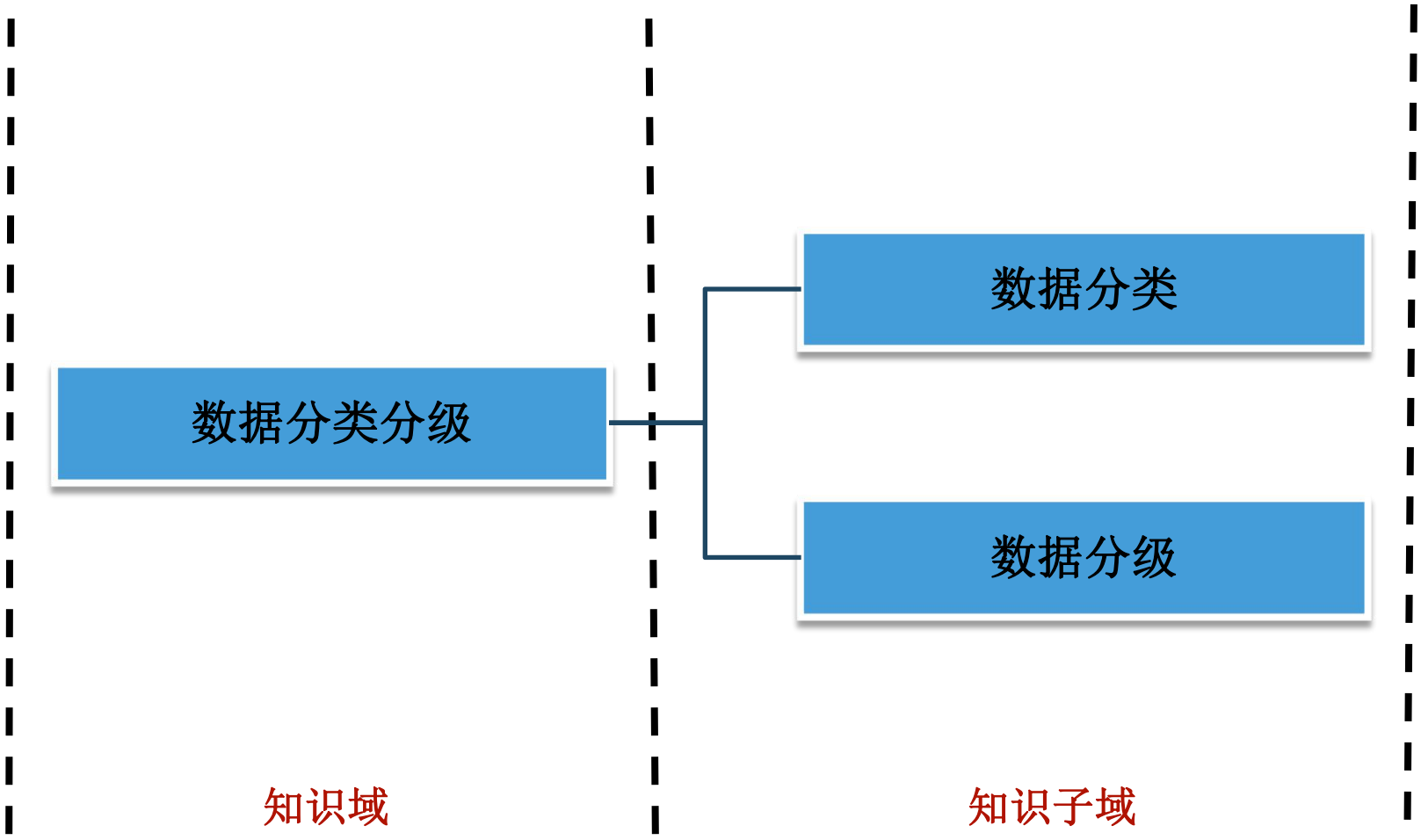
CISP-DSG 数据安全评估

版本：1.0

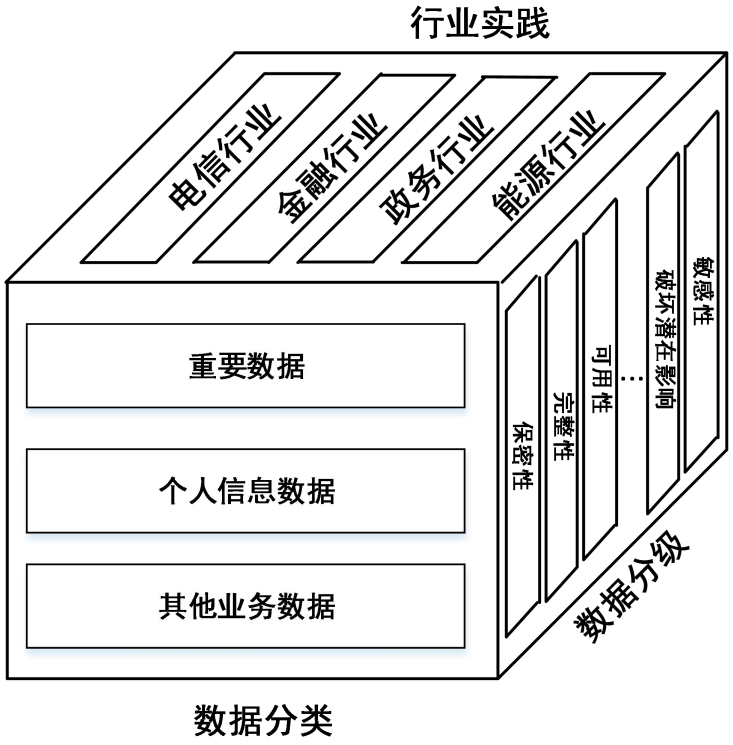
讲师姓名　　机构名称

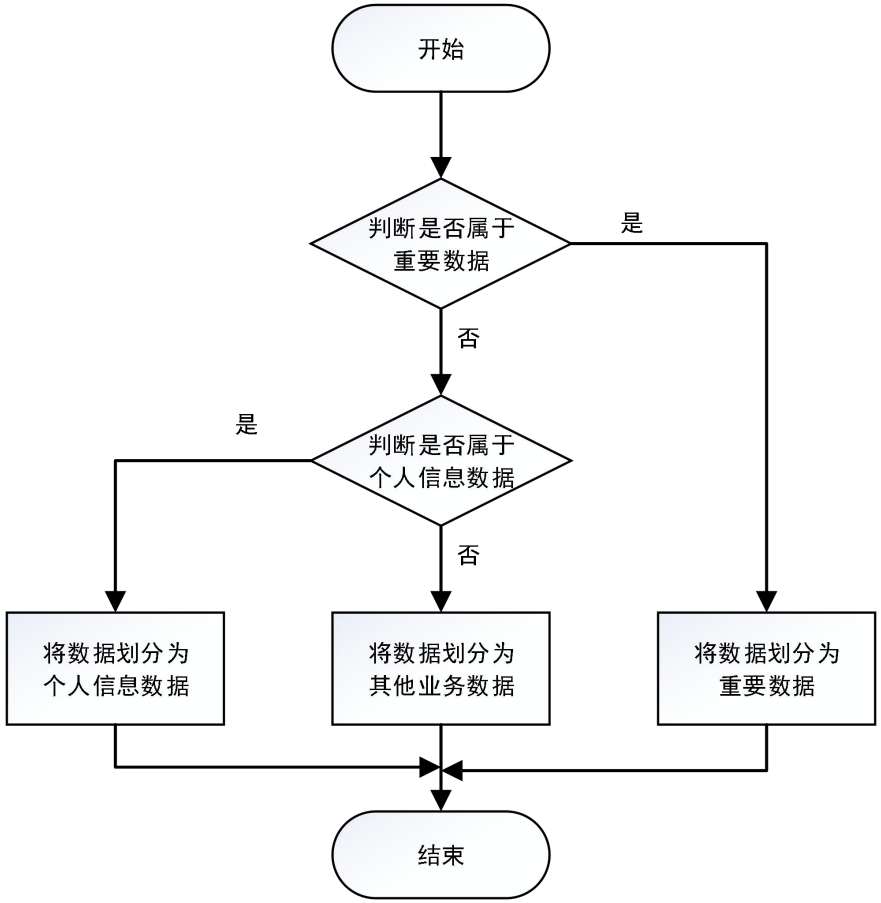
课程内容

- 知识体：数据安全评估



2.1 数据分类分级过程





摘自：《数据安全分类分级实施指南》研究报告

2.2 数据分类分级原则

2.3 数据分类方法

创建 → 存储 → 使用 → 共享 → 归档 → 销毁

- 确定所有者

数据所有者理解应该如何使用数据，可以合理的分类数据。

常见分类方法

- 监管合规
- 业务功能
- 功能单元
- 基于项目

2.4 数据分级方法

常见分级方法

敏感性	司法管辖	关键性
秘密	中国	重要
机密	美国	内部
绝密	欧盟	公开

2.5 我国的数据分类及分级

重要数据

- 危害国家安全
- 公共利益生命财产安全
- 危害国家关键基础设施
- 扰乱市场秩序
- 可推论出国家秘密

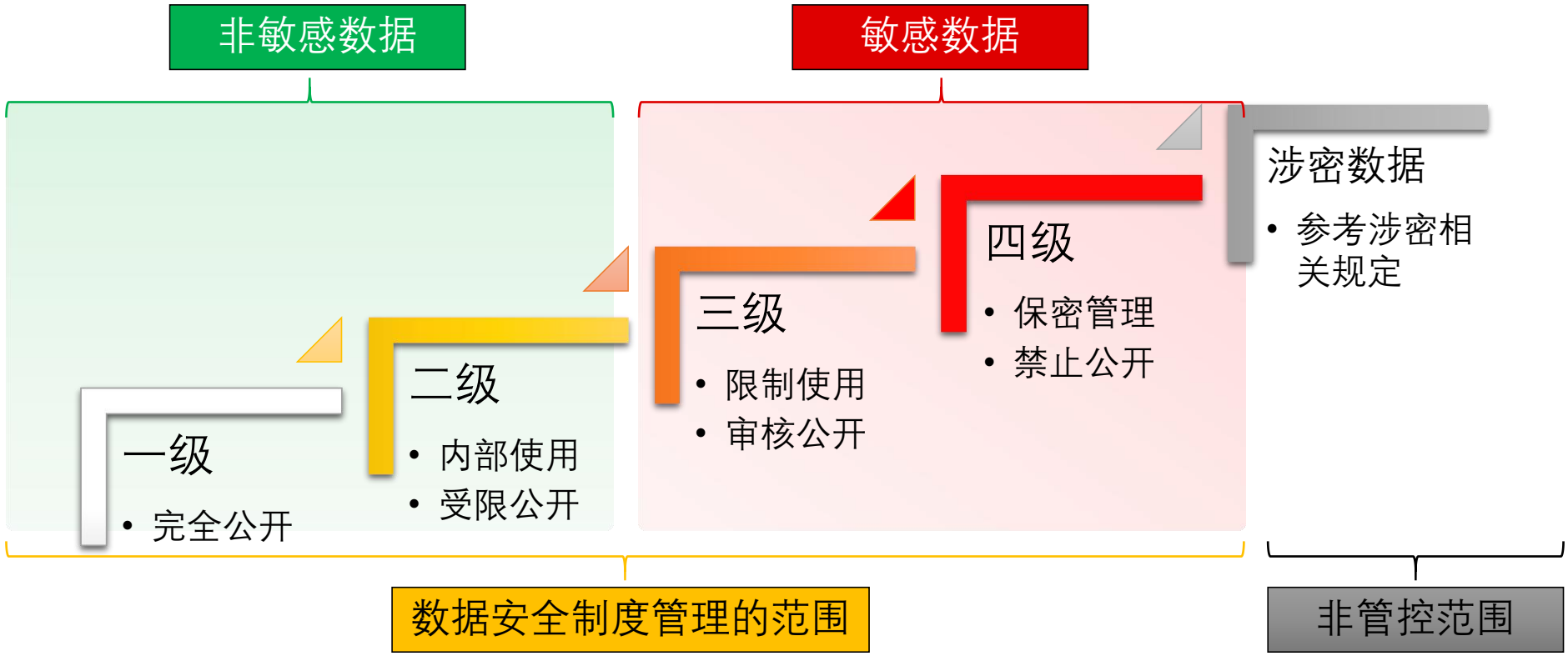
个人及企业信息

- 直接个人信息：单独识别本人
- 间接个人信息：不能单独识别
- 与企业直接或间接相关的信息

业务数据

- 完成业务使命数据
- 运行过程产生的数据

数据分级思路


非敏感数据
敏感数据
一级
• 完全公开
二级
• 内部使用
• 受限公开
三级
• 限制使用
• 审核公开
四级
• 保密管理
• 禁止公开
涉密数据
• 参考涉密相关规定
数据安全制度管理的范围
非管控范围

