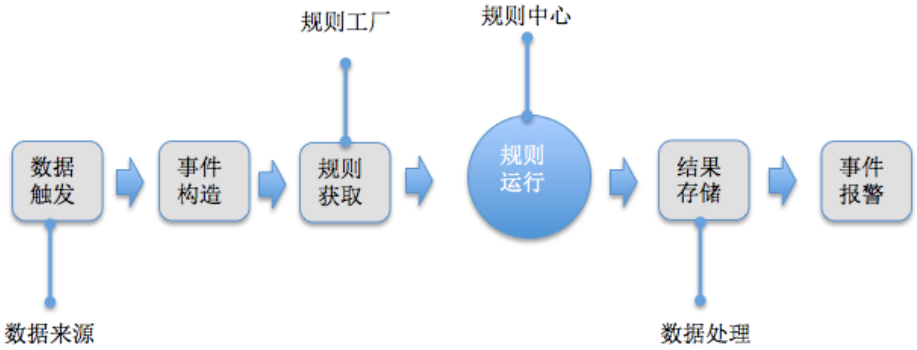

图8：某在线业务数据质量监控实现流程

10.2 数据传输安全

10.2.1 PA05 数据传输加密

10.2.1.1 过程域设定背景和目标

数据在通过不可信或者较低安全性的网络进行传输时，容易发生数据被窃取、伪造和篡改等安全风险，因此需要建立相关的安全防护措施，保障数据在传输过程中的安全性，而加密是保证数据安全的常用手段。本过程域的设定，即要求建立相关加密措施来保障数据在传输过程中的机密性、完整性和可信任性。

10.2.1.2 过程域具体标准要求解读

该过程域要求组织机构采用适当的加密保护措施，确保数据在传输过程中的安全性。然而对数据进行加密传输会消耗系统资源，降低数据传输接口的吞吐量和响应速度，增加使用成本。同时采用不同的加密算法和使用不同强度的密钥，也会导致系统开销的差异化，带来不同的使用成本。因此组织需要对使用加密传输的业务场景以及使用的加密传输方式进行明确定义，并建立相关的技术工具。

- 制度流程：

  ——根据国家法律法规的要求，以及所属行业监管部门的要求，结合自身业务数据对保密性和完整性的需求，来确定需要加密传输的场景，通常情况下，凡是涉及到国家重要信息、企业机密信息和个人隐私信息的数据传输场景，都应进行加密传输。

  ——在做好数据分类分级的工作的基础上，进一步在制度中明确不同安全级别数据的加密传输要求，包括采用的算法要求和密钥的管理要求。即明确什么安全级别的数据，应采用什么加密算法（国密算法还是国际算法，对称加密算法还是非对称加密算法），应使用多少加密强度的密钥，密钥的有效期是多久（多长时间需要更换加密密钥）等。

- 技术工具：

  ——要求在建立传输加密通道前，对两端的主体身份进行鉴别和认证，确保数据传输双方是可信

任的。

——针对需要加密的场景确定加密的方案，通过加密产品或工具落实制度规范所约定的加密算法要求和密钥管理要求，确保数据传输过程中机密性和完整性的保护，同时加密算法的配置、变更、密钥的管理等操作过程应具有审核机制和监控手段。

——需要有完整的密钥管理系统，实现对密钥生命周期的安全管理。

总体来讲，是需要通过加密传输达到以下目的：

——机密性：只有自己和允许的人才能看到或看懂数据；

——完整性：数据在传输过程中没有被破坏或篡改；

——可信任性：确保消息是对方发的，不是伪造者发的。

10.2.1.3 过程域充分定义实施指南

组织首先应明确需要进行加密传输的场景，并非所有的数据都需要进行加密传输，通常需要进行加密传输的数据包括但不限于**系统管理数据、鉴别信息、重要业务数据和重要个人信息等对机密性和完整性要求较高的数据。**这些数据在以下场景下传输时应考虑加密方式传输：

——通过不安全或者不可控的网络进行数据传输的，例如互联网、政务外网等。

——从高安全等级区域经过低安全等级区域向高安全等级区域传输的。

——在等保定级为三级或三级以上信息系统中传输的。

在定义好需要加密的场景后，组织应选择合适的加密算法对数据进行加密传输，在数据传输场景中主要用到的加密算法有对称加密算法、非对称加密算法和哈希算法。

对称加密算法：对称加密算法的基本特征是用于加解密的密钥相同，且加密的操作是可逆的。即通过同一把密钥将明文数据变成密文数据，同时可以用同一把密钥将密文数据还原成明文数据，主要用来实现数据传输的机密性保障。对称加密算法的优点是算法简单、计算量小、加密速度快、加密效率高，适合加密大量数据。缺点是密钥管理不方便，传输双方之间需要共享密钥，随着网络规模的增大密钥会越来越多，管理会越来越困难，其次因为使用同一把密钥进行加解密，传输双方的密钥共享过程也存在风险，密钥可能会被窃取。目前主要的对称加密算法有：DES、IDEA、AES、SM1（国密算法）等

非对称加密算法：非对称加密算法（也叫公钥密码算法）加密密钥和解密密钥不同，由加密密钥很难（基本不可能）推导出解密密钥。一个密钥可以公开，称为公钥，另一个密钥只有自己知道，称为私钥。用公钥加密的内容只能由相应的私钥来解密，反过来，用私钥加密的内容只能由相应的公钥来解密。对称加密算法可用于解决数据传输机密性保障（用公钥加密数据，用私钥解密数据），同时也可用于身份的确认（用私钥加密数据，公钥解密数据），因为私钥是不公开且被用户个人保护的，因此一个加密数据能用谁的公钥解密，就可以认为是该用户发送的信息。非对称加密算法的优点是密钥管理很方便，由于一个密钥可公开，很好解决了对称加密算法密钥传递的问题。缺点是计算复杂、消耗资源大，加密速度慢。常用

的非对称加密算法有RSA、ECC、SM2（国密算法）。 为了方便传递公钥私钥，一般把它存储在数字证书中，为了保证证书的可信性，一般由专业第三方证书机构颁发。

哈希算法：哈希算法是一种单向函数，其特点是正向计算很容易，而反向计算非常困难。通过哈希算法将任意长度的数据映射成为固定长度的输出，输出称作哈希值，不同数据通过哈希函数计算后会得出不同的哈希值，通过哈希值的比对可以判断数据是否被修改过，可用于数据完整性校验。哈希函数主要有MD5、SHA等算法。

在实际的加密传输场景中，我们通常采用了以上算法的组合，来实现对数据传输过程的机密性和完整性保护，通常较多的采用建立VPN加密传输通道、使用SSL/TLS加密传输协议等技术方式来实现，这些技术普遍采用非对称加密来建立连接，确认双方的身份并交换加密密钥，用对称加密来传输数据，并用哈希算法来保障数据的完整性。这样既保证了密钥分发的安全，也保证了通信的效率。

由于目前加密技术的实现都依赖于密钥，因此对密钥的安全管理是非常重要的环节。只有密钥安全，不容易被敌方得到或破坏，才能保障实际传输中加密数据的安全，密钥管理系统就是为解决密钥的安全管理问题，实现对密钥生命周期的安全管理。密钥管理系统主要解决如何在不安全的环境下，为用户分发密钥信息，使得密钥能够安全、准备并有效的使用，并在安全策略的指导下处理密钥自产生到最终销毁的整个过程。

最后，对于负责加密策略配置以及密钥系统管理的人员，必须有一个审核监督机制，确保其加密算法的配置和变更都是得到授权和认可的，目前通常采用堡垒机的方式进行监督管理。即要求管理人员通过堡垒机来操作对传输加密策略的配置和密钥管理系统的管理操作，堡垒机可以在用户执行这些操作的时候对他的操作情况进行记录，以便后期审核，同时可规定执行哪些操作需要相关人员的授权和确认。

10.2.2 PA06 网络可用性管理

10.2.2.1 过程域设定背景和目标

数据在网络传输过程中依赖网络的可用性，一旦发生网络故障或者瘫痪，数据传输也会受到影响甚至中断。本过程域的设定，即要求建设高可用性的网络，从而保证数据传输过程的稳定性。

10.2.2.2 过程域具体标准要求解读

该过程域要求组织机构采取适当的措施，确保关键业务网络的高可用，并在技术工具维度进行了指导建议，一是对关键业务网络的传输链路、网络设备节点进行冗余建设。二是借助负载均衡、防入侵攻击等安全设备来降低网络的可用性风险。

10.2.2.3 过程域充分定义实施指南

网络节点与网络链路的故障无法完全避免，所以提升网络可用性的重要方法之一是尽量降低系统的故障恢复时间，而通过冗余配置，将发生故障的网络设备或系统切换至备用的设备或系统上，是恢复业务的最快方式。

可用性考核指标：

表6：网络可用性常见考核指标参考

要求	指标说明	建议要求指标
单次最长故障时间	单次最长的非计划性不可用时间	<1h
重大事件发生次数	发生重大事件的数量	<2/年
网络可用性	在整个系统的运行时间内，正常事件占全部运行事件的比例	>=99.5%(运行时间按5*8或7*24计算)

系统冗余建设通常有以下几种方法：

1） 硬件冗余：

a) 电源冗余：核心层设备上采用双电源冗余，由芯片控制电源进行负载均衡。

b) 引擎冗余：核心路由器、交换机等重要网络设备使用具备双引擎设备。

c) 模块冗余：核心关键设备需要进行1：1的模块冗余，即每个接口需要一个备份接口，每个模块需要一个备份模块。

d) 设备堆叠：使用堆叠技术实现单交换机端口的扩充。

e) 链路冗余：为上层的冗余设备架设物理上的链接，在冗余网络中，还需要通过二层STP算法或三层动态路由协议实现将特定的端口阻塞或不转发流量，来实现既没有环路也可以冗余的网络。

f) 设备冗余：核心或出口设备上采冗余备份设计。由各设备HA控制流量进行负载均衡。

g) 负载均衡：使用负载均衡技术将特定的业务(网络服务、网络流量等)分担给多个服务器或网络设备。

2） 软件冗余：

a) 链路捆绑技术：把多条独立的网络链路捆绑成为一条单独的逻辑链路，一条链路失效，流量可以在剩下的链路上继续传输。

3） 路由冗余：

a) VRRP：采用虚拟路由冗余协议（VRRP，Virtual Router Redundancy Protocol），可解决局域网中配置静态网关出现单点失效现象的路由协议。

b) 动态路由协议：网络中使用RIP、OSPF等动态路由协议，实现网络路由的冗余备份，当一个主路由发生故障后，网络可以自动切换到它的备份路由实现网络的连接。

- 标准参考：

——GB／T 25068.1-2012《信息技术 安全技术 IT 网络安全 第 1 部分:网络安全管理》第 13.4 节“网络安全管理”