我国的数据分类及分级
——重要数据

重要数据分级

第一级：	第二级：	第三级：	第四级：	第五级：
数据受到破坏后，会对**公民、法人**和**其他组织**的合法权益造成**损害**，但不损害国家安全、社会秩序和公共利益。	数据受到破坏后，会对**公民、法人**和**其他组织**的合法权益产生**严重损害**，或者对**社会秩序**和**公共利益**造成**损害**，但不损害国家安全。	数据受到破坏后，会对**社会秩序**和**公共利益**造成**严重损害**，或者对国家安全造成损害。	数据受到破坏后，会对**社会秩序**和**公共利益**造成**特别严重损害**，或者对**国家安全**造成**严重损害**。	数据受到破坏后，会对**国家安全**造成**特别严重损害**。

我国的数据分类及分级
——个人及企业信息

个人及企业信息分级

低	中	高
• **保密：**非授权用户获取个人信息数据对个人或群体等造成有限的不良影响。 • **完整：**个人信息数据被非法授权修改和破坏对个人或群体等造成有限的不良影响。 • **可用：**合法用户使用个人信息数据被不正当拒绝对个人或群体等造成有限的不良影响。	• **保密：**非授权用户获取个人信息数据对个人或群体等造成严重的不良影响。 • **完整：**个人信息数据被非法授权修改和破坏对个人或群体等造成严重的不良影响。 • **可用：**合法用户使用个人信息数据被不正当拒绝对个人或群体等造成严重的不良影响。	• **保密：**非授权用户获取个人信息数据对个人或群体等造成灾难性的不良影响。 • **完整：**个人信息数据被非法授权修改和破坏对个人或群体等造成灾难性的不良影响。 • **可用：**合法用户使用个人信息数据被不正当拒绝对个人或群体等造成灾难性的不良影响。

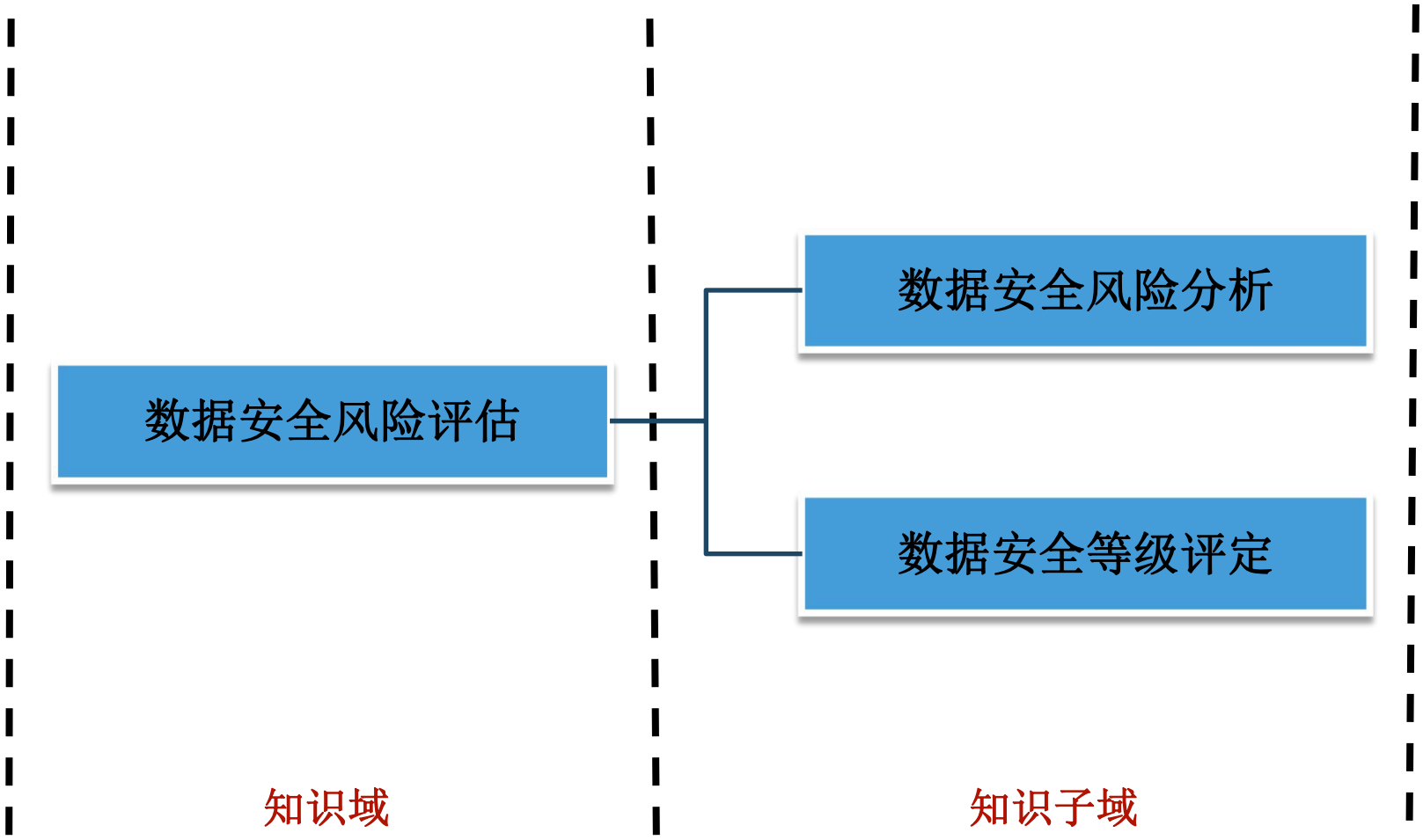
我国的数据分类及分级
——业务数据

业务数据分级

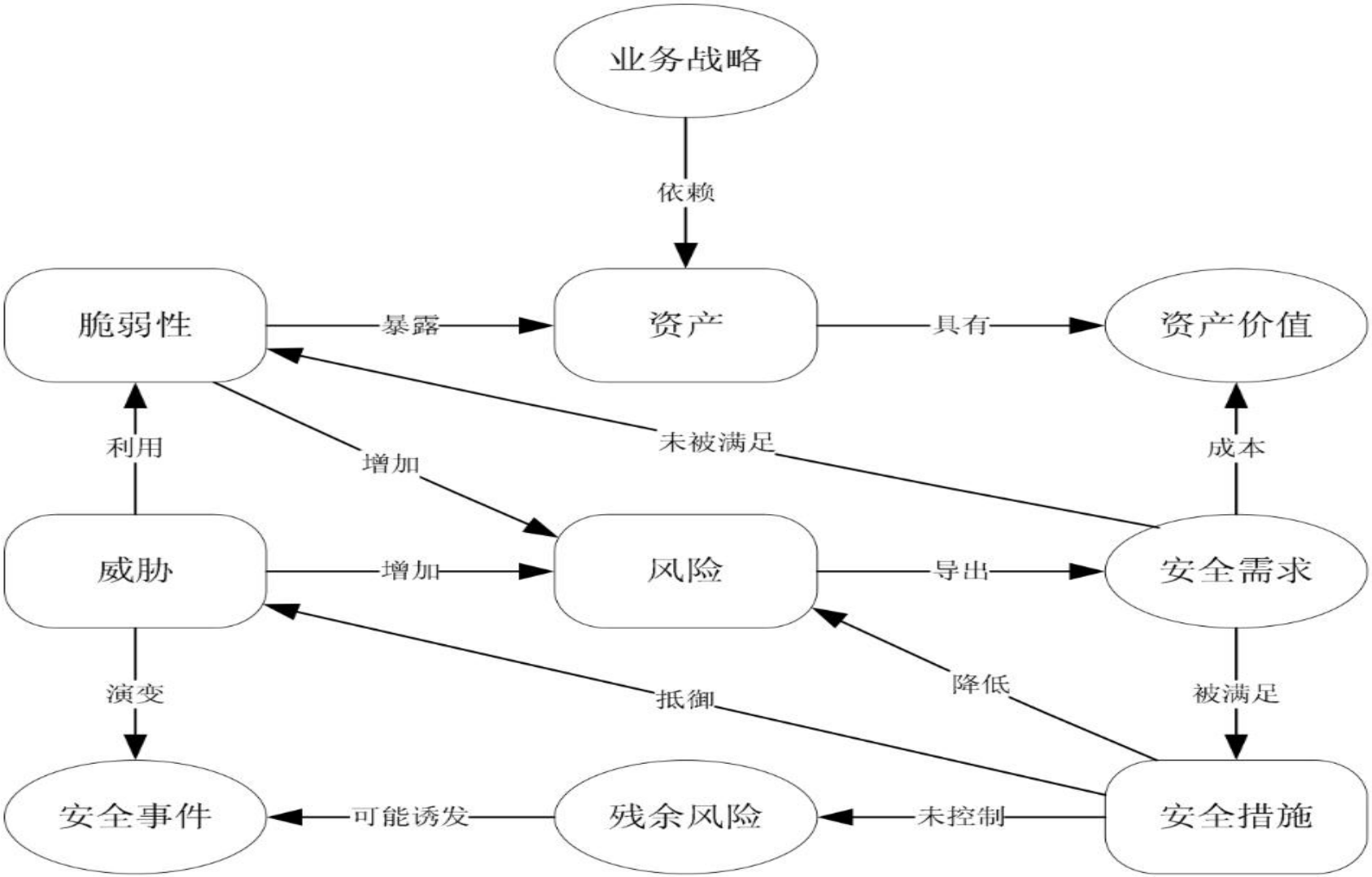
低	中	高
• **保密：**非授权用户获取业务数据对组织运营、组织资产等造成有限的不良影响。 • **完整：**业务数据被非法授权修改和破坏对组织运营、组织资产等造成有限的不良影响。 • **可用：**合法用户使用业务数据被不正当拒绝对组织运营、组织资产等造成有限的不良影响。	• **保密：**非授权用户获取业务数据对组织运营、组织资产等造成严重的不良影响。 • **完整：**业务数据被非法授权修改和破坏对组织运营、组织资产等造成严重的不良影响。 • **可用：**合法用户使用业务数据被不正当拒绝对组织运营、组织资产等造成严重的不良影响。	• **保密：**非授权用户获取业务数据对组织运营、组织资产等造成灾难性的不良影响。 • **完整：**业务数据被非法授权修改和破坏对组织运营、组织资产等造成灾难性的不良影响。 • **可用：**合法用户使用业务数据被不正当拒绝对组织运营、组织资产等造成灾难性的不良影响。

课程内容

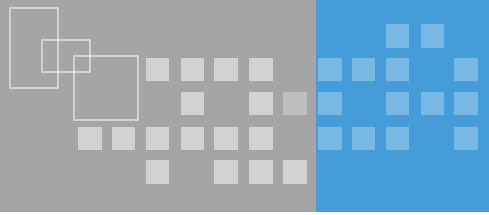
❖ 知识体：数据安全评估



回顾：风险评估要素之间关系



数据安全风险分析-总体过程



业务识别

- 安全责权
- 业务关系
- 关键路径
- 安全偏好
- ……

数据识别

- 数据分类
- 数据分级
- 数据流向
- 生命周期
- 特征模型
- ……

风险识别

- 管理风险
- 技术风险
- 运营风险
- ……

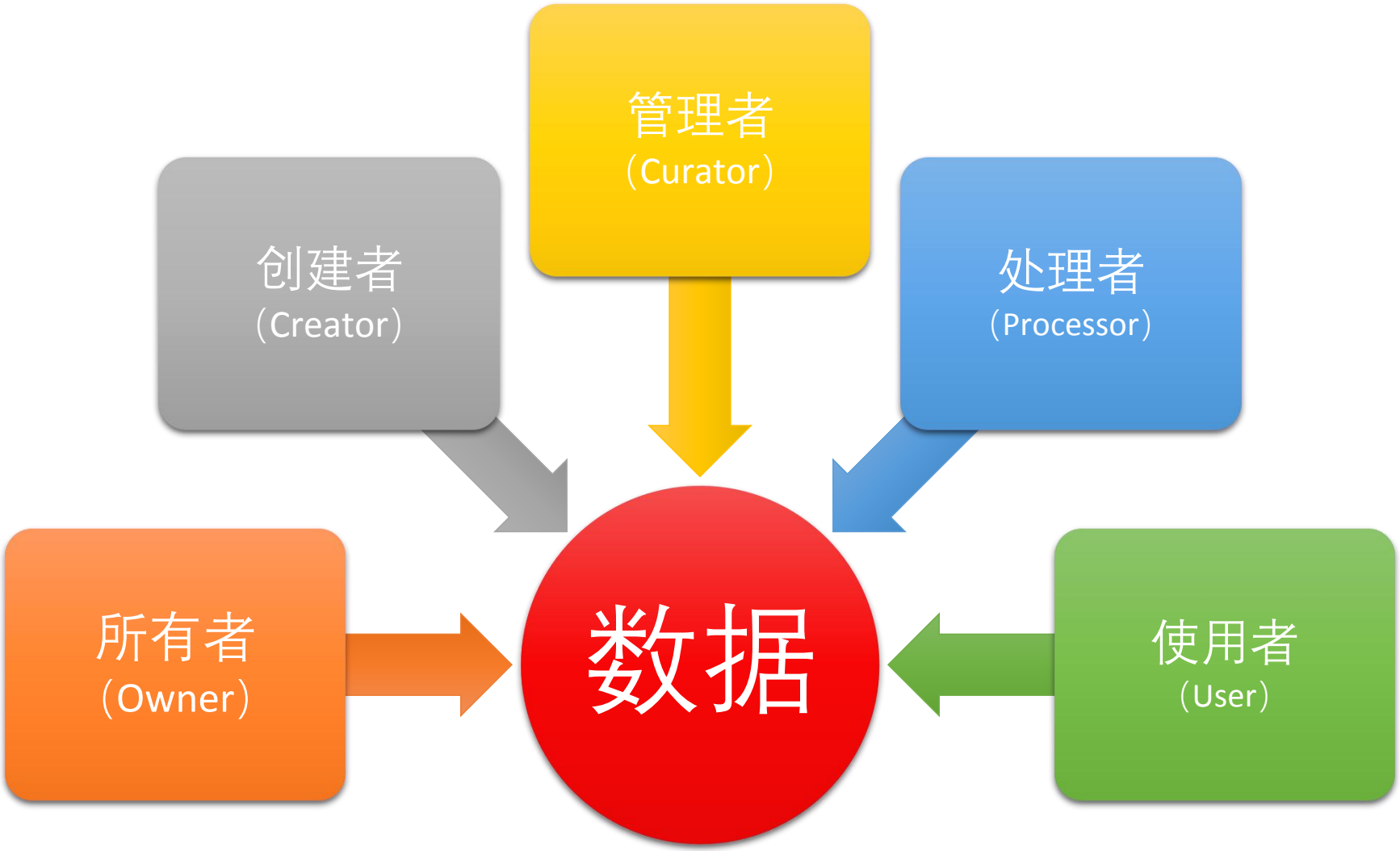
策略保障

- 能力目标
- 策略梳理
- 策略制定
- 策略优化
- 流程优化
- 管理优化
- ……

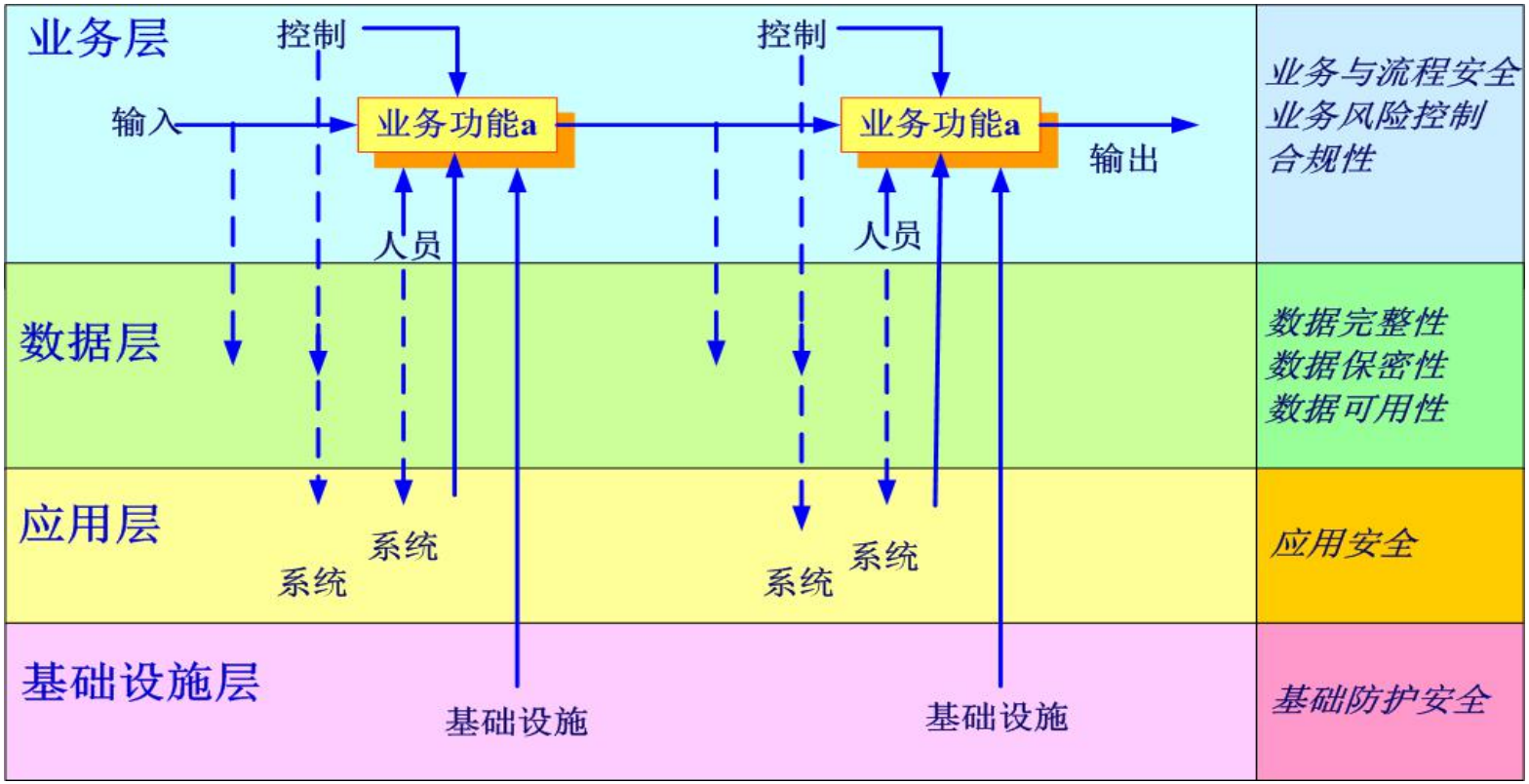
重要成果

数据资产清单	数据分类分级清单	业务访问过程与数据流向	敏感数据分布与流转分析	脆弱性总结报告	风险分析报告	安全成熟度评估	安全策略指导建议	组织架构调整建议	管理体系改进建议	……