10.3 数据存储安全

10.3.1 PA07 存储介质安全

10.3.1.1 过程域设定背景和目标

数据存储在介质上，比如物理实体介质（磁盘/硬盘/），虚拟存储介质（容器/虚拟盘）等，对介质的不当使用及其容易引发数据泄露风险。

10.3.1.2 过程域具体标准要求解读

- 制度流程：

  ——存储介质及其类型定义，比如物理实体介质（磁盘/硬盘/），虚拟存储介质（容器/虚拟盘）等；

  ——不同分类分级的存储介质要求；

  ——存储介质购买和可信渠道审批要求；

  ——存储介质使用审批和净化处理要求，比如对介质访问的身份识别，权限控制，以及数据清理或销毁等；

  ——存储介质标记要求，比如分类,标签及其有效期等；

  ——存储介质入库和保存要求，比如介质库存放要注意防尘、防潮，远离高温和强磁场，以及保存期限等；

  ——存储介质使用的常规和随机审查要求，比如对介质定期检查，以防信息丢失；

- 技术工具：

  ——介质净化工具，主要是针对物理实体介质（磁盘/硬盘/）

10.3.1.3 过程域充分定义级实施指南

- 制度流程参考：

  案例1：《xxxx信息中心存储介质安全管理规定》关键内容：

  - 存储介质定义
  - 安全管理员职责

- 存储介质管理要求
- 存储介质中数据测试
- 存储介质维修要求
- 存储介质销毁和报废要求
- 附件：使用/维修/报废登记表

案例2：《xxxx公司介质安全管理规范》关键内容：

- 存储介质及其分类定义
- 介质存放环境要求：仓库/指定区域/防尘防潮防静电/防盗/监控/出入库登记
- 介质运输安全：发货/收货
- 介质使用规范：申请工单/使用人登记
- 介质维修规范： 返厂/操作人/时间/场地等
- 介质销毁规范：消磁机/SSD数据擦除机/销毁平台/销毁方式/销毁记录等

- 技术工具参考：

市面上针对存储介质上数据的消除工具，很多还是根据基于国家保密局颁发的BMB21-2007《涉及国家秘密的载体销毁与信息消除安全保密要求》为标准研发的。支持对硬盘、软盘、U盘、CF卡等多种存储介质的信息消除。消除方法灵活多样，既可以对计算机上的硬盘直接进行信息消除，也可以对拆卸下来的硬盘等进行信息消除。存储介质被信息消除后仍然可以根据国家保密局的相关规定重复使用。

比如某信息清除工具的主要功能：

系统平台：基于Windows操作系统平台，可限度的利用Windows对各种存储介质的兼容性优势

擦除速度：擦除速度可利用当前计算机的CPU频率，避免ARM和工控机结构擦除工具带来的CPU速度瓶颈问题

介质类型：可擦除硬盘、U盘、CF卡等各种存储介质，的存储兼容性

擦除效率：最多可以同时擦除25个存储介质，擦除效率高

擦除方法：既可以对整个存储介质进行擦除，也可以对分区进行擦除，还可以删除指定文件目录和单个文件，根据要求，还可以清除未使用的扇区和磁道

状态显示：各种状态显示完整，用户对消除过程一目了然

稳定性能：擦除过程中拔插存储介质不影响工具的正常运行，稳定性好

擦除标识：信息消除后可以打印出不干胶贴，粘帖在介质上，方便识别

存储介质主要包括：

- 磁带：分为Type I、II、III等3类，Type I指磁化记录时的磁场强度为350厄斯特（oersted，磁场强度单位，缩写为Oe）以下，Type II介于351与7500e之间，Type III则大于7500e；目前最普遍使用的LTO-3、4磁带，磁场强度便分别高达2600与27100e。
- 磁盘：包括Bernoulli式磁盘、软盘、不可移动的硬盘与可移动的硬盘等4种类型。
- 光盘：包括可多次读写、只读与一次写入多次读取（WORM）等3种。
- 内存：包括动态随机存取内存（DRAM）、静态随机存取内存（SRAM）、只读存储器（ROM）、可程序化只读存储器（PROM）、可程序化可抹除只读存储器（EPROM）、快闪EPROM（Flash EPROM）、电子可变只读存储器（EAPROM）、电子可抹除只读存储器（EEPROM）、非挥发性RAM（NOVRAM），还有古老的磁芯、磁泡、磁阻与镀磁线等13种内存。

- 标准参考：

——BMB21-2007《涉及国家秘密的载体销毁与信息消除安全保密要求》

——SJ 20901-2004 硬磁盘信息消除器通用规范

10.3.2 PA08 逻辑存储安全

10.3.2.1 过程域设定背景和目标

针对存储容器和存储架构的安全要求，比如认证鉴权、访问控制、日志管理、通信举证、文件防病毒等安全配置，以及安全配置策略，以保证数据存储安全。

10.3.2.2 过程域具体标准要求解读

- 制度流程：

——逻辑存储系统和存储设备定义；

——逻辑存储系统架构设计及其安全要求；

——逻辑存储的安全配置规则，以及配置变更和发布要求；

——逻辑存储的多租户隔离、授权管理规范要求；

——存储设备安全管理规范和操作规程，如标准操作流程、维护操作流程、应急操作流程等；

——存储系统的账号和权限、日志管理、加密管理、版本升级等要求。

- 技术工具：

——定期对重要的数据存储系统其安全配置进行扫描，以保证符合安全基线要求。

——采集存储系统的操作日志，识别访问账号和鉴别权限，监测数据使用规范性和合理性。

10.3.2.3 过程域充分定义级实施指南

- 制度流程参考：

案例1：《XXX存储系统的安全配置》：

- 认证鉴权：存储系统通过管理平面认证和业务平面的认证，限制可访问存储系统的维护终端及应用服务器。当用户使用存储系统时，只有认证通过后才能对存储系统执行管理操作，并对存储系统上的业务数据进行读写操作。
- 访问控制：提供GUI和CLI两种方式供用户访问存储系统，并对管理资源和业务资源进行访问控制，以确保存储设备和业务数据的安全。
- 日志管理：按时间顺序记录存储系统发生的一系列活动。日志记录可以帮助用户按照顺序搭建及测试周边环境，也可以帮助用户了解在与安全相关的事务中所涉及到的操作、流程以及事件的整体信息。
- 安全策略：管理界面配置用户名策略、密码策略、登录策略和帐号审计策略的方法
- 通信矩阵：各类组件所使用的数据传输端口是存储系统通讯重要的部件。当用户对网络配置安全性要求较高时，请先了解各类组件所需的网络端口类型，以便在搭建组网时，开启相应的端口，以便链路正常连接。
- 安全加固：对存储系统的弱点进行识别和修复，消除或降低存储系统的安全隐患。OceanStor 2200 V3/2600 V3存储系统支持对操作系统加固、Web服务加固、HTTP服务加固以及其他组件加固。
- 文件防病毒：当存储系统运行文件业务并通过CIFS共享将文件系统共享给客户端时，利用第三方防病毒软件触发病毒扫描，及时清理被病毒感染的文件，可以提高存储系统的安全性。

案例2：《Oracle逻辑存储结构介绍》：

- 逻辑存储结构：逻辑存储层次结构和逻辑空间管理
- 数据块：数据块和操作系统块、数据块格式、数据块压缩、数据块的空间管理
- 扩展区：分配扩展区、 释放扩展区、扩展区的存储参数
- 段概述：用户段、临时段、撤销段、段空间和高水位标记
- 表空间：永久表空间、临时表空间、表空间模式、表空间文件大小、实验
- 管理归档日志：预备知识、归档重做日志文件、利用归档恢复过程

- 标准参考：

——GB／T 31916.1-2015《信息技术云数据存储和管理 第 1 部分:总则》

10.3.3 PA09 数据备份和恢复

10.3.3.1 过程域设定背景和目标

备份与恢复是为了提高信息系统的高可用性和灾难可恢复性，在数据库系统崩溃的时候，没有数据库备份就没法找到数据。保证数据可用性是数据安全的基础。

10.3.3.2 过程域具体标准要求解读

- 制度流程：

  ——数据服务可靠性和可用性安全保护目标

  ——数据存储冗余策略和设计指导；

  ——数据复制、备份与恢复的操作规程，如数据复制、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

  ——数据复制、数据备份与恢复的定期检查和更新工作要求，如数据副本更新频率、保存期限等，确保数据副本或备份数据的有效性等。

- 技术工具：

  ——数据备份和恢复的技术工具要统一，并做到自动化执行。

  ——对已备份的数据要有安全管理技术手段，包括但不限于对备份数据的访问控制、压缩或加密管理、完整性和可用性管理。

10.3.3.3 过程域充分定义级实施指南

- 制度流程参考：

  案例1：《XXX公司电子数据备份和恢复管理规程》关键内容：

  - 术语定义：备份/恢复/存档
  - 备份整体要求和原则
  - 独立数据文件：全量和增量
  - 稳健性数据库备份
  - 关系型数据库备份
  - 备份周期
  - 备份完整性检查
  - 备份数据的存储介质要求及其标识
  - 恢复场景
  - 备份日志
  - 相关表格模板：备份记录、检查记录

  案例2：《XXX公司数据备份和恢复管理规范》关键内容：

- 总则：备份和恢复管理范围、关键信息系统定义、管理团队等；
- 数据备份、归档和恢复原则；
- 存储、备份设备及相关设备管理；
- 备份和恢复相关人员职责
- 运维管理流程
- 惩罚措施

- 技术工具参考：

  业界很成熟的技术，这里不赘述。

- 标准参考：

  ——GB／T 31500-2015《信息安全技术 存储介质数据恢复服务要求》

  ——GBT 22239-2008《信息安全技术 信息系统安全等级保护基本要求》

10.4 数据处理安全

10.4.1 PA10 数据脱敏

10.4.1.1 过程域设定背景和目标

数据作为一种重要的生产资料，充分分析与挖掘数据的内在价值成为了现代企业创新成长的必经之路，但同时敏感数据的泄露风险也与日俱增。严格意义上来讲，任何有权限访问数据的人员，均有可能导致敏感数据的泄露。另一方面，没有数据访问权限的人员，也可能有对该数据进行分析挖掘的需求，数据的访问约束大大限制了充分挖掘数据价值的范围。数据脱敏技术通过将敏感数据进行数据的变形，为用户提供虚假数据而非真实数据，实现敏感隐私数据的可靠保护。这样就可以在开发、测试和其它非生产环境以及外包环境中安全地使用脱敏后的真实数据集，既保护了组织的敏感信息不泄露，又达到了挖掘数据价值的目标。本过程域的设定，即要求组织通过建立脱敏机制，来防止组织敏感数据的泄露。