数据安全风险分析——角色识别



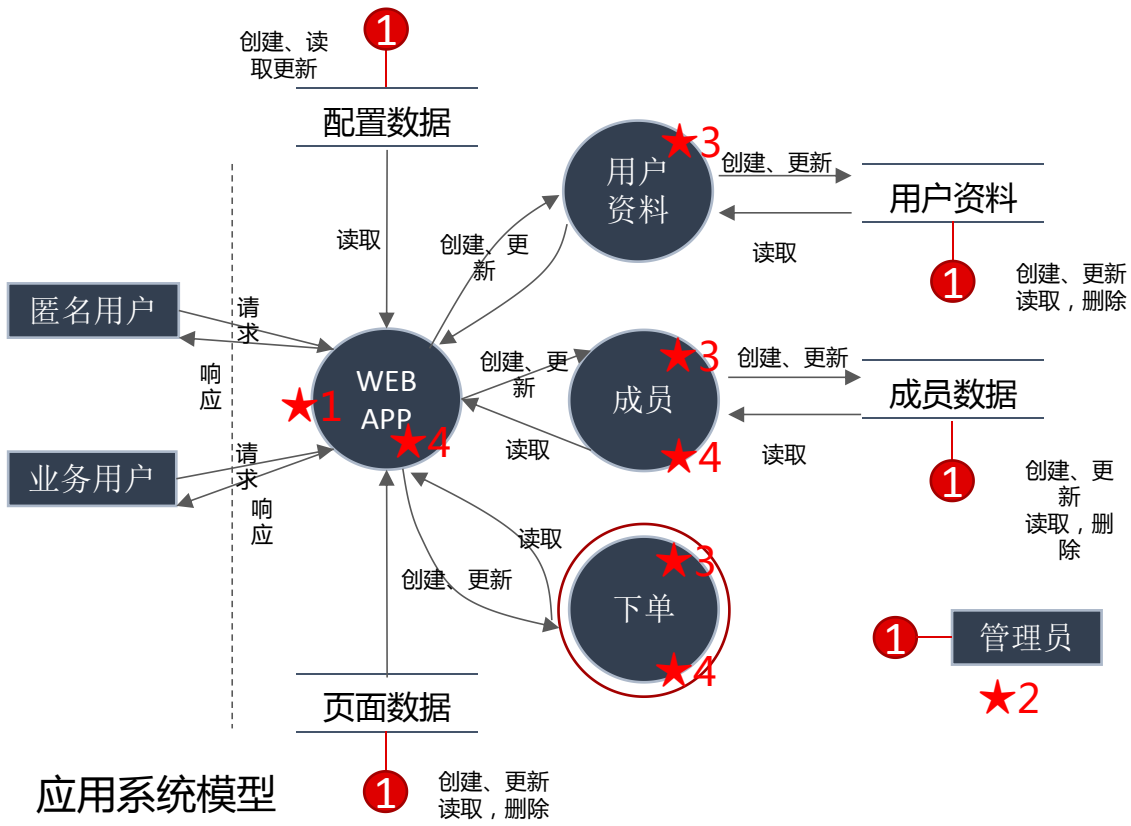
数据安全风险分析——业务分析



- 需求调研方式
  - 信息收集整理分析：收集已有的业务数据流分析、安全管理制度、已有安全建设成果等文档数据并进行深入分析，梳理系统运行环境及业务数据流安全现状。
  - 人员访谈和问卷调查：通过请相关业务、技术和管理人员填写问题表格，进行人员访谈，深入理解信息系统的重要程度、功能、流程，重要信息的分类情况，以及用户分布情况。
  - 现场核查：根据需要及授权登录系统，观察并收集系统运行环境及业务数据流相关的信息。

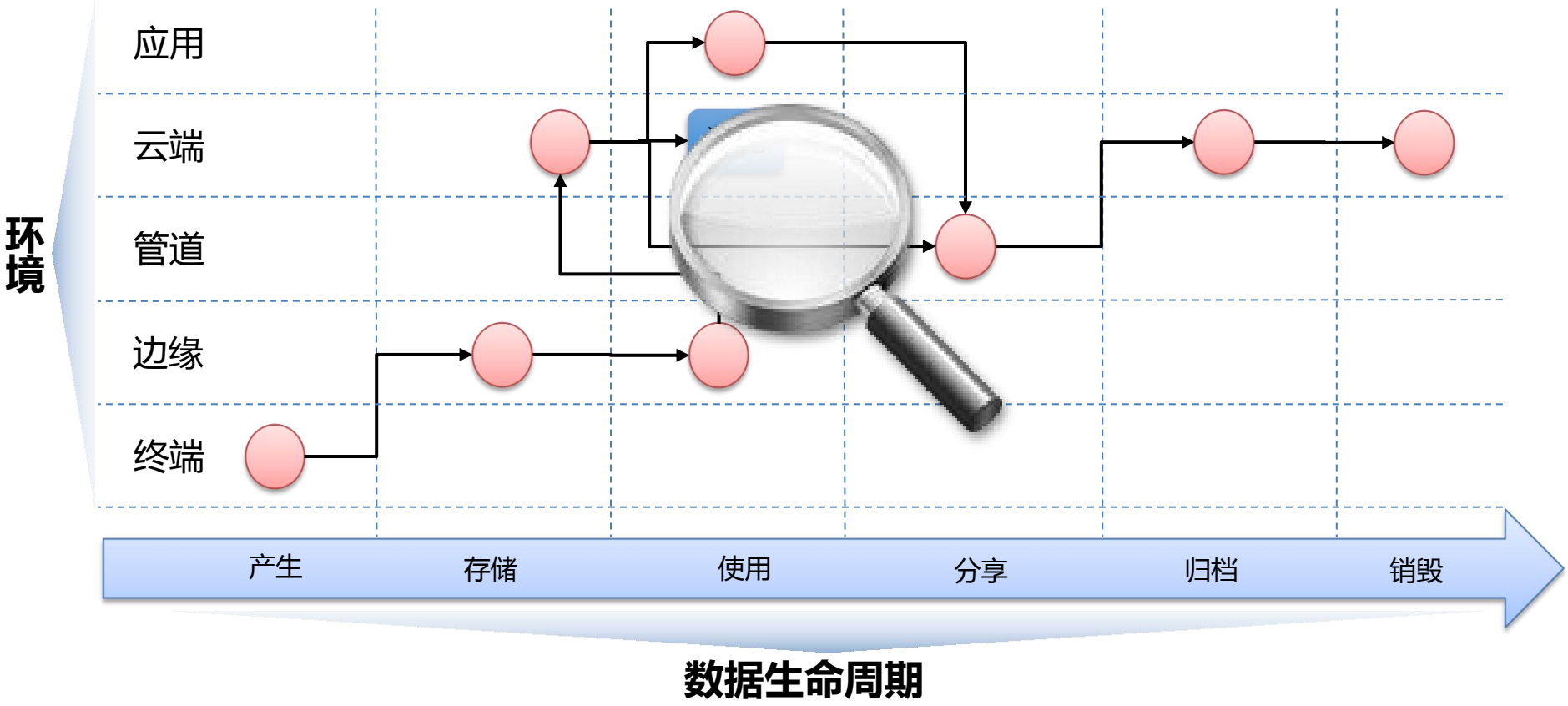
数据安全风险分析——业务建模

- 通过业务建模，明确业务访问及数据流转过程



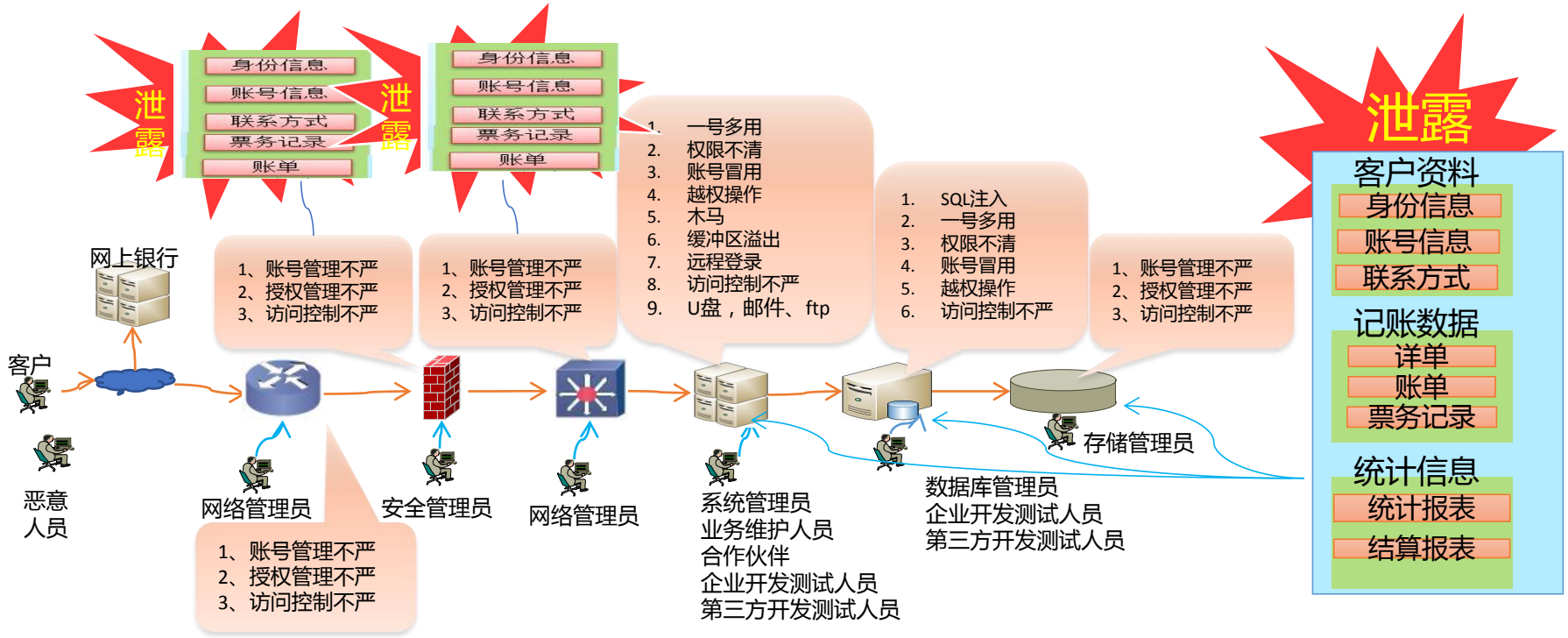
数据安全风险分析——数据生命周期

- 基于业务建模结果，从全局角度识别关键数据生命周期演化过程。



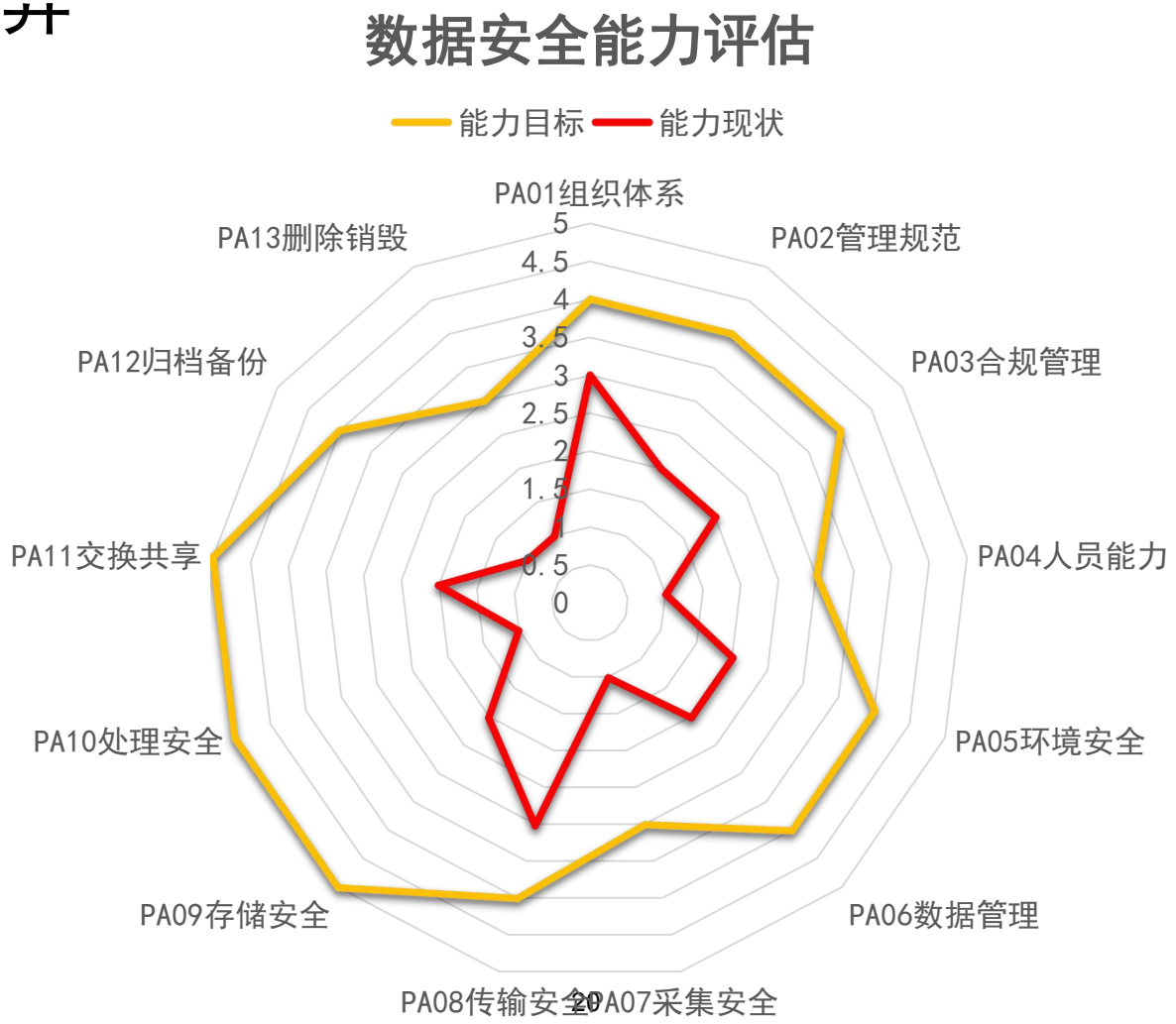
数据安全风险分析——风险识别分析

- 识别敏感数据访问的关键路径，并基于网络安全风险评估手段，分析并识别主要的数据安全风险



数据安全等级评定

- 通过数据安全能力评估，找出现状与能力目标的差异



数据安全策略制定

1）谁？

- 银行员工
- 外包人员
- 合作伙伴
- 客户

2）何时、何地（哪来、去哪）？

- 生产网
- 办公网
- 互联网
- 移动互联网

3）做什么？

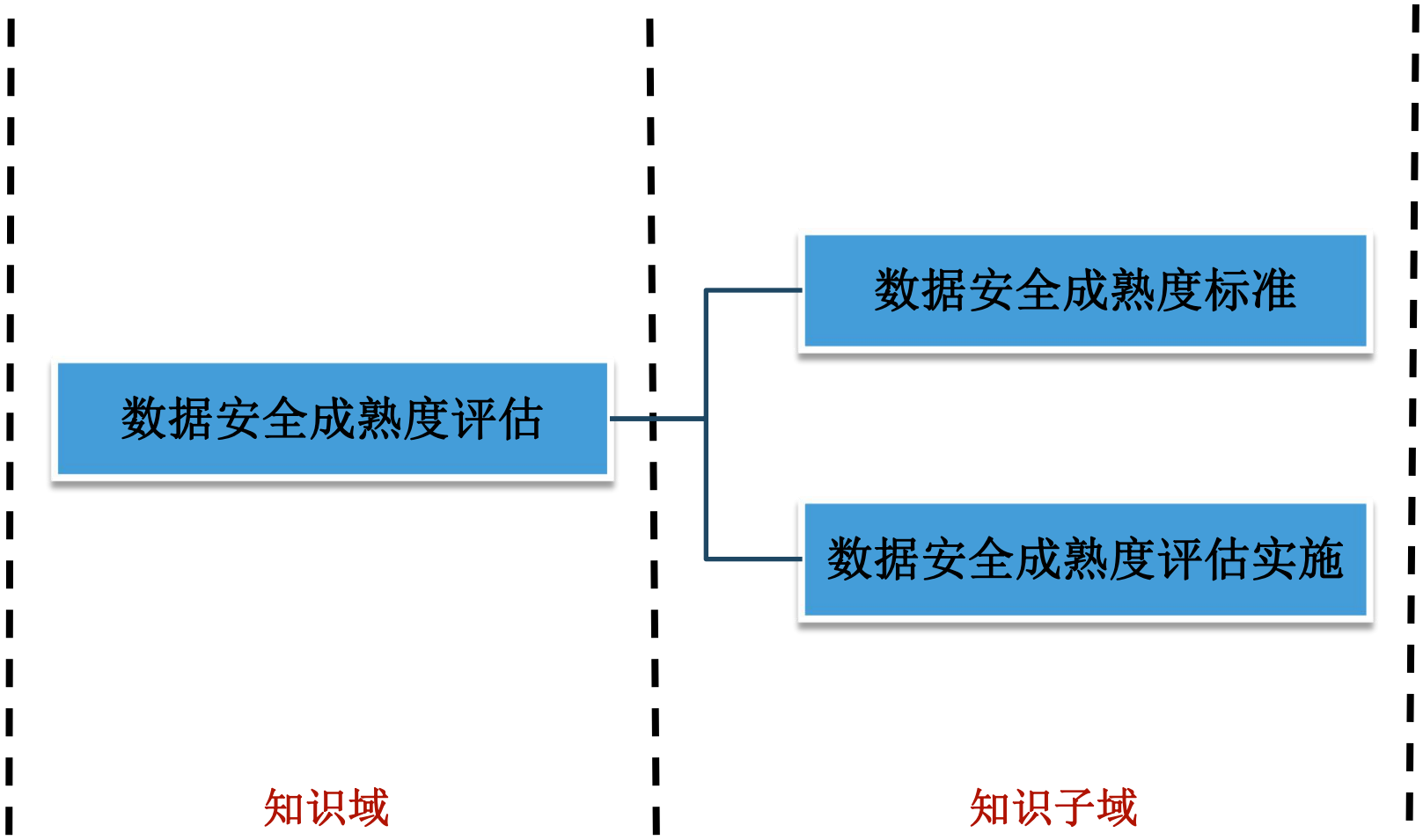
- 帐号维护
- 权限调整
- 数据输入
- 数据查询
- 报表统计
- 数据下载
- 批量导出

4）对象是什么？

- 生产数据
- 管理数据
- 办公数据
- 统计数据

课程内容

❖ 知识体：数据安全评估

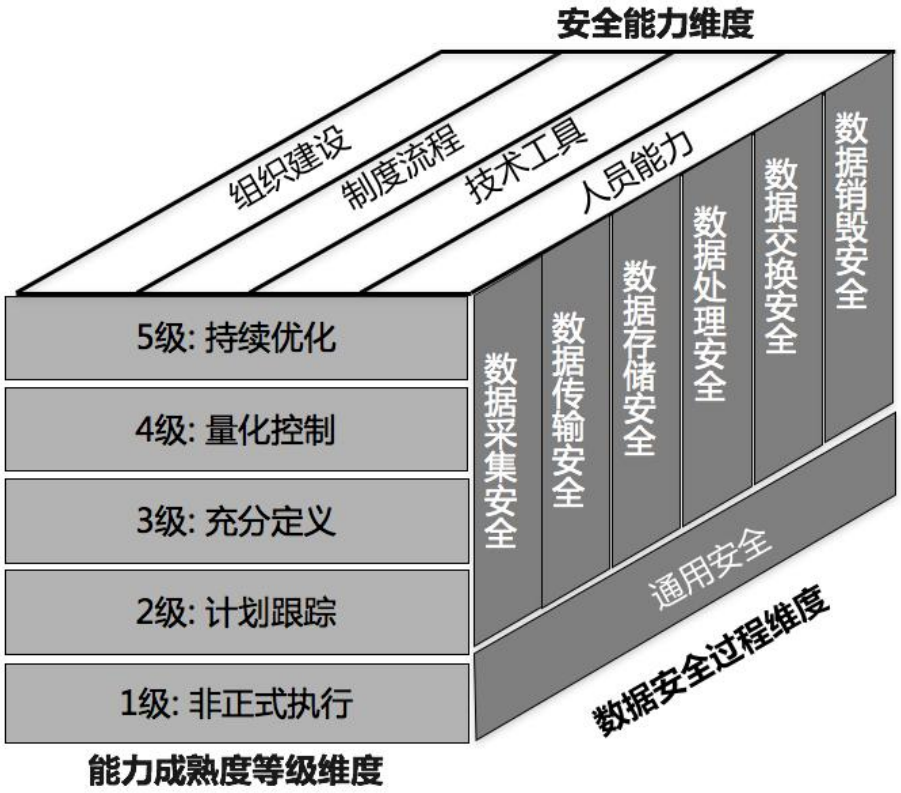


数据安全成熟度标准

- 标准名称：《信息安全技术 数据安全能力成熟度模型》（报批阶段）2018-7-23
- 编制单位：阿里巴巴、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、联想、公安三所、清华大学、中国信息安全认证中心、中科院软件所、中国移动、阿里云、北京天融信、中国科院信工所、陕西省信息化工程研究院、西北大学、浪潮、北京易华录信息技术、新华三、勤智数码科技、北京数字认证、启明星辰、海信集团、银川市大数据管理服务局、南京中新赛克科技、北京微步在线科技、上海观安、华为、三六零、中电长城

数据安全成熟度标准

❖DSMM模型框架



数据安全能力成熟度模型架构图

围绕数据生命周期

- 以数据为中心
- 以组织为单位
- 以能力成熟度为抓手
- 聚焦组织在数据上的安全管理能力
- 贯穿组织建设、人员能力、制度流程、技术工具四个维度

适用于

- 传统及互联网各类组织
- 电子化数据
- 自评估及第三方测评
- 数据安全能力建设

数据安全成熟度标准

安全能力维度

- 通过对组织机构各数据安全过程所需具备安全能力的量化，进而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关键能力展开。
  - 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：组织机构数据安全领域的制度规范和流程执行。
  - 技术工具：通过技术手段和产品工具落实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安全意识及相关专业能力。

数据安全成熟度标准

安全能力维度——组织建设

- 从承担数据安全工作的组织机构应具备的组织建设能力出发，根据以下方面进行能力等级区分：
  - 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。

数据安全成熟度标准

安全能力维度——制度流程

- 从组织机构在数据安全制度流程的建设以及执行情况出发，根据以下方面进行能力等级区分：
  - 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。
  - 制度流程落地执行的一致性和有效性。

数据安全成熟度标准

安全能力维度——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，根据以下方面进行能力等级区分：
  - 数据安全技术在数据全生命周期过程中的利用情况，应对数据全生命周期安全风险的能力。
  - 利用技术工具对数据安全工作的自动化支持能力，对数据安全制度流程固化执行的实现能力。

数据安全成熟度标准

安全能力维度——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，根据以下方面进行能力等级区分：
  - 数据安全人员所具备的数据安全技能是否能够满足实现安全目标的能力要求(对数据相关业务的理解程度以及数据安全专业能力)。
  - 数据安全人员的数据安全意识以及对关键数据安全岗位员工数据安全能力的培养。