10.4.1.2 过程域具体标准要求解读

本过程域要求组织根据相关法律法规、标准的要求，以及组织自身业务的需求，明确需要脱敏的业务场景、规范要求及使用的脱敏工具。

- 制度流程：

  ——要求组织建立统一的数据脱敏制度规范和流程，明确数据脱敏的业务场景，以及在不同业务应用场景下数据脱敏的规则和方法，这里重点强调的是组织需要统一策略，统一规范。

  ——脱敏应跟使用者的业务权限和数据的使用场景来动态调整，用户申请对敏感数据的访问处理

时，应根据使用者的岗位职责、业务范围等，来评估其使用真实数据的必要性，并根据其业务职责来选择不同的数据脱敏规则及方法。

- 技术工具：

——要求组织具备统一的数据脱敏工具，数据脱敏工具应具备静态脱敏和动态脱敏的功能。

——脱敏工具应与组织的数据权限管理平台实现联动，可以根据使用者的职责权限或者业务处理活动动态化的调整脱敏的规则，职责权限一般用来决定他可以访问哪些敏感数据，业务处理活动则主要决定采用哪些脱敏方式，例如用户展现的敏感数据则可以通过部分数据遮蔽等方式实现，用户开发测试的数据则通过同义替换的方式实现。

——脱敏工具对数据的脱敏操作过程都应该留存日志记录，以审核违规使用和恶意行为，防止意外的敏感数据泄露。

10.4.1.3 过程域充分定义级实施指南

- 制度流程参考：

以下数据在使用时应进行脱敏处理。

——个人信息：能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息。包括个人基本资料、个人身份信息、个人生物识别信息、网络身份标识信息、个人健康生理信息、个人教育工作信息、个人财产信息、个人通信信息、联系人信息、个人上网记录、个人常用设备信息、个人位置信息等。具体可参考 GB/T35273 《信息安全技术 个人信息安全规范》

——组织敏感信息：涉及到组织的商业秘密、经营状况、核心技术的重要信息，包括但不限于客户信息、供应商信息、产品开发信息、关键人事信息、财务信息等。

——国家重要数据：国家重要数据是指组织在境内收集、产生、控制的不涉及国家秘密，但与国家安全、经济发展、社会稳定，以及企业和公共利益密切相关的数据，包括这些数据的原始数据和衍生数据。

- 技术工具参考：

脱敏在技术实现上，主要有以下几种技术方式：

1) **泛化技术。**在保留原始数据局部特征的前提下使用一般值替代原始数据，泛化后的数据具有不可逆性，具体的技术方法包括但不限于：

a) 数据截断：直接舍弃业务不需要的信息，仅保留部分关键信息，例如将手机号码13500010001截断为135；

b) 日期偏移取整：按照一定粒度对时间进行向上或向下偏移取整，可在保证时间数据一定分布特 征的情况下隐藏原始时间，例如将时间20150101 01:01:09按照5秒钟粒度向下取整得到20150101 01:01:05；

c） 规整：将数据按照大小规整到预定义的多个档位，例如将客户资产按照规模分为高、中、低三 个级别，将客户资产数据用这三个级别代替。

2） **抑制技术。**通过隐藏数据中部分信息的方式来对原始数据的值进行转换，又称为隐藏技术，具体的技术方法，具体的技术方法包括但不限于：

a） 掩码：用通用字符替换原始数据中的部分信息，例如将手机号码13500010001经过掩码得到135****0001，掩码后的数据长度与原始数据一样。

3） **扰乱技术。**通过加入噪声的方式对原始数据进行干扰，以实现对原始数据的扭曲、改变，扰乱后的数据仍保留着原始数据的分布特征，具体的技术方法包括但不限于：

a） 加密：使用加密算法对原始数据进行加密，例如将编号12345加密为abcde；

b） 重排：将原始数据按照特定的规则进行重新排列，例如将序号12345重排为54321；

c） 替换：按照特定规则对原始数据进行替换，如统一将女性性别替换为F；

d） 重写：参考原数据的特征，重新生成数据。重写与整体替换较为类似，但替换后的数据与原始 数据通常存在特定规则的映射关系，而重写生成的数据与原始数据则一般不具有映射关系。例如对雇员工资，可使用在一定范围内随机生成的方式重新构造数据；

e） 均化：针对数值性的敏感数据，在保证脱敏后数据集总值或平均值与原数据集相同的情况下，改变数值的原始值；

f） 散列：即对原始数据取散列值，使用散列值来代替原始数据。

4） 有损技术。通过损失部分数据的方式来保护整个敏感数据集，适用于数据集的全部数据汇总后才构成敏感信息的场景，具体的技术方法包括但不限于：

a） 限制返回行数：仅仅返回可用数据集合中一定行数的数据，例如商品配方数据，只有在拿到所有配方数据后才具有意义，可在脱敏时仅返回一行数据；

b） 限制返回列数：仅仅返回可用数据集合中一定列数的数据，例如在查询人员基本信息时，对于某些敏感列，不包含在返回的数据集中。

数据脱敏的核心是实现数据可用性和安全性之间的平衡，既要考虑系统开销，满足业务系统的需求，又要兼顾最小可用原则，最大限度的敏感信息泄露。因此在实施过程中，也应该围绕这两个点进行规范。即首先需要对敏感数据进行识别和定义，其次基于使用者的职责以及业务范围判断他是否需要使用这些敏感数据，他用这些数据来做哪些事，然后基于这些判断来选择数据脱敏的方法和技术措施。例如开发人员需要用这些数据进行测试的，应满足能够保留数据属性特征，可以采用扰乱等脱敏方式。如果是要投到大屏做展示用的，则可以选择掩码方式隐藏部分敏感内容。企业应结合自身业务开展的情况，分类分析数据需要脱敏的场景，规范每种场景下数据脱敏的规则和流程。组织在确定好数据脱敏的场景和脱敏的规则并形成制度文件后，就可以选择配置相关的数据脱敏工具，统一在业务系统中部署，配合制度文件的落实。

- 标准参考：

——ISO&IEC 27038_2014《数字脱敏规范》

——DB52/T 1126-2016《政府数据 数据脱敏工作指南》

10.4.2 PA11 数据分析安全

10.4.2.1 过程域设定背景和目标

在大数据环境下，企业对多来源多类型数据集进行关联分析和深度挖掘，可以复原匿名化数据，进而能够识别特定个人，获取有价值的个人信息或敏感数据。本过程域的设定用于规范数据分析的行为，通过在数据分析过程采取适当的安全控制措施，防止数据挖掘、分析过程中有价值信息和个人隐私泄露的安全风险。

10.4.2.2 过程域标准要求解读

- 制度流程：

  ——制定数据分析过程中数据资源操作规范和实施指南，明确各种分析算法可获取的数据来源和授权使用范围，并明确相关的数据保护要求。

  ——建立对数据分析结果进行风险评估的机制，确保衍生数据不超过原始数据的授权范围和安全使用要求，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。

- 技术工具：

  ——具备对个人信息去标识化的处理工具，通过对个人信息的技术处理，使其在不借助额外信息的情况下，无法识别特定的个人。

  ——具备对个人身份信息、重要或敏感数据进行处理操作的日志记录工具，以便对分析的结果进行溯源，对分析的行为进行审核。

10.4.2.3 过程域充分定义级实施指南

数据分析是数据产生价值的关键，是为了提取有用信息和形成结论而对收集来的数据加以详细研究和概括总结的过程。数据分析的目的是把隐没在一大批看来杂乱无章的数据中的信息集中、萃取和提炼出来，以找出所研究对象的内在规律，在实际应用中，数据分析可帮助人们做出预测性的判断，以便采取适当的行动。本过程域的数据分析特指组织有目的收集数据、分析数据，使之成为对组织经营有帮助的信息内容，数据分析过程往往会获取一些对于组织来说较为敏感的数据，因此需要对分析的过程进行安全控制。

- 制度流程参考：

可从以下几方面来考虑数据安全分析制度规范：

1) 明确各种数据分析工具所用到的算法是什么，以及该算法如何具体使用数据，使用哪些数据，并对算法本身进行风险评估，以确定该算法输出的分析结果不会涉及到用户个人隐私和组织的敏感信息。
2) 明确哪些人员可以使用数据分析工具，开展哪些分析业务，根据最少够用原则，允许其获取完成业务所需的最少数据集。
3) 制定数据分析结果审核机制，规定数据分析的结果需经过二次评估后才允许导出，重点评估分析结果是否与使用者所申报的使用范围一致。
4) 对于分析算法的变更要重新进行风险评估，以确保算法的变更不会导致敏感信息和个人隐私的泄露。
5) 应在制度中规定数据分析者不能将分析结果数据用于授权范围外的其他业务。

- 技术工具参考：

在技术工具的选择上，对需要汇聚大量个人信息进行分析的业务场景，应选取具有个人信息去标识化的工具， 断开这些信息和个人信息主体的关联，确保数据集中后无法联系到个人主体。具体可参考《个人信息去标识化指南》附录A的内容，选择合适的个人去标识化技术工具。

其次数据分析工具应具备日志记录功能，记录完整的数据分析过程日志，并实时传输到日志集中平台，确保数据分析事件可被审计和追溯。

- 标准参考：

——GB／T 35274-2017《信息安全技术 大数据服务安全能力要求》6.4 节“数据处理”

10.4.3 PA12 数据正当使用

10.4.3.1 过程域设定背景和目标

大数据时代，数据的价值越来越高，容易导致组织内部合法人员被数据的价值吸引而违规、违法的获取、处理和泄露数据。该过程域的设立，通过建立数据使用过程中的相关责任和管控机制，保证数据的正当使用。

10.4.3.2 过程域标准要求解读

- 制度流程：

——制定整体的数据权限管理制度，基于国家相关的法律法规要求以及组织数据分类分级标准规范，建立不同类别和级别的数据访问授权规则和授权流程，明确谁申请、谁授权、谁审批、谁使用、谁监管，确保所有的数据使用过程都是经过授权和审批的。