数据安全成熟度标准

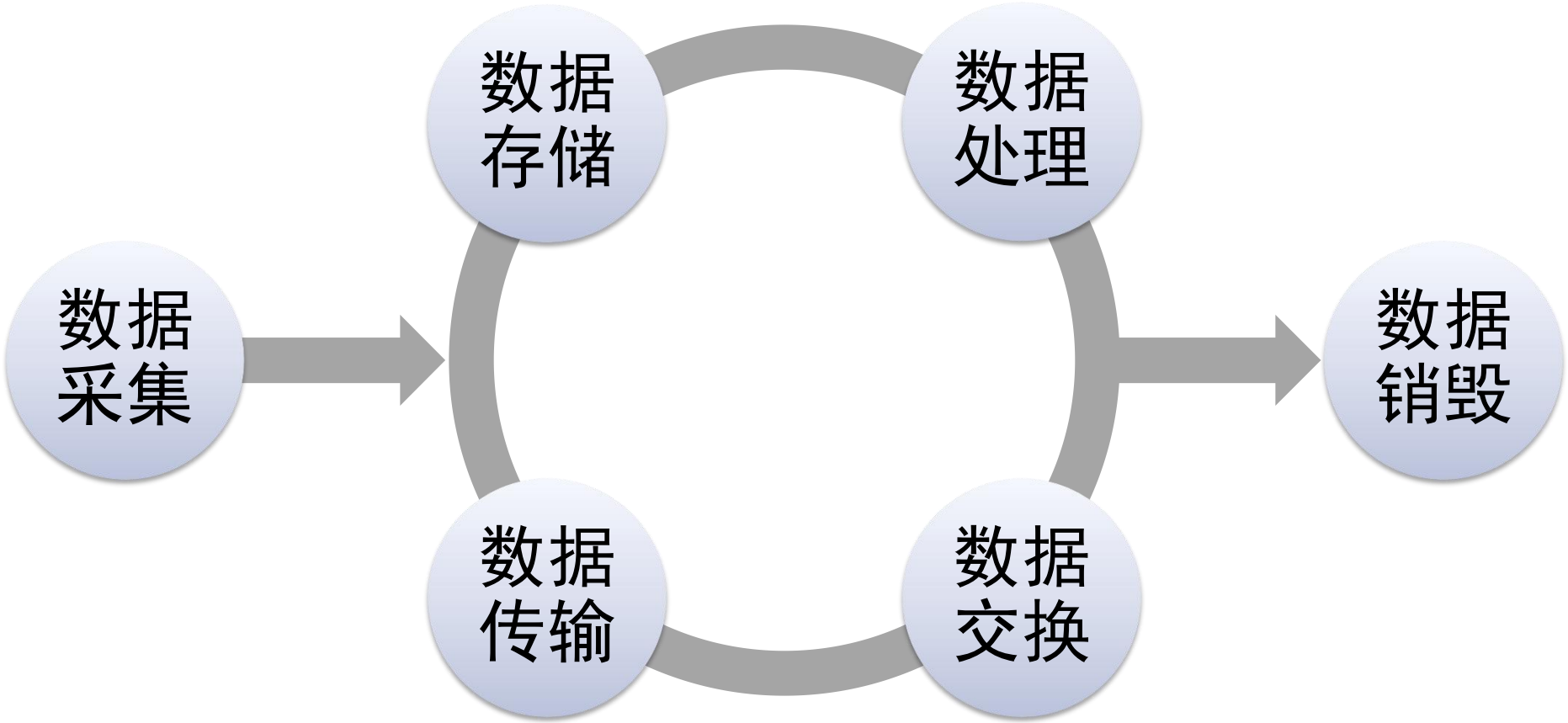
能力成熟度等级

- 组织机构的数据安全能力成熟度等级共分为5级，随着组织机构的数据安全能力成熟度的不断提升，数据安全能力成熟度从1级至5级逐级提高。

等级	成熟度等级特征
等级1：非正式执行	**基本实践：**随机、无序、被动地执行安全过程，依赖于个人经验，无法复制。
等级2：计划跟踪	**规划、规范、验证、跟踪：**在业务系统级别主动地实现了安全过程的计划与执行，但没有形成体系化。
等级3：充分定义	**定义、执行标准过程、协调安全实践：**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	**建立可测安全目标、客观地管理执行：**建立了量化目标，安全过程可度量。
等级5：持续优化	**改进组织能力、改进过程有效性：**根据组织机构的整体目标，不断改进和优化安全过程。

数据安全成熟度标准

- 数据安全过程——数据生命周期



数据安全成熟度标准

数据安全过程——数据生命周期

- 本标准基于大数据环境下数据在组织机构业务中的流转情况，定义了数据生命周期的六个阶段
  - 数据采集：组织机构内部系统中新产生数据，以及从外部系统收集数据的阶段。
  - 数据传输：数据从一个实体通过网络流动到另一个实体的阶段。
  - 数据存储：数据以任何数字格式进行物理存储或云存储的阶段。

数据安全成熟度标准

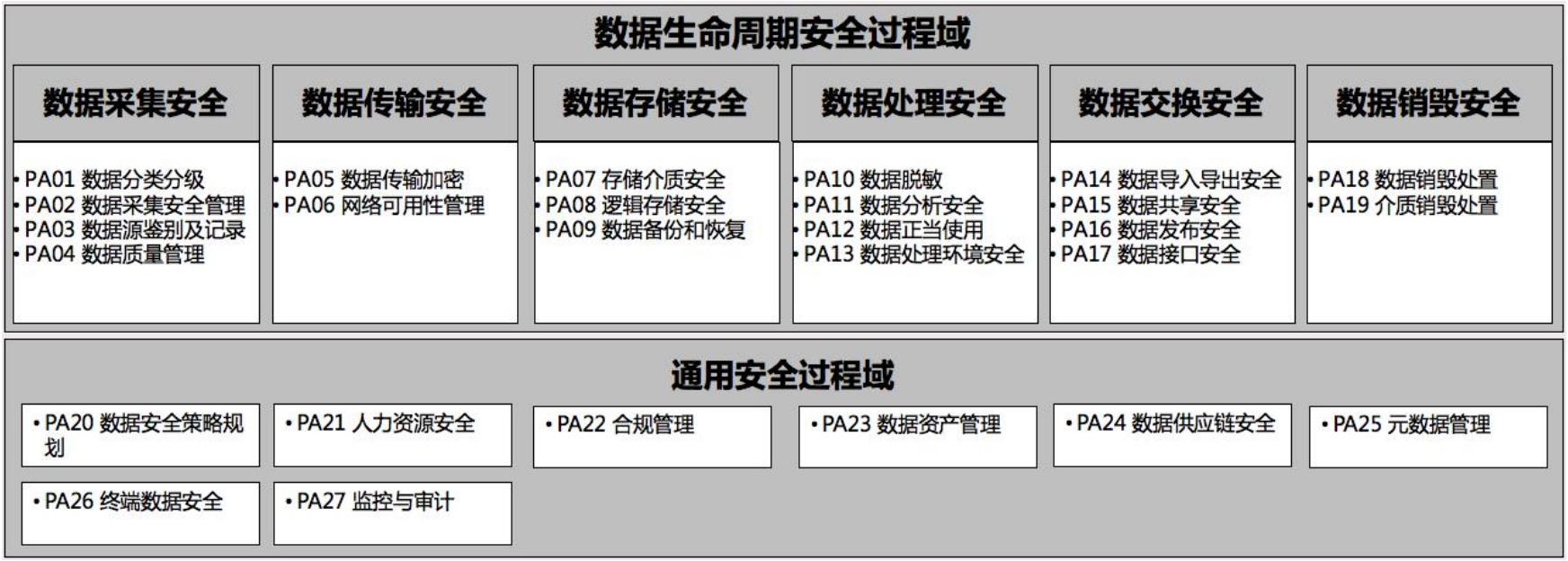
数据安全过程——数据生命周期

- 数据处理：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：组织机构与组织机构及个人进行数据交互的阶段。
- 数据销毁：通过对数据及数据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地经历六个阶段。

数据安全成熟度标准

❖ 数据安全过程——数据安全过程域体系



数据安全过程域体系

数据安全成熟度标准

数据采集安全

- 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

数据安全成熟度标准

数据采集安全——PA01数据分类分级

- 基于法律法规以及业务需求确定组织机构内部的数据分类分级方法，对生成或收集的数据进行分类分级标识。

	组织建设	制度流程	技术工具	人员能力
等级1	–	临时需求 个人经验	–	–
等级2	业务团队负责	业务特性 外部合规 分类分级原则	–	–
等级3	专门管理人员 业务团队执行	方法及细则 分级安全策略 变更审核	自动分级标识 变更记录审计	理解业务场景 理解数据风险
等级4	–	–	提升标识工具	–
等级5	–	定期评审改进	策略定期更新	–

数据安全成熟度标准

数据采集安全——PA02数据采集安全管理

- 在采集外部客户、合作伙伴等相关方的数据的过程中，需明确采集数据的目的和用途，确保数据源的真实性、有效性和最少够用等原则要求，并规范数据采集的渠道、数据的格式以及相关的流程和方式，从而保证数据采集的合规性、正当性和执行上的一致性，符合相关法律法规要求。

	组织建设	制度流程	技术工具	人员能力
等级1	–	–	–	–
等级2	核心业务管理	合规采集规则 取得主体同意	–	–
等级3	成立管理团队 风险评估小组	定义流程方法 明确数据来源 风险评估流程 安全控制措施 安全保护部门	规范采集工具 采集过程防泄露	充分理解需求 提出解决方案
等级4	建立度量机制	–	采集数据验证	–
等级5	–	持续优化	优化采集工具	–

数据安全成熟度标准

数据采集安全——PA03数据源鉴别及记录

- 对产生数据的数据源进行身份鉴别和记录，防止数据仿冒和数据伪造。

	组织建设	制度流程	技术工具	人员能力
等级1	–	个别临时记录	–	–
等级2	业务团队负责	核心业务流程	鉴别和记录	–
等级3	专门管理人员	制定管理规范 要求鉴别记录	识别和记录	理解业务场景 理解鉴别标准
等级4	–	定义可追溯要求 合规审核机制	数据管理平台	–
等级5	–	方法持续改进	持续改进工具	–

数据安全成熟度标准

数据采集安全——PA04数据质量管理

- 建立组织机构的数据质量管理体系，保证对数据采集过程中收集/产生的数据的准确性、一致性和完整性。

	组织建设	制度流程	技术工具	人员能力
等级1	–	–	–	–
等级2	业务团队负责	核心业务要求	–	具备理论基础 场景防范能力
等级3	专门管理人员	制定管理规范 建立监控规则	元数据管理平台	基于实际需求 理解质量标准
等级4	–	质量分级标准 质量分析盘点	–	–
等级5	可持续优化	–	平台量化评估	–

数据安全成熟度标准

数据传输安全

- PA05 数据传输加密
- PA06 网络可用性管理

数据安全成熟度标准

数据传输安全——PA05数据传输加密

- 根据组织机构内部和外部的数据传输需求，采用适当的加密保护措施，保证传输通道、传输节点和传输数据的安全，防止传输过程中数据被截取所引发的数据泄漏。

	组织建设	制度流程	技术工具	人员能力
等级1	-	个别业务	-	-
等级2	业务团队负责	明确加密范围 国家认可算法	-	-
等级3	专业管理人员	明确业务场景 密钥管理规范	两端鉴别认证 统一加密方案 密钥管理系统	了解主流技术 了解加密算法
等级4	-	分级传输要求	全面证书认证 量化评估审核 统一加密模块	-
等级5	-	-	技术提升改进	-