——建立数据使用者安全责任制度，确保数据使用者在事先声明的使用目的和范围内使用受保护

的数据，并在使用过程中采取保护措施。

- 技术工具：

——具备统一的身份及访问管理平台，实现对数据访问人员的统一账号管理、统一认证、统一授权、统一审计，确保组织数据权限管理制度的有效执行。

——身份及访问管理平台应具备双因素认证，以及细粒度的授权能力。

10.4.3.3 过程域充分定义级实施指南

- 制度流程参考：

在组织的数据授权管理制度上，应具备以下几点要求：

1） 明确授权审批的整个流程，关键节点的人员职责；

2） 如需使用个人信息，必须取得个人信息主体的明示同意；

3） 数据授权过程应遵循最少够用原则，即给与使用者完成业务处理活动的最少数据集；

4） 定期审核当前的数据资源访问权限是否合理

5） 违规处罚的制度和惩罚措施

- 技术工具参考：

数据权限管理平台可参考业界成熟的IAM系统，同时可部署日志审计类产品，集中收集数据使用过程中的日志，进行行为分析和操作溯源，以备潜在违约使用者责任的识别和追责。

- 标准参考：

——GB／T 35274-2017《信息安全技术 大数据服务安全能力要求》6.4 节“数据处理”

10.4.4 PA13 数据处理环境安全

10.4.4.1 过程域设定背景和目标

数据处理的安全是指如何有效的防止数据在录入、处理、统计或打印中由于硬件故障、断电、死机、人为的误操作、程序缺陷、病毒或黑客等造成的数据库损坏或数据丢失现象，某些敏感或保密的数据可能不具备资格的人员或操作员阅读，而造成数据泄密等后果。本过程域设定用于保护数据在处理过程中不被损坏、丢失或窃取，建立数据处理的环境保护机制，保障数据处理过程中有完整的安全管理和技术支持。

10.4.4.2 过程域具体标准要求解读

该过程域要求组织机构采用统一的数据计算、开发平台，确保数据在处理过程中的安全性。为数据处理环境建立和采用的技术和管理的安全保护，保护计算机硬件、软件和数据不因偶然和恶意的原因遭到破坏、更改和泄露。

- 制度流程：

——建立统一的数据计算、开发平台，在平台上实现统一的安全管理措施。

——在平台的设计、开发和运维阶段都需要相应的安全技术控制手段，来实现对平台全生命周期的风险管理。

- 技术工具：

——需要同步和联动数据处理平台和数据权限管理平台的权限设置，确保用户在使用数据处理平台前已经获得数据权限管理平台的授权。

——针对大数据处理平台多租户的特性，需要对租户之间进行逻辑隔离，确保该租户在平台中的数据、系统功能、会话、调度和运营环境等资源独立运行。

——要在数据处理的同时设置日志管理工具，针对用户的数据处理操作进行记录和审计，为后续的事件追溯提供依据。

——基于云平台的数据处理平台，还要通过伪装风险监测、恶意篡改监测技术来保障各个工作环节的功能稳定。

10.4.4.3 过程域充分定义级实施指南

通过数据处理平台进行统一管理，采取严格的访问控制、监控审计和职责分离来确保数据处理安全。

- **网络访问控制**

1.网络隔离

平台对生产数据网络与非生产数据网络进行安全隔离，从非生产网络不能直接访问生产网络的任何服务器和网络设备，也就不能从非生产网络发起对生产网络的攻击。

租户之间网络及设备进行安全隔离，内部无法直接访问租户间的服务器和网络设备。

2.堡垒机

为了平衡效率和安全性，在运维入口部署了堡垒机，只允许办公网的运维人员可以快速通过堡垒机进入数据处理平台进行运维管理。

运维人员登录堡垒机时使用域账号密码加动态口令方式进行双因素认证。堡垒机使用高强度加密算法保障运维通道数据传输的机密性和完整性。

3.远程运维

不在公司的员工提供远程运维通道。运维人员预先申请VPN接入公司办公网之后访问堡垒机的权限。VPN拨入公司办公网络的接入区时使用域账号密码加动态口令方式进行双因素认证。再从办公网接入区访问堡垒机。VPN使用高强度加密算法保障运维通道数据传输的机密性和完整性。

- **账号管理和身份认证**

数据处理平台使用统一的账号管理和身份认证系统。每个员工存在唯一的账号。账号的唯一性保证了审计时可以定位到个人。集中下发密码策略，强制要求员工设置符合密码长度、复杂度要求的密码，并定期修改密码。账号管理和身份认证的集中，使得其他信息系统不需要管理身份信息，也不需要保存多余的

账号密码，从而降低了应用的复杂性，提高了账号的安全性。账号管理与授权管理分离还可以防止私建账号越权操作行为。

- **授权**

数据权限管理平台统一的权限申请和授权管理系统。基于员工工作岗位和角色，遵循最小权限和职责分离原则，授予员工有限的资源访问权限。员工根据工作需要通过权限管理平台申请VPN访问权限、堡垒机访问权限、管控平台以及生产系统访问权限，经主管、数据或系统所有者、安全管理员以及相关部门审批后，进行授权。

运维和审计实施职责分离，由安全管理部门负责审计。数据库管理员和系统管理员由不同的人担任。适当的职责分离能有效防止权限滥用和审计失效。

- **监控**

使用自动化监控系统对云平台网络设备、服务器、数据库、应用集群以及核心业务进行全面实时监控。监控系统展示云平台关键运营指标，并可配置告警阈值，当关键运营指标超过设置的告警阈值时，自动通知运维和管理人员。

- **审计**

员工对数据处理平台的所有运维操作必须且只能通过堡垒机进行。所有操作过程完整记录下来实时传输到集中日志平台。堡垒机对于Linux操作记录所有命令行，对于Windows操作录屏并记录键盘操作。

员工需要通过数据处理平台唯一的数据权限管理账号对数据进行处理、访问和使用，所有的操作及过程都会完整的记录下来实时传输到集中日志平台。

- 标准参考：

——GB／T 35274-2017《信息安全技术 大数据服务安全能力要求》6.4 节“数据处理”

10.5 数据交换安全

10.5.1 PA14 数据导入导出安全

10.5.1.1 过程域设定背景和目标

数据导入导出广泛存在于数据交换过程中，通过数据导入导出，数据被批量化流转，加速数据应用价值的体现。如果没有安全保障措施，非法人员可能通过非法技术手段导出非授权数据，导入恶意数据等，带来数据篡改和数据泄漏的重大事故，由于一般数据导入导出的数据量都很大，因此相关安全风险和安全危害也会被乘倍放大。在本过程域中，需要采用有效的制度和工具控制数据导入导出的安全风险。

10.5.1.2 过程域具体标准要求解读

- 制度流程：

数据导入导出安全保障的制度流程，应当首先建立数据导入导出安全制度规范，规范导入导出安全策略，然后规范相应的权限审批和授权流程，同时也需要建立数据导出介质的安全技术标准，保障导出介质的合法合规使用。

—— 建立数据导入导出的安全制度规范，对各业务中的导入导出场景进行了充分合理的安全需求分析，能够依据不同的场景，并基于数据分类分级要求定义数据导入导出安全策略，例如访问控制策略、不一致处理策略、流程控制策略、审计策略、日志管理策略等。

—— 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。

—— 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。

- 技术工具：

—— 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。

—— 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。

—— 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。

10.5.1.3 过程域充分定义级实施指南

- 制度流程参考：

案例：《XX集团数据导入导出安全管理规范》关键内容：

- 总体说明（目的）
- 导入导出场景
- 安全要求（包含工具、介质等）
- 岗位职责说明
- 导入导出工具
- 导入导出流程

- 技术工具参考：

建立独立的数据导入导出安全控制平台，或者与在统一的用户认证平台、权限管理平台，流程审批平台，监控审计平台中支持数据导入导出的安全控制功能。具体核心功能如下：

- 数据导入导出权限管理：权限管理设置数据目录或者数据资产的导入导出访问权限，包括但不限于访问范围、访问人员分组，访问时间，访问频次等。
- 数据导入导出审批人管理：支持设置数据访问权限的审核人和审批人，支持设置多级审批人。
- 数据导入导出工作流管理：建立数据导入导出工作流机制，对于数据导入导出进行审核和授权。数据操作人员通过工作流申请数据导入导出权限，通过审核和授权后，遵循数据导入导出权限管理的数据导入导出才能被允许执行。
- 数据导入导出身份认证：对于数据导入导出的操作人员进行多重身份鉴定，包括双因子认证等，确保操作人员身份的合法性。
- 数据导入导出完整性验证：为了防止数据在导入导出过程中被篡改，数据导入导出增加完整性保护，在导入导出完成后需要进行完整性效验，确保数据合法性。
- 数据导入导出日志审计和风险控制：对于数据导入导出的所有操作和行为进行日志记录，并对高危行为进行风险识别。在安全事件发生后，能通过安全日志快速进行回溯分析。

- 标准参考：

  ——GB／T 35274-2017《信息安全技术 大数据服务安全能力要求》6.5 节“数据交换”

10.5.2 PA15 数据共享安全

10.5.2.1 过程域设定背景和目标

在数据交换环节中，业务系统将数据共享给外部组织机构，或者以合作方式与第三方合作伙伴交换数据，数据在共享后释放更大价值，并支撑数据业务的深入开展。

数据共享过程中面临巨大安全风险，数据本身存在敏感性，共享保护措施不当将带来敏感数据和重要数据的泄漏。因此，在本过程域中，需要采取安全保护措施保障数据共享后数据的完整性、保密性和可用性，防止数据丢失、篡改、假冒和泄露。

10.5.2.2 过程域具体标准要求解读

- 制度流程：

  —— 组织机构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的相关职责和权限，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

具有对共享数据足够的保护能力，从而保障数据共享安全策略的有效性。

—— 组织机构在原则要求的基础上根据组织机构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，以满足数据共享业务场景需求范围，提高数据共享效率，指导具体数据共享场景的风险把控。

—— 组织机构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。

—— 组织机构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。

—— 针对数据交换过程中涉及到第三方的数据交换加工平台的场景，组织机构制定了明确的安全评估的要求和流程，以保证该数据交换加工平台已符合组织机构对数据交换过程中的数据安全要求。

- 技术工具：

—— 组织机构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，确保没有超出数据服务提供者的数据所有权和授权使用范围。

—— 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。

—— 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。

—— 建立数据共享审计和审计日志管理的工具，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。

10.5.2.3 过程域充分定义级实施指南

- 制度流程参考：

案例暂无

- 技术工具参考：

建立数据共享安全管理平台，或者与在统一的用户认证平台、权限管理平台，流程审批平台，监控审计平台中支持数据共享的安全控制功能，并结合数据脱敏等数据保护技术保护敏感数据。数据共享安全工具对于共享资源的数据目录或者数据资产进行安全管理，确保共享数据的规范性和安全性，主要核心功能如下：

- 数据共享目录审核确认工作流：建立了数据共享审核流程确认工作流，对共享数据的目录进行审核，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。

- 数据共享权限审批人管理：支持设置数据共享权限的审核人和审批人，支持设置多级审批人。
- 敏感数据保护：如果共享数据中包含重要数据、个人隐私数据等敏感数据，支持对于共享数据进行加密、脱敏等数据保护工具处理后再共享，有效保护敏感数据。
- 数据安全交换：如果共享数据中包含重要数据、个人隐私数据等敏感数据，因为数据有效性不能对数据进行匿名化处理，需要支持数据进行安全交换，做到数据“可用不可见”。在用户不直接接触原始数据的情况下，依然可以使用共享数据进行计算分析得到结果。
- 数据共享日志审计和风险控制：对于数据共享的所有操作和行为进行日志记录，并对高危行为进行风险识别。在安全事件发生后，能通过安全日志快速进行回溯分析。

10.5.3 PA16 数据发布安全

10.5.3.1 过程域设定背景和目标

数据发布是指组织内部数据通过各种途径向外部组织公开的一个过程，如数据开放、企业宣传、网站内容发布、社交媒体发布、PPT资料对外宣讲等，防止出现违规对外披露造成对组织的名誉损害，资产损失等不良影响事件发生。数据发布安全保障发布内容的真实性、正确性、实效性和准确性。

10.5.3.2 过程域具体标准要求解读

- 制度流程：

  ——数据发布管理制度是建立在数据分类分级的基础上，针对可对外公开和发布的数据进行发布前、发布中、发布后安全管理过程，包括发布前的数据内容、发布范围等审核，发布中对定期审查，以及发布后可能出现不良影响的应急处理机制；

- 技术工具：

  ——建立数据资源公开数据库、数据发布平台和应急处理平台，实现公共数据资源登记、数据资源发布和数据发布事件应急响应功能。

  ——建立数据资源公开数据库，实现公开数据资源登记、发布用户注册、发布数据和发布组件验证互认机制等功能

  ——建立数据发布平台，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功能。

  ——建立数据资源公开事件应急处理平台，对于各类安全事件进行有效应急处置。

10.5.3.3 过程域充分定义级实施指南

- 管理流程参考：

案例：《XX组织数据发布安全管理制度》关键内容：

- 明确数据发布的内容和适用范围
- 数据发布相关人员职责和分工
- 数据发布的管理和审核流程
- 数据发布事件应急处理流程
- 数据发布的监管要求

- 技术工具参考：
  - 浙江省政务公开服务平台：http://data.zjzwfw.gov.cn
  - 深圳数据开放平台：http://opendata.sz.gov.cn

- 标准参考：

——GB／T 35274-2017《信息安全技术 大数据服务安全能力要求》6.5.4 节“数据发布安全”

10.5.4 PA17 数据接口安全

10.5.4.1 过程域设定背景和目标

在数据共享交换中，通过API数据接口获取数据是常见的方式。如果对于数据接口进行攻击，将导致数据通过数据接口泄漏，相关可能存在的攻击方式如下：

- 伪装攻击。例如：第三方有意或恶意的调用。
- 篡改攻击。例如：请求头/查询字符串/内容 在传输过程被修改。
- 重放攻击。例如：请求被截获，稍后被重放或多次重放。
- 数据信息监听。例如：截获用户登录请求，截获到账号、密码等敏感信息。

通过建立组织机构的对外数据接口安全管理机制，防范组织机构在数据接口调用过程中的安全风险。

10.5.4.2 过程域具体标准要求解读

- **制度流程：**

——从接口身份认证、防重放、数据防篡改、防泄漏角度制定数据接口的安全限制和安全控制措施；

——通过制定数据接口安全规范，明确数据接口设计要求；

——通过合作协议明确数据接口调用的目的、用途等内容，对接口调用方的行为进行合法性和正当性约束；

- **技术工具：**

——通过 HTTPS 协议构建的可进行加密传输、身份认证的网络协议，解决信任主机和通讯过程中的数据泄密和数据被篡改的问题；

——通过公私钥签名或加密机制提供细粒度的身份认证和访问、权限控制，满足数据防篡改和数据防泄漏要求；

——实现时间戳超时机制，过期失效，满足接口防重放要求；

——通过接口参数过滤、限制，防止接口特殊参数注入引发的安全问题；

——通过接口调用日志的收集、处理、分析，从接口画像、IP 画像、用户画像等维度进行接口调用行为分析，并且产出异常事件通过告警机制进行实时通知；

10.5.4.3 过程域充分定义级实施指南

- **技术工具：**

案例：《XX接口开发规范》关键内容：

- 统一接入URL：https://open-api.***.***.com
- 接入方式：支持http的get或post方式，具体参看接口
- 系统编码： UTF-8
- 接入认证：
- appkey:应用key
- secretkey:应用密钥
- 签名机制：

所有的 URL 调用里需要携带如下四个参数：

表 7：URL 调用携带的参数

字段	描述	说明和示例
appkey	密钥	Xxxx
timestamp	unix 时间戳	精确到秒,如：1482595200
v	调用接口 api 版本	目前 API 版本，初始接口版本都是 1.0
sign	签名	SHA256(appkey=xxx&timestamp=xxx&v=xxx&appsecret=xxx),结果采用小写方式，如:

		ff3f4036a1164d1ddbad5b3edf9022addb3e1961a54a922708a6c1ffc49e5489

- 返回结果：

调用结果都以 json 形式返回，其中如下参数用于判断调用状态：

表 8：判断调用状态的参数

字段	描述	说明和示例
success	布尔型，调用结果状态	成功时候为:true　失败为:false
message	字符串，调用描述	如"successful"
code	整型，状态码	正常为 200，服务器错误时候可能为其他，可以忽略，只看 success 状态
data	结构体，数据内容	由 items（数组）和 total 组成

- 标准参考：

——GB／T 32908-2016《非结构化数据访问接口规范》

10.6　数据销毁安全

10.6.1　PA18 数据销毁处置

10.6.1.1　过程域设定背景和目标

数据销毁有两个目的，一是合规要求，国家法律法规要求重要数据不被泄露；另外就是组织本身的业务发展或管理需要。计算机或设备在弃置、转售或捐赠前必须将其所有数据彻底删除，无法复原，以免造成信息泄露，尤其是国家涉密数据。有许多政府机关、民营企业，受限于法律规范，必须确保许多数据的机密。另外，存储大量、过时的数据不仅消耗硬盘存储空间，而且还会拖慢计算机系统运行速度，甚至可能增加被黑客攻击的风险。

日常工作过程中，用户往往采取删除、硬盘格式化、文件粉碎等方法销毁数据，这样的做法非常不安全。以下是对这几种普通的“数据销毁”方式安全性分析。

- 删除文件：删除操作并不能真正擦除磁盘数据区信息。用户的删除命令只是将文件目录项做了一个删除标记，数据区并没有任何改变。一些数据恢复工具正是利用了这点，绕过文件分配表，直接读取数据区，恢复被删除的文件。因此，这种数据销毁方法最不安全。
- 格式化硬盘：“格式化”又分为高级格式化、低级格式化、快速格式化等多种类型。多数情况下，普通用户采用的格式化不会影响硬盘上的数据区。格式化仅仅是为操作系统创建一个全新的空文件索引。将所有扇区标记为“未使用”状态，让操作系统认为硬盘上没有文件。因此，采用数据恢复工具软件也可以恢复格式化后数据区中的数据。
- 使用文件粉碎软件：为满足用户彻底删除数据的需要，网上出现了很多所谓的文件粉碎软件，一些防病毒软件也增加了文件粉碎功能，不过这些软件大多没有通过专门机构的认证，可信度和安全性都值得怀疑，用于处理一般的私人数据还可以，但不能用于处理带有密级的数据。

基于以上考虑，组织要根据不同要求和需要采取不同的数据销毁策略和技术手段，已实现对数据的有效销毁，防止因对存储介质中的数据内容进行恶意恢复而导致的数据泄漏风险。

10.6.1.2 过程域具体标准要求解读

- 制度流程：

——数据销毁场景：什么场景下需要做数据销毁，结合业务和数据重要性需要；

——数据销毁方法：根据数据分类和分级，已经场景需要，确定销毁手段和方法，包括物理销毁和逻辑销毁，比如覆写法、消磁法、捣碎法/剪碎法、焚毁法。

——数据销审批流程：主要针对重要数据，销毁的合理性和必要性评估；

——数据销毁监督流程：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；

——数据销毁指南：针对不同介质所存储数据的具体销毁方法和技术，比如针对网络存储、闪存、硬盘、磁带、光盘等存储数据所应采用的数据销毁的方法和技术，建立网络数据分布式存储的销毁策略与机制。

- 技术工具：

——数据销毁的技术工具要多样化，保证满足各种类型的数据销毁，比如：针对网络存储数据、针对闪存、硬盘、磁带、光盘等存储数据；保以不可逆方式销毁数据及其副本内容

10.6.1.3 过程域充分定义级实施指南

两种清除数据需求：

- 清除（Clearing）：在重新使用媒体之前，彻底删除媒体中数据的程序，且在清除媒体中数据之前，作业环境可提供可接受的保护等级。举例来说，所有内部存储器、缓冲区或其他可重复使用

的内存，都必须执行清除，以有效杜绝读取先前储存的数据。

- 销毁（Sanitization）：在重新使用媒体之前，彻底删除媒体中数据的程序，且在销毁媒体中数据之前，作业环境无法提供可接受的保护等级。例如，当信息系统资源从保密信息管制下释出、或释出到较低的保密层级使用前，都必须执行数据销毁。

执行数据清除或销毁的方法：

无论旧版DOD 5220.22-M或后来的DSS C&SM，均分别针对磁带、磁盘、光盘、内存等四种类型的储存媒体，以及同样会暂存数据的打印机，提出了17种删除数据的方式。而这些方式中，有15种适用于储存媒体，又可分为消磁、覆写、紫外线删除与物理摧毁等基本方式：