数据安全成熟度标准

数据传输安全——PA06网络可用性管理

- 通过网络基础链路、关键网络设备的备份建设，实现网络的高可用性，从而保证数据传输过程的稳定性。

	组织建设	制度流程	技术工具	人员能力
等级1	–	部分业务	–	–
等级2	网络团队负责	关键链路可用	–	–
等级3	–	关键业务要求	部署安全设备	制定有效方案
等级4	–	–	定量分析	–
等级5	–	–	优化网络架构	–

数据安全成熟度标准

数据存储安全

- PA07 存储介质安全
- PA08 逻辑存储安全
- PA09 数据备份和恢复

数据安全成熟度标准

数据存储安全——PA07存储介质安全

- 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，提供有效的技术和管理手段，防止对介质的不当使用而可能引发的数据泄露风险。

	组织建设	制度流程	技术工具	人员能力
等级1	–	–	–	–
等级2	明确管理人员	建立安全制度	–	熟悉制度要求
等级3	统一管理岗位	策略管理规范 购买及使用 标记及检查	净化工具 行为记录审计	熟悉合规要求
等级4	–	–	使用传递跟踪	–
等级5	–	–	工具持续更新	–

数据安全成熟度标准

数据存储安全——PA08逻辑存储安全

- 基于组织机构内部的业务特性和数据存储安全要求，建立针对数据逻辑存储、存储容器和架构的有效安全控制。

	组织建设	制度流程	技术工具	人员能力
等级1	–	–	系统默认	–
等级2	核心业务管理	–	采用技术工具	–
等级3	统一负责人员 明确管理人员	明确安全规则 明确逻辑隔离 制定规范规程	安全扫描工具 使用行为监测	熟悉技术架构 能够判断风险
等级4	–	分层授权管理 分布式安全规则	统一管理控制 可伸缩架构	–
等级5	定期审核改进	–	–	–

数据安全成熟度标准

数据存储安全——PA09数据备份和恢复

- 通过执行定期的数据备份和恢复，实现对存储数据的冗余管理，保护数据的可用性。

	组织建设	制度流程	技术工具	人员能力
等级1	–	–	–	–
等级2	–	部分业务场景	–	–
等级3	明确负责人员	建立管理制度 建立操作规程 检查更新程序	统一技术工具 备份数据管理	有效备份恢复
等级4	–	控制策略与规范 定期统计	多级数据归档	–
等级5	–	采纳优秀方案	–	–

数据安全成熟度标准

数据处理安全

- 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

数据安全成熟度标准

数据处理安全——PA10数据脱敏

- 根据相关法律法规、标准的要求以及业务需求，明确敏感数据的脱敏需求和规则，对敏感数据进行脱敏处理，保证数据可用性和安全性的平衡。

	组织建设	制度流程	技术工具	人员能力
等级1	–	部分业务字段	–	–
等级2	业务团队负责	–	–	了解常用技术 业务场景分析
等级3	统一负责人员	建立脱敏规范 申请阶段评估	统一脱敏工具 场景脱敏定制 过程记录审计	数据常规技术 方案定制化
等级4	–	脱敏资产清单 明确规范要求	数据识别 效果验证 场景策略 动态脱敏	定期能力考核
等级5	–	–	跟踪最佳实践 整体解决方案	–

数据安全成熟度标准

数据处理安全——PA11 数据分析安全

- 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。

	组织建设	制度流程	技术工具	人员能力
等级1	部分业务	–	–	–
等级2	业务团队负责 核心业务分析 个人数据人工审核	–	–	–
等级3	统一负责岗位	安全保护规范 操作实施指南 结果审查评估 操作审计分析	去标识化 日志记录溯源	风险有效评估 提出解决方案
等级4	–	–	多种技术结合 结果数据扫描 风险监控平台	–
等级5	–	持续跟进合规	–	跟进最佳实践

数据安全成熟度标准

数据处理安全——PA12 数据正当使用

- 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。

	组织建设	制度流程	技术工具	人员能力
等级1	相关业务中	–	–	–
等级2	业务团队负责	身份及访问要求	–	–
等级3	统一负责人员	整体权限管理 统一管理流程 内部责任制度	统一身份管理 多因素认证 最小权限原则 完成操作日志	了解身份管理 有效管理方案
等级4	–	具备策略流程 违规处理流程 定期审核	–	风险分析跟进
等级5	–	–	自动化分析处理	–

数据安全成熟度标准

数据处理安全——PA13 数据处理环境安全

- 为组织机构内部的数据处理环境建立安全保护机制，提供统一的数据计算、开发平台，确保数据处理的过程中有完整的安全控制管理和技术支持

	组织建设	制度流程	技术工具	人员能力
等级1	部分业务	–	–	–
等级2	业务团队负责	–	–	–
等级3	统一负责人员	安全控制措施	权限管理联动 多租户隔离 日志审计溯源 节点风险监测	了解主要风险 有效规避风险
等级4	–	定期审计	–	–
等级5	–	操作实时监控 及时风险控制	–	–

数据安全成熟度标准

数据交换安全

- 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

数据安全成熟度标准

数据交换安全——PA14 数据导入导出安全

- 通过对数据导入、导出过程中对数据的安全性进行管理，防止数据导入导出过程中可能对数据自身的可用性和完整性构成的危害，降低可能存在的数据泄漏风险。

	组织建设	制度流程	技术工具	人员能力
等级1	临时需求 个人经验	–	–	–
等级2	业务团队负责	制定策略规程	–	理解业务场景
等级3	统一负责人员	建立制度规范 介质标识规范	在线审批平台 安全技术方案 日志管理审计	充分理解策略
等级4	–	–	统一导入导出 通道备份监控 风险审核提示	–
等级5	–	方案持续优化	–	–

数据安全成熟度标准

数据交换安全——PA15 数据共享安全

- 通过在业务系统、产品对外部组织机构提供数据时，以及通过合作的方式与第三方合作伙伴交换数据时执行共享数据的安全风险控制，以降低数据共享场景下的安全风险。

	组织建设	制度流程	技术工具	人员能力
等级1	–	–	–	–
等级2	业务团队负责	场景分析 建立方案	–	理解业务场景
等级3	统一管理人员	原则及措施 场景细化规范 共享审核流程 日志管理审计 第三方平台评估	在线审核平台 关键数据加密 共享监控工具 日志审计工具	充分理解策略
等级4	–	关键场景细则 风险持续可控	安全风险提示 安全防护基线	–
等级5	–	定期评估 持续优化	–	–

数据安全成熟度标准

数据交换安全——PA16 数据发布安全

- 通过在对外部组织机构进行数据发布的过程中对发布数据的格式、适用范围、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。

	组织建设	制度流程	技术工具	人员能力
等级1	临时需求	–	–	–
等级2	业务团队负责	明确规范要求	–	基本理解制度
等级3	统一负责人员 专人信息披露	审核制度流程 应急处理流程 定期审查机制	资源公开数据库 数据发布平台 应急处理平台	充分理解制度
等级4	–	关键数据细则 细化审核流程	安全风险提示	–
等级5	–	–	接口及格式规范	–

数据安全成熟度标准

数据交换安全——PA17 数据接口安全

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

	组织建设	制度流程	技术工具	人员能力
等级1	临时需求	–	–	–
等级2	业务团队负责	接口调用规范	–	基本安全能力
等级3	统一负责人员	接口控制策略 接口安全规范 签署合作协议	接口控制措施 日志记录审计 安全通道加密	充分理解场景 充分控制能力
等级4	–	–	自动监控处理	–
等级5	–	–	安全持续改进	–

数据安全成熟度标准

数据销毁安全

- PA18 数据销毁处置
- PA19 介质销毁处置

数据安全成熟度标准

数据销毁安全——PA18 数据销毁处置

- 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，防止因对存储介质中的数据内容进行恶意恢复而导致的数据泄漏风险。

	组织建设	制度流程	技术工具	人员能力
等级1	具体业务个案	–	–	–
等级2	业务团队负责	核心业务方案	普通擦除指令	指定销毁方案
等级3	统一负责人员	指定销毁规范 建立销毁机制 详细销毁指南	整体提供工具	熟悉合规要求
等级4	–	效果评估机制	销毁需求标识	–
等级5	–	审核存储时长 及时更新方案	–	–

数据安全成熟度标准

数据销毁安全——PA19介质销毁处置

- 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。

	组织建设	制度流程	技术工具	人员能力
等级1	部分业务	–	–	–
等级2	业务团队负责	核心业务方案	物理销毁	判断必要性
等级3	统一负责人员	制定管理制度 销毁监管机制	统一销毁工具	依据整体需求
等级4	–	过程监控机制	认证机构或设备	–
等级5	–	持续优化流程	持续更新技术	–

数据安全成熟度标准

通用安全

- PA20 数据安全策略规划
- 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 元数据管理
- PA26 终端数据安全
- PA27 监控与审计

数据安全成熟度标准

通用安全——PA20数据安全策略规划

- 建立适用于组织机构数据安全风险现状的组织机构内部整体的数据安全策略规划，数据安全策略规划的内容应实现对数据全生命周期风险的覆盖。

	组织建设	制度流程	技术工具	人员能力
等级1	–	个人经验	–	–
等级2	设立负责人员	基于生命周期	–	安全评估能力 形成制度规范
等级3	专职负责人员	定义管理方针 核心制度体系 评审发布流程	运营管理工具	了解业务目标 安全管理体系 制度有效解读
等级4	–	有效性持续评估	–	评估实时效果
等级5	–	跟踪发展改进	–	趋势洞察能力

数据安全成熟度标准

通用安全——PA21人力资源安全

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

	组织建设	制度流程	技术工具	人员能力
等级1	部分业务	个人经验	–	–
等级2	人力团队负责 关键业务环节	违规处理过程 执行背景调查 定义岗位职责	–	充分了解定位
等级3	部门有效配合 充分定义职能 数据安全领导小组 职责分离原则	专业能力调查 标准合同协议 转岗离职流程 激励处罚制度 职能工作规范	流程自动化 公开职能架构	充分理解环节 教育培训考核 明确安全目标
等级4	效果量化评估 职能关系评估	–	在线人力平台	–
等级5	持续优化职能	优化人力流程	–	–

数据安全成熟度标准

通用安全——PA22合规管理

- 持续跟进组织机构需符合的法律法规要求，以保证组织机构业务的发展不会面临个人信息保护、重要数据保护、跨境数据传输等方面的安全合规的风险。

	组织建设	制度流程	技术工具	人员能力
等级1	业务触发	个人经验	–	–
等级2	核心业务控制	业务环节措施	–	基本理解要求
等级3	专职人员负责	梳理合规清单 统一制度规范 生命周期规范 跨境传输规范	合规资料库 个人信息保护 行为合规分析 跨境在线审批	理解合规要求
等级4	–	业务场景细则 定期审查检验	合规量化呈现 技术手段评价 定期审核	–
等级5	专门监管对接	及时跟进合规	及时更新技术	–

数据安全成熟度标准

通用安全——PA23数据资产管理

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

	组织建设	制度流程	技术工具	人员能力
等级1	业务方承担	–	–	–
等级2	业务人员负责	资产登记清单	–	判断价值损害
等级3	专职负责人员	资产管理制度 登记机制 标记规程 变更审批机制	资产登记工具 自动标识管理	了解管理要求 建立管理制度
等级4	–	安全审查规程	整体量化统计 量化管理情况	–
等级5	–	及时更新机制	–	–