- 消磁：可适用于磁带与磁盘，分为 Type I 与 Type II 两种层次的消磁，对应于 Type I、II 两种类型的磁带。
- 使用消磁要特别注意，首先某些磁带与抽取式硬盘（如 LTO 磁带与 Zip 盘片）内含有出厂时预录的讯息，若强制执行消磁而使这些讯息消失，这些媒体将无法再被重复使用。其次是美国国防部的 Type I/II 消磁标准已太过老旧，要对当前的磁带实施消磁，最少也得使用消磁能力 2500～30000e 的消磁机；若要消磁硬盘，则需要的消磁能力将达到 4000～5000 Oe 以上。
- 覆写：包括几种不同方法，如把所有储存寻址位置都填入单一字符；所有寻址位置都填入单一字符后，再随机填入字符；以随机方式覆写所有寻址位置，所有位置都填入二进制 0 值、所有位置都填入二进制 1 值；或事先透过制造商提供的工具删除芯片中数据，然后把所有寻址位置都填入单一字符，然后重复三次等等。
- 紫外线照射删除与移除电源：紫外线照射删除适用于 EPROM，移除包括电池在内的所有电源则适用于 DRAM、NOVRAM 与 SRAM。

- 技术工具参考：

选购消磁机时，必须考虑的产品规格要素有几点：

——要进行数据清除或销毁的储存媒体磁场强度。针对高磁场强度的媒体，必须选择更强力的消磁机。

——需执行数据清除或销毁的储存媒体数量，如果数量不多，可选购手动式的桌上型单卷或多卷装消磁机；如果每月都要销毁上百台硬盘或磁带中的数据，则需选择自动化、有输送带设备的大型消磁机。

——确认是否有遵循官方认证的需求。比如通过国家保密局认证或军 C+级认证等，若企业为美国或其他西方政府机构的合约商、或业务上牵涉到必须遵循某些美国数据安全管理法令，则需使用通过特定认证许可的消磁机机型。

- 标准参考：

——GB／T 35274-2017《信息安全技术 大数据服务安全能力要求》6.6 节“数据销毁”

——美国国防部 DoD 5220.22-M 国家工业安全计划操作手册（National Industrial Security Program Operating Manual，NISPOM）（95 年 1 月发布，97 年 7 月修正）第 8 章第 3 节的一部分，提供了一个清除与销毁数据方法的参考矩阵表。

——美国国防部所属国防保安处（Defense Security Service，DSS）提供数据清除与销毁方法参考矩阵表（Clearing and Sanitization Matrix，C&SM）。

——GA/T 1143-2014《信息安全技术 数据销毁软件产品安全技术要求》

10.6.2 PA19 介质销毁处置

10.6.2.1 过程域设定背景和目标

这部分主要是考虑到存储介质需要被替换掉或淘汰掉不再使用，对存储介质进行彻底的物理销毁，保证数据无法复原，以免造成信息泄露，尤其是国家涉密数据。

10.6.2.2 过程域具体标准要求解读

- 制度流程：

——介质销毁方法介绍，如捣碎法/剪碎法、焚毁法。

——介质销毁审批流程：主要针对重要数据，销毁的合理性和必要性评估；

——数据销毁监督流程：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；

——数据销毁指南：针对不同介质所存储数据的具体销毁方法和技术，比如针对网络存储、闪存、硬盘、磁带、光盘等存储数据所应采用的数据销毁的方法和技术，建立网络数据分布式存储的销毁策略与机制。

10.6.2.3 过程域充分定义级实施指南

- 技术工具参考：

——捣碎法/剪碎法：破坏实体的储存媒体，让数据无法被系统读出，也是确保数据机密性与安全性的方法之一。采用实体捣碎的方式，让数据储存媒体残骸，无法被有心人士利用。比如，某些大型企业会将储存数据的光盘片，进行大型机器捣碎、绞碎的动作。

——焚毁法：几乎每一个需要汰换的储存媒体最终都会面临，藉由焚毁让数据真正化为灰烬，永久不复存在。有的企业甚至要求主管部门领导必须亲临现场监督旧数据焚毁状况与进度，落

实数据保全的最后一步。

- 标准参考：

——BMB21-2007《涉及国家秘密的载体销毁与信息消除安全保密要求》

——GB／T 35274-2017《信息安全技术 大数据服务安全能力要求》6.6 节“数据销毁”

10.7 通用安全

10.7.1 PA20 数据安全策略规划

10.7.1.1 过程域设定背景和目标

基于组织业务发展需要，对当前组织面临的数据安全风险现状进行梳理并制定整体的规划，着眼于未来，是需要高管参与讨论和制定的。数据安全工作不是某个业务或部门的单方面的事，需要整个组织所有部门都参与进来，要平衡与业务发展的冲突，自上而下的推动，才可能保证落到实处和效果。

10.7.1.2 过程域具体标准要求解读

- 制度流程：

——数据安全策略是顶层的，要从组织级层面通盘考虑，所以需要组织的高管参与共同制定；既不能对当前业务发展有严重影响，也要考虑到业务长远发展需要，所以需要高层讨论商定取得合理的平衡；

——数据安全方针和策略，需明确数据对组织的价值和意义，应该以数据为核心围绕数据做工作，而不是其他诸如信息系统或研发技术等；

——策略规划的编写、评审、发布如果没有流程规范，容易导致组织内各业务部门获取不到最新版本，或者理解偏差，所以需要统一的发布窗口或路径，以及解读和宣贯，以确保策略的有效性和及时性；

- 技术工具：

——运营管理技术工具，是为了方便方针策略的发布有统一和唯一的官方渠道，保证版本内容最新最准准确，且在组织内传达和推广高效，更便于策略规范的落地推进。

10.7.1.3 过程域充分定义级实施指南

- **制度流程参考：**

主要有两份输出：数据安全方针政策和数据安全策略规划，及其编写、评审和发布等方面。

- 方针政策：是对组织级数据安全管理的基本原则和办法，可以结合数据安全总纲从目标、

原则、监管合规、数据生命周期、数据资产和分类分级定义，及相关违规处罚等方面进行描述；

- 策略规划：需要周期性地输出数据安全能力战略规划，比如半年度/年度/三年/五年等；

另外，数据安全策略的编写、评审、发布及更新，要明确到具体责任团队和责任人，可以由数据安全管理团队牵头编写，并由高管组成的数据管理委员会评审和批准发布。

案例参考：

案例1：《XXX公司信息安全管理方针和策略》关键内容：

- 信息安全管理目标
- 内部环境
- 外部环境
- 信息安全管理体系
- 领导力和管理承诺
- 应对风险和机会措施

案例2：《xxx公司数据安全总体规范》关键内容：

- 数据安全管理目标
- 数据安全基本原则
- 数据安全监管合规
- 数据生命周期安全管理
- 数据资产和系统资产
- 数据分类和分级
- 数据安全违规处分

- **技术工具参考：**
  - 建立一个网站平台即可，也可以考虑在内部OA系统有专门板块向组织全体员工发布数据安全策略规划，以及相应落地解读材料，以便于策略规范的落地推进。
- 标准参考

  ——GB／T 35274-2017《信息安全技术 大数据服务安全能力要求》5.1 节“策略与规程”

10.7.2 PA21 人力资源安全

10.7.2.1 过程域设定背景和目标

组织的数据安全策略、制度流程和技术工具等推进落地终究离不开人的执行，组织内不同部门、不等层级及不同来源的员工，在不同场景下直接和间接地接触数据资产，所以风险始终存在于人身上，需要联合人力资源部在员工的招聘/引进、入职、转岗/调岗、离职等各个环节设置相应的风险控制措施，以降低人本身问题导致的数据安全风险。

10.7.2.2 过程域具体标准要求解读

- 制度流程：

——数据安全在员工方面的风险，人力资源部要配合高管建立和优化组织级的数据安全管理部门和岗位设置，引进数据安全专业人才，并配合数据安全管理部门在人力资源管理过程关键环节推行数据安全管理措施，以及安全文化宣导和安全意识提升等；

——对组织内员工类型进行合理分类，比如正式员工、外包员工、试用期员工、实习生，其他兼职和外聘人员等，以及不同层级和职位，以方便数据安全策略在相不用类型及不同层级的员工之间进行风险控制；

——人力资源部需要制定不同类型员工激励和处罚的制度，并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。

- 技术工具：

——数据安全控制措施要和人力资源管理系统相结合，尽可能做到线上审批流程必须的审批或确认步骤；

——向组织全体员工公示的内容包括数据安全策略、数据安全管理制度、数据安全管理团队和业务部门负责人，以及数据安全违规处罚等。

10.7.2.3 过程域充分定义级实施指南

- 制度流程参考：

可以分别从以下各方面考虑人力资源的制度规范，

- 组织内各职能部门和岗位之间涉及数据安全相关工作的协作关系，运行配合要求。
- 招聘：员工候选人背景调查，根据法律法规、行业道德准则要求等方面进行；
- 培训：对新入职和在岗员工进行定期或不定期的数据安全制度和意识宣贯。
- 考核：根据不同层级和岗位的数据安全的考核或考评要求；
- 转岗：在职期间转岗的工作交接，权限回收及已落到办公终端本地的数据清理等；
- 离职：提出离职到正式离职期间工作交接，权限回收和已落到办公终端本地的数据清理等，离职后的竞业协议协商和签署等；

- 激励和处罚：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；

案例参考：

暂无

- 技术工具参考：

可以考虑两类主要工具，

- 人力资源管理系统，在招聘、入职、转岗/调岗、离职，以及培训考试和绩效考核等子系统或环节，将数据安全控制要求植入，作为必须的审批或确认步骤；
- 和数据安全策略公布一样，有独立网站或在内部 OA 系统设置专门板块，向组织全体员工发布数据安全策略、管理制度、数据安全管理团队及业务部门负责人等。

案例参考：

暂无

- 标准参考

——GB／T 35274-2017《信息安全技术 大数据服务安全能力要求》5.3 节“组织与人员管理”

10.7.3 PA22 合规管理

10.7.3.1 过程域设定背景和目标

合规管理是组织数据安全最基础的能力层面和底线，合规管理的目标是避免组织违反需要符合的国内外法律、行业监管指引、制度、规范，避免因不合规导致的风险。本过程域的设定，即要求建立数据安全合规文化和有效的合规风险预防、预警及监督机制。

10.7.3.2 过程域具体标准要求解读

- **制度流程：**

——依据法律法规及相关标准中对重要数据的保护要求，建立组织统一的符合性管理规范，该规范应包括但不限于个人信息保护、重要数据保护、跨境数据传输等方面的安全合规需求，并对相关方宣贯合规要求的内容，以保证组织整体合规意识的提升；

——建立一份当前组织需要遵照的外部合规要求清单，并实时跟踪外部合规要求的发布、预研，保持清单的更新；

——建立一套适用的数据安全合规监督检查标准和清单，用于指导常规检查、专项检查和事件驱动检查等，以确保符合相应的数据安全政策、标准及其他数据安全要求；

——建立一套适用的整改和考核规范，用于指导检查发现和整改情况的跟踪、报告管理、问题管理等。

- **技术工具：**

——建立法律、行业监管指引、外部制度、规范条款的统一电子合规平台，并将各类外部要求去重合并、分解转化为数据安全合规元要求，并据此和组织实际情况梳理出内部管理要求；

——建立一套检查跟踪系统，实现检查计划制定、检查实施、报告管理、问题跟踪等全过程的电子化管理，并将检查发现和整改情况纳入问题管理流程。

10.7.3.3 过程域充分定义级实施指南

参考案例：

某行业案例1：规章文档平台

在办公系统中，建立了规章文档平台，供员工查询和学习。通过该平台的建立：

- 统一来自所有金融风险管理系统的合规和风险信息，形成涵盖整个组织的风险视图；
- 供内部使用的可以根据关键字进行快速检索查询外部标准和要求；
- 统一的数据安全元要求，并形成外部标准和内部管理规范的对应关系，定期更新和查漏补缺，避免合规风险。

某行业案例2：法律、标准：

- 我国在2016年出台，2017年6月1日正式生效的网络安全法，全称《中华人民共和国网络安全法》；
- 欧盟在2015年出台，2018年5月正式生效的一般数据保护条例，全称为《General Data Protection Regulation》（简称 GDPR）；
- 我国在2018年正式出台，5月1日正式生效的GB/T 35273《信息安全技术 个人信息安全规范》；
- 2018年5月21日银保监会正式发布的《银行业金融机构数据治理指引》；
- 我国已经在制定即将颁布的《数据出境管理办法》、《重要数据管理办法》、《中华人民共和国密码法》等。

某行业案例3：合规监督检查

- 依据监管要求、外部标准、内部规范梳理出一套适用的检查标准，并进行全面覆盖的检查。通过识别，外部规范分解成3大类、27小类要求，去重合并后形成外规内规对应关系，也就是数据安全风险检查标准库；
- 制定全年检查计划，建立常规检查、专项检查、事件驱动检查相结合的方式，100%覆盖数据安全风险检查标准库；

- 专项检查围绕数据安全域，包括数据采集安全、数据传输安全、数据处理安全、数据交换安全以及通用安全域；
- 常规检查注重数据权限管理、数据对外数据等日常运营重点模块；
- 事件驱动检查一般在发生可用性事件、信息安全事件或重大违规违纪事件发生后进行。检查发现，全部纳入问题管理流程进行跟踪管理。通过问题跟踪机制，可以充分确保问题统一归口管理无遗漏，相关整改的方案可实施、进度有跟踪、实施有成效。

10.7.4 PA23 数据资产管理

10.7.4.1 过程域设定背景和目标

数据资产是组织拥有和控制的、能够给企业管理、应用服务和商业拓展带来价值的数据信息。只有洞悉数据资产重要程度与分布、使用对象与场景、授权与责任等，才能有效的实施数据资产风险管理和安全防护。一般而言，数据资产安全管理工作包含资产识别、资产重要度定级、资产变更管理与监测、资产风险管理等。

10.7.4.2 过程域具体标准要求解读

- **组织建设：**

——设置数据资产管理组织，按照统一的规章制度管理企业数据资源，各业务团队应配置具体人员负责本级业务范围内的数据资产管理工作。

- **制度流程：**

——实施数据资产全生命周期监督管理，各业务团队数据资产管理责任人应按照相关要求及时登记、更新和定期维护本级数据资源；

——建立数据资产目录（数据资产地图）并提供检索服务，数据表责任到人；

——建立数据资产变更管理审批流程，实时监控数据资产的上线、变更、转移、销毁等信息，并配置相适应的安全管控措施。

- **技术工具：**

——通过智能数据目录等技术工具辅助实现数据资产登记和分类工作。

10.7.4.3 过程域充分定义级实施指南

数据资产管理案例：数据资产管理平台

该组织的业务部门多、数据来源广、人员角色复杂、数据使用链路有待完善，通过统一的数据资产管理平台，全面掌握了数据分布、使用流向、人员访问等，有效提高了数据安全管理能力。

- 数据类目体系，依托企业数据知识图谱，对全量数据资产进行业务打标和类目挂载，从而构造出数据资产地图，实现数据资产可视化，全面把握及科学分析数据资产、帮助用户清晰查看及快速使用数据资产。
- 数据资产等级，根据数据被使用场景的重要程度，对数据资产划分等级。对不同等级的数据，给予不同等级的保障，包括但不限于：资源、监控、变更通知等。
- 全链路数据追踪，通过构建采集端-生产端-服务端全链路闭环，实现从数据采集、数据加工生产、数据服务到用户消费的全链路分析保障，包括数据质量、安全、时效性及稳定性保障。

- 标准参考

——GB／T 35274-2017《信息安全技术 大数据服务安全能力要求》5.2 节“数据与系统资产”

10.7.5 PA24 数据供应链安全

10.7.5.1 过程域设定背景和目标

数据供应链是数据生产及流通过程中，涉及将数据产品或服务提供给最终用户所形成的网链结构。数据供应链安全管理的核心是厘清各方权力责任边界，对各方数据交互行为进行合规管理，防范组织上下游的数据供应过程中的安全风险。

10.7.5.2 过程域具体标准要求解读

- **制度流程：**

——根据法律法规和企业规定，制定数据供应链安全管理的基本要求，包括数据供应链上下游的责任和义务、合同要件、数据交互审批和审计原则。

——通过协议方式，明确数据供应链上下游数据使用目的、使用方法、供应方式、保密约定等。

——对数据服务商的数据安全能力进行评估，并将评估结果应用于供应商选择、供应商审核等供应商管理过程中。

- **技术工具：**

——通过技术工具完整的记录数据供应链授权信息、流转对账信息、场景使用信息等元数据信息，实时监测和查询数据链路整体情况。通过日志分析等事后追踪分析手段，审计数据供应链上

下游合规遵循情况。

——基于数据供应记录，利用技术工具对数据供应链上下游相关方的开展数据处理合规性审核和分析。

10.7.5.3 过程域充分定义级实施指南

参考案例：

全链路数据追踪技术

全链路数据追踪是针对数据从哪里来、到哪里去，数据加工链路是什么，数据被哪些产品使用，一个产品的加工链路如何保障等企业数据管理痛点问题，提出的产品及技术应用体系。全链路数据追踪技术覆盖采集端、数据端、应用端、数据接口四个部分，能打通数据采集、生产、消费、到产品服务的整个生产链路，服务于数据治理、数据安全、数据ROI评估等数据管理各个方面。

- 标准参考

——GB／T 35274-2017《信息安全技术 大数据服务安全能力要求》5.5 节“供应链管理”

10.7.6 PA25 元数据管理

10.7.6.1 过程域设定背景和目标

元数据主要是描述数据属性的，或者描述信息资源或数据等对象的数据。同时元数据本身也是数据，因此可以用类似数据的方法在数据库中进行存储和获取，进行元数据管理目的在于：识别和评价数据资源，追踪数据资源在使用过程中的变化；实现简单高效地管理大量网络化数据；实现信息资源的有效发现、查找、一体化组织和对使用资源的有效管理。如果没有元数据，组织IT系统中收集和存储的所有数据都会失去意义，也就没有业务价值。

元数据根据本不同维度有不同分类，常见的按功能分为管理元数据、技术元数据和业务元数据。

管理元数据：面向管理人员，对管理相关信息的描述，如管理流程、人员职责、工作内容分配等；

技术元数据：面向技术人员，对数据结构和数据处理细节等方面的技术化描述，如数据库结构，数据集市定义，数据处理过程描述等；

业务元数据：面向业务分析人员的数据和处理规则业务化描述，比如业务规则、业务术语、指标口径和信息分类等。

DSMM对元数据及其管理的定义相对比较窄，主要是指技术元数据。

10.7.6.2 过程域具体标准要求解读

- 制度流程：

——元数据及数据字典定义；

——元数据统一编写要求，比如数据格式、数据域、字段类型、表结构等；

——元数据访问控制要求，比如数据管理角色及其授权；

——元数据的更新和变更管理要求；

——元数据变更和访问操作日志记录和审计要求；

- 技术工具：

——元数据管理平台将各个领域的元数据集中起来统一提供服务，在同一领域应“标准化”；在不同领域，应妥善解决不同格式的互操作问题；

——对元数据本身的访问需要进行身份验证和授权，根据不同角色合理需求开放，并记录操作日志以便于监控和审计。

10.7.6.3 过程域充分定义级实施指南

- 技术工具参考：

元数据管理系统参考示意：

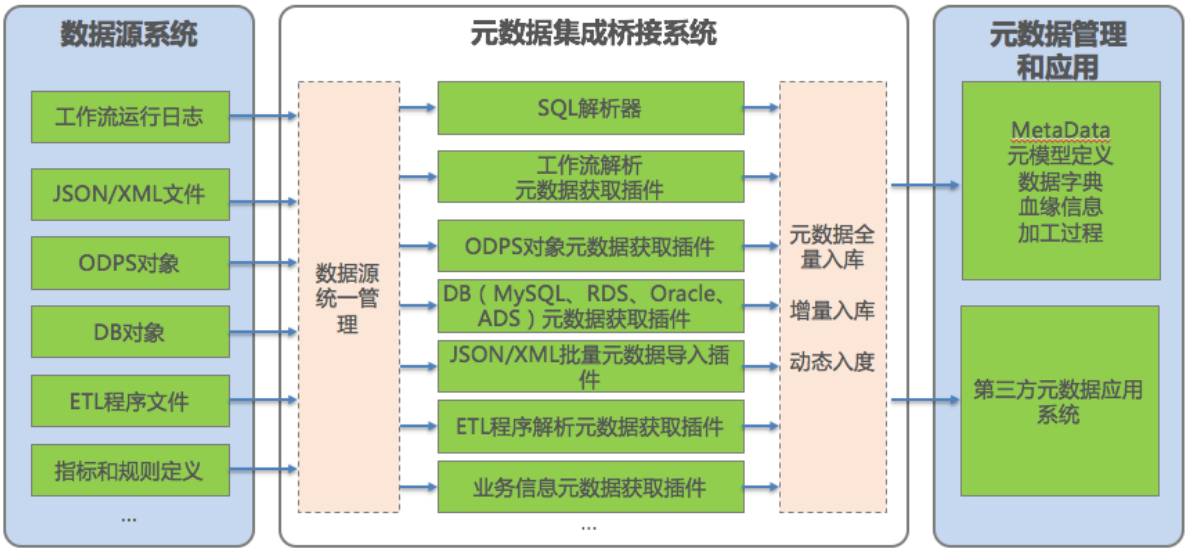

图9：元数据管理系统架构设计

- 相关实践参考：
  - **电信元数据管理** 64 页
  - **信息集成：元数据管理全景** 40 页
  - **浅谈电子政务元数据框架** 3 页

- **电子文件管理中的元数据** 21 页
- **中国移动元数据经营分析** 47 页

- 标准参考

  ——GB／T 35274-2017《信息安全技术 大数据服务安全能力要求》5.4 节“元数据安全”