数据安全成熟度标准

通用安全——PA24数据供应链安全

- 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。

	组织建设	制度流程	技术工具	人员能力
等级1	部分业务	–	–	–
等级2	业务人员负责	签署合作协议	–	风险评估能力
等级3	整体管理人员	建立管理规范 能力评估规范	整体供应链库 记录审核分析	整体了解 推进方案落地
等级4	–	合规审核流程 定期风险评估	量化跟踪分析 合规审核工具	–
等级5	–	及时调整方案	–	–

数据安全成熟度标准

通用安全——PA25元数据管理

- 建立组织机构的元数据管理体系，实现对组织机构内元数据的有效集中管理。

	组织建设	制度流程	技术工具	人员能力
等级1	–	部分业务	–	–
等级2	核心业务部门	核心业务规范	–	–
等级3	统一负责人员	服务元数据规范 安全元数据规范 访问控制策略 操作审计追溯	建立管理平台 授权控制技术 日志审计追溯	了解理论基础 理解管理需求
等级4	–	–	可视化数据标签 量化关系管理	–
等级5	–	–	扩大覆盖范围 提升使用效率	–

数据安全成熟度标准

通用安全——PA26终端数据安全

- 基于组织机构对终端层面的数据保护要求，针对组织机构内部的工作终端采取相应的技术和管理方案。

	组织建设	制度流程	技术工具	人员能力
等级1	终端管理团队	–	–	–
等级2	–	终端管理规范	员工终端绑定 统一防毒软件	–
等级3	统一管理人员	终端防泄露要求 泄露事件处理	终端准入控制 统一防护工具 终端防泄露 整体安全方案	了解数据风险 利用工具控制
等级4	–	–	成效量化评估	–
等级5	–	–	多终端防泄露	–

数据安全成熟度标准

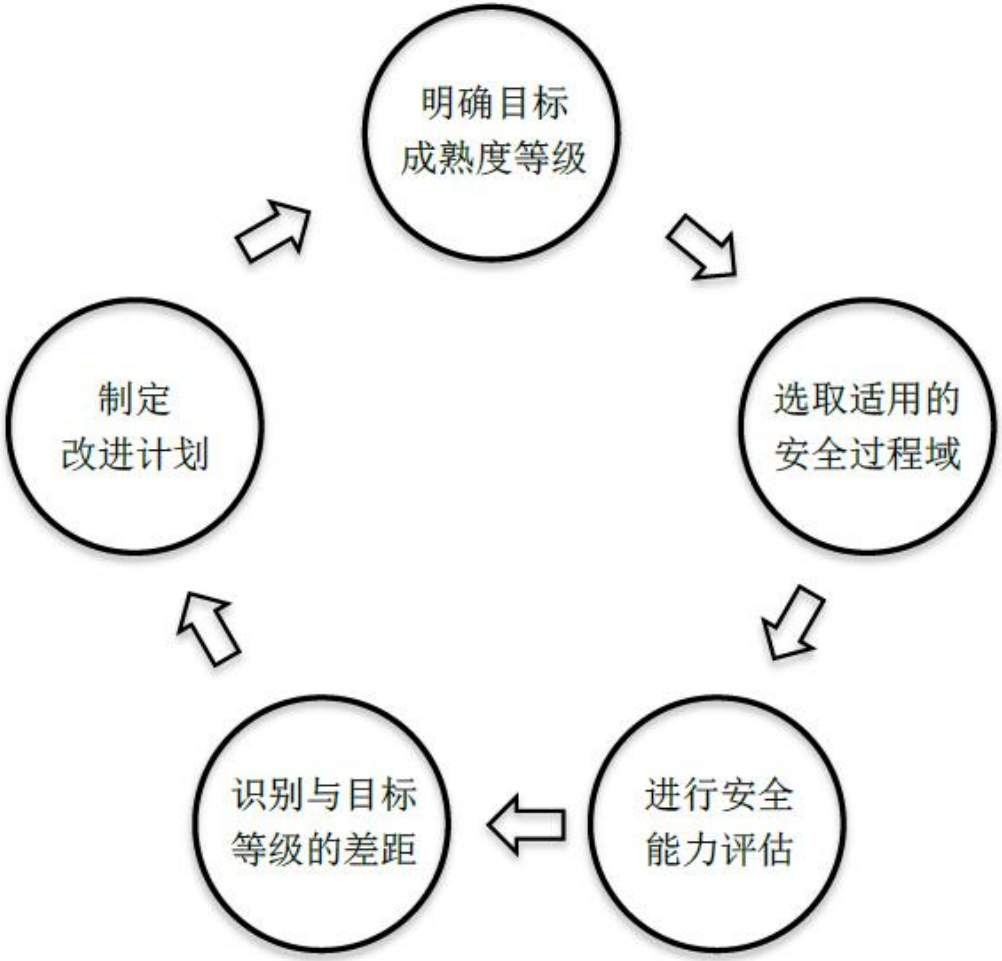
通用安全——PA27监控与审计

- 针对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，以保证对数据的访问和操作均得到有效的监控和审计，以实现对数据生命周期各阶段中可能存在的未授权访问、数据滥用、数据泄漏等安全风险的防控。

	组织建设	制度流程	技术工具	人员能力
等级1	–	–	–	–
等级2	业务部门负责	生命周期监控	日志审计告警	–
等级3	专职负责人员	操作日志监控	日志监控技术	了解数据范围 风险判断能力
等级4	–	–	统一日志监控 整理量化感知	–
等级5	–	–	日志大数据分析	–

数据安全成熟度评估实施

- 能力成熟度模型使用方法



数据安全成熟度评估实施

❖ 能力成熟度等级评估流程

确定模型适用范围	• 分析需要保护的数据资产及业务范围，确定模型使用或评估范围
确定能力成熟度级别目标	• 分析组织机构数据安全风险，确定能力成熟度等级建设目标
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（PA）
执行基本实践	• 依据标准对各等级数据安全基本实践（BP）要求，从四个关键能力进行落地和不断改进提升
过程域（PA）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
确定组织机构整体等级	• 结合所有过程域的等级，确定组织机构整体的数据安全能力成熟度等级，对数据安全能力进行持续建设和改进

数据安全成熟度评估实施

- 四个关键能力的评估方法
  - 1）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。
  - 2）制度流程：检查 是否有 关键数据安全领域的制度规范和流程 及其 在组织 机构 内的落地执行情况。
  - 3）技术工具：检查组织 机构 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。
  - 4）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。

数据安全成熟度评估实施

数据安全成熟度评估的手段

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，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等级的技术能力要求

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

数据安全成熟度评估的手段

数据安全成熟度评估实施

❖ 能力成熟度等级综合判定参考方法

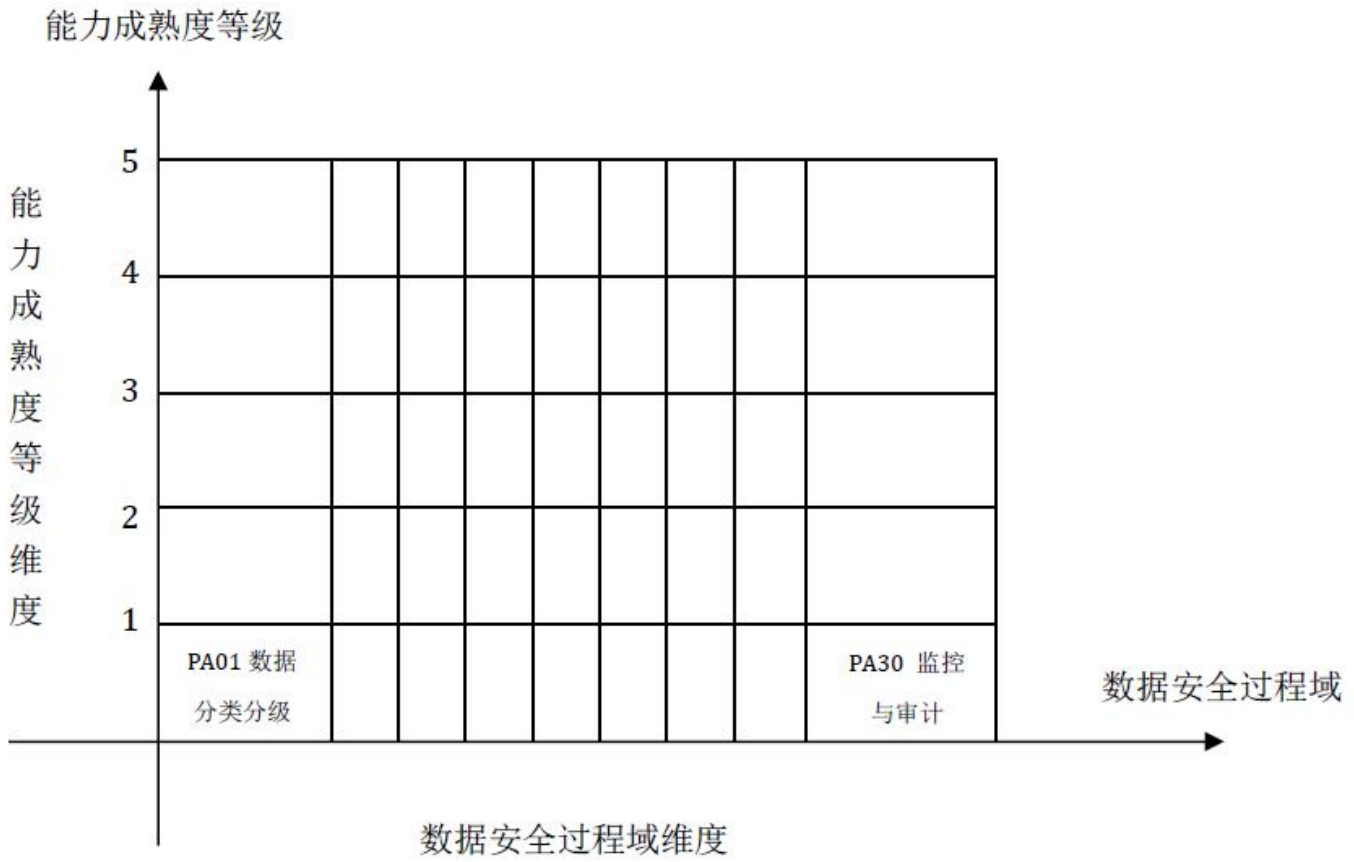
表B.1　过程域评估表

过程域	是否适用，如果不适用，给出说明	评估小结	评估等级	修正因子	修正后等级
PA（X）	是/否		1—5	0.8-1.2	1—5
…					
综合等级评定					1-5

1. 基于对组织机构业务场景和数据安全风险，可对数据生命周期各阶段安全（PA01-P23）进行适用性判断；
2. 基于数据安全行业专家经验和组织机构对某一过程域数据安全风险的接受程度，可对等级结果进行修订，修订因子不超过0.5-1.5区间范围，修正后向下取整；
3. 组织机构综合数据安全等级评定，可以采用“木桶原理”，即各过程域评级最低级别为最终级别。

数据安全成熟度评估实施

- 能力成熟度等级维度与数据安全过程域维度之间的映射关系



CISP

谢谢，请提问题！