10.7.7 PA26 数据终端安全

10.7.7.1 过程域设定背景和目标

终端是组织存储、处理、交换大量敏感数据的环境，一方面终端环境的复杂、多变、使用体验等都给终端数据安全管控的实践带来更多的挑战，另一方面在不同人员角色、复杂使用场景以及跨国、组织和系统的数据流动下，给组织数据安全带来更多的威胁。本过程域的设定，即要求建立相关管理和技术的终端保护措施来保证数据可用性和安全性的平衡。

10.7.7.2 过程域具体标准要求解读

- **制度流程：**

  ——建立终端安全管控规范，至少覆盖网络准入、补丁管理、安全基线、入侵防御、防病毒、数据防泄漏、软件管理、行为审计等方面。终端防护对象需根据组织实际资产展开，包括但不限于：各类办公终端、业务终端、移动终端等；

  ——建立员工终端行为管理规范，对用户在终端上的数据访问、处理、存储和交换行为进行明确要求、检测和管控，并明确责任和义务；

  ——建立或在原有信息安全事件处置中新增数据丢失、泄露、篡改类事件的应急预案、处置流程。

- **技术工具：**

  组织应整体考虑终端安全解决方案，包括终端环境的安全性和数据流动的安全管控：

  ——建立一套或兼容的终端管理平台，实现终端准入、资产管理、补丁管理、安全基线、入侵检测、防病毒、行为审计等方面的管控；

  ——建立数据防泄漏（DLP）平台，可根据组织业务场景需要构建基于加密或边界管控的思路来实现，辅助以水印、标记、协议管控、打印管控等手段，实现发现、加密/边界管控、审计的数据泄露闭环防护体系；

  ——建立移动安全管理平台，对移动端的数据存储、数据传输、数据分发、数据访问等行为进行管控。

10.7.7.3 过程域充分定义级实施指南

某行业案例1：某组织数据终端安全管理实践

1）制度建设

《终端安全管理办法》关键内容

- 总则，说明背景、管理对象和范围、名词解释等
- 组织管理，说明组织架构、管理职责等
- 终端管控，说明网络准入、补丁管理、安全基线、入侵防御、防病毒、数据防泄漏、软件管理、行为审计等方面的管理要求等
- 附则，约定罚则、制度生效日等

《员工桌面计算机使用安全管理手册》

- 总则，说明背景、管理对象和范围、名词解释等
- 总体原则，约定员工使用等
- 使用规范，包括系统使用、办公安全、病毒防护等方面；
- 附则，约定罚则、制度生效日等

2）数据防泄漏（DLP）平台

通过部署数据防泄漏（DLP）平台，以统一策略为基础，以敏感数据为保护对象，根据数据内容主动防护，对所有敏感数据的输入输出通道如邮件、U盘拷贝、打印、共享等多渠道进行监管，根据策略管控要求进行预警、提示、拦截、阻断、管控及告警等。平台实施后，4个高风险不复存在,完全被降低为中低风险。并通过强化敏感数据审核与管控机制以降低敏感数据外泄的发生几率及提升可追朔性。

某行业案例2：某组织桌面管理系统、杀毒软件、入侵检测系统

该组织在全国各地均有办公地点，在业务合作、系统开发测试和运维领域均有大量的合作外包，通过桌面管理系统、杀毒软件、入侵检测系统和桌面虚拟化实现了接入、设备、应用、数据等多维度管控，从而保证了数据的安全性：

1) 通过桌面管理系统实现办公终端网络准入控制，实现终端使用者身份验证、终端设备安全合规检查、使用者访问权限控制；

2) 通过桌面管理系统实现办公终端安全运维管理及审计,包括并不限于终端软、硬件信息搜集、设备拓扑发现、设备定位、本地安全管理、终端流量控制、补丁管理、软件分发、远程协助、非法外联、移动介质管理和操作审计等；
3) 通过主机入侵防御系统（HIPS），实时监控系统异常操作行为，第一时间发现和阻断入侵行为；
4) 通过统一管理的杀毒软件系统，实现覆盖全网的、可快速应急的防病毒体系；
5) 通过桌面虚拟化环境，对驻场的开发、测试、业务等外包场景进行集中管理、统一配置，杜绝私自的数据交换场景，避免了数据外泄的风险。

某行业案例3：移动安全管理平台

该组织的移动办公和业务开展场景应用广泛，办公类包括移动审批、移动OA、移动财务、移动HR等，业务开展场景包括移动展业、移动营销等。通过部署了MDM解决业务场景，部署MAM和MCM结合管控解决BYOD场景。基于以上举措解决了移动终端的数据安全风险。

1) 移动终端部署虚拟安全域，通过对应用增加一个“壳”文件，使应用运行在安全的容器内，监控管理应用的各种操作，实现安全防护；
2) 应用级安全接入隧道，仅允许指定的工作应用，例如邮箱、OA应用，通过应用级的VPN连接到组织内部网络，保证敏感数据在传输过程中的安全性；
3) 移动应用本地敏感数据根据需要进行转加密，并控制应用调用权限；
4) 移动应用截屏保护、录屏保护、应用限制分享。

- 标准参考

——GB／T 34977-2017《信息安全技术 移动智能终端数据存储安全技术要求与测试评价》
——GB/T 34978-2017 《信息安全技术 移动智能终端个人信息保护技术要求》
——GB/T 35278-2017 《信息安全技术 移动终端安全保护技术要求》

10.7.8 PA27 监控与审计

10.7.8.1 过程域设定背景和目标

数据安全保护的一个前提是知晓数据在组织内的安全状态，由于数据风险通过数据流动，贯穿多个系统和阶段中，形成了一个难以分割的风险整体，所以需要组织在数据生命周期各阶段（数据采集、数据传输、数据存储、数据处理、数据交换、数据销毁）开展安全监控和审计，以实现对数据安全风险的

防控。本过程域的设定，即要求建立相关的措施对非法采集、未授权访问、数据滥用、数据泄漏进行监控和审计。通过数据分析来支撑有效的安全、合规决策，从而降低数据安全风险。

10.7.8.2 过程域具体标准要求解读

- **制度流程：**

——建立或在数据安全整体策略中规范数据安全监控审计策略，覆盖数据采集、数据传输、数据存储、数据处理、数据交换、数据销毁各阶段的监控和审计；

——建立或在原有信息安全事件处置中新增监控审计出数据安全类事件的应急预案、处置流程。

- **技术工具：**

——建立数据安全监控审计平台，对组织内所有网络、系统、应用、数据平台等核心资产中的数据流动进行监控和审计，并进行风险识别与预警，以实现数据全生命周期各阶段的安全风险防控；

10.7.8.3 过程域充分定义级实施指南

某行业案例1：制度建设

《数据安全日常监控和审计管理办法》

- 总则，说明背景、管理对象和范围、名词解释等
- 组织管理，说明组织架构、管理职责等
- 管理内容，说明监控和审计的策略、对象、内容、监控要求、日志保存要求等；
- 异常流程处置，约定发生事件的处理流程和参考文件；
- 附则，约定罚则、制度生效日等

某行业案例2：数据安全监控审计平台

该组织的业务场景变化迅速、组织和人员角色复杂、数据输出管控有待完善，通过部署数据安全监控审计平台，对人员、业务、系统、合作伙伴进行全面布控，有效提高风险预警能力和风险运营能力。

工具平台：

- 数据采集，数据来源包括了员工基础数据、网络数据、终端数据、系统和应用数据等；日志数据获取的方式支持了JDBC、文本文件、Syslog、SNMP、API、Agent 、WINDOWS事件日志、Netflow等，日志内容支持文本、XML、JSON等，可针对特殊采集场景进行定制化；

- 数据整合，通过关联业务数据对采集的信息进行补全和数据的标准化定义，按照5W1H的方法进行数据统一，并根据行为共性，抽像出归一化的数据流动和行为主题域；
- 数据分析，以敏感数据为中心，建立多维度行为基线，利用机器学习算法和预定义规则找出严重偏离基线的异常行为，及时发现内部用户、合作伙伴窃取数据等违规行为；
- 平台运营，建立了发现、审计、处置和反馈的运营循环机制。
- 风险大图，可视化、可感知使得风险统一监控、统一告警、统一处置、统一恢复；

覆盖场景：

- 敏感数据外发
- u盘大量拷贝文件或大量打印文件
- 内网机器向外网大量发送文件
- 特定账号从FTP下载大量文件
- FTP账号被暴力破解后窃取数据
- 文件服务器下载大量文件
- 数据库dump操作（数据库拖库）
- 特定账号FTP下载文件后上传同名文件
- FTP账号被暴力破解后篡改数据
- 发现勒索软件
- 数据库危险操作或高危命令
- API滥用
- ……

- 标准参考

——GB/T 35274-2017 《信息安全技术 大数据服务安全能力要求》

——GB/T 22239-2008《信息安全技术 信息系统安全等级保护基本要求》

11 参考文献

[1] DB 52/T 1123—2016《政府数据 数据分类分级指南》

[2] 国发〔2016〕51 号《政务信息资源共享管理暂行办法》

[3] BMB21-2007《涉及国家秘密的载体销毁与信息消除安全保密要求》

[4] SJ 20901-2004《硬磁盘信息消除器通用规范》

[5] 美国国防部 DoD 5220.22-M 国家工业安全计划操作手册（National Industrial Security Program Operating Manual，NISPOM）

[6] 美国国防部所属国防保安处（Defense Security Service，DSS）提供数据清除与销毁方法参考矩阵表（Clearing and Sanitization Matrix，C&SM）

[7] GA/T 1143-2014《信息安全技术 数据销毁软件产品安全技术要求》

[8] BMB21-2007《涉及国家秘密的载体销毁与信息消除安全保密要求》

[9] GBT19710-2005《地理信息元数据》

[10] GB／T 35274-2017 《信息安全技术 大数据服务安全能力要求》

[11]GB／T 34977-2017《信息安全技术 移动智能终端数据存储安全技术要求与测试评价》

[12]YD/T 1699-2007《移动终端信息安全技术要求》

[13] GBT 22239-2008《信息安全技术 信息系统安全等级保护基本要求》