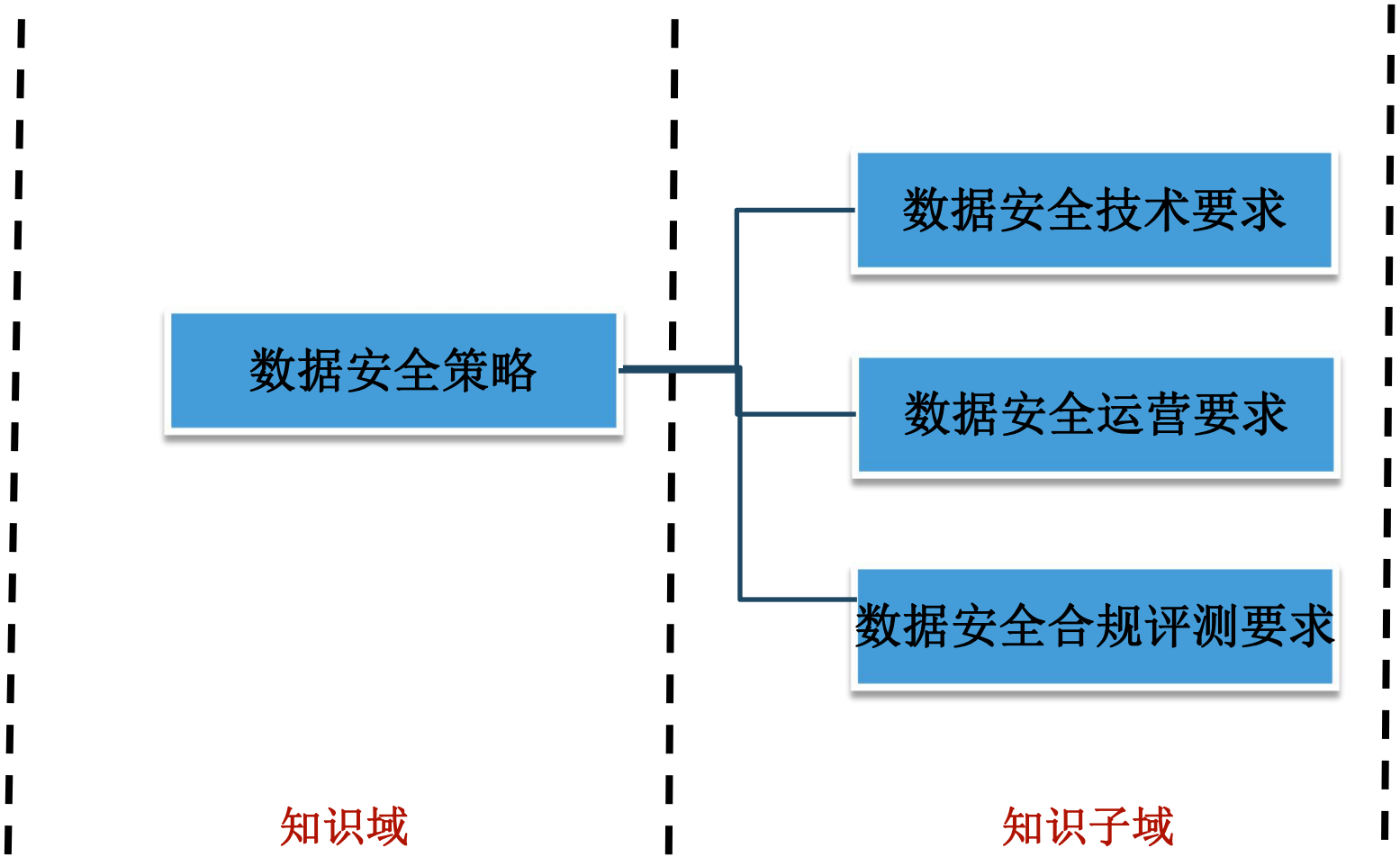
CISP-DSG 数据安全策略

版本：1.0

讲师姓名　　机构名称

课程内容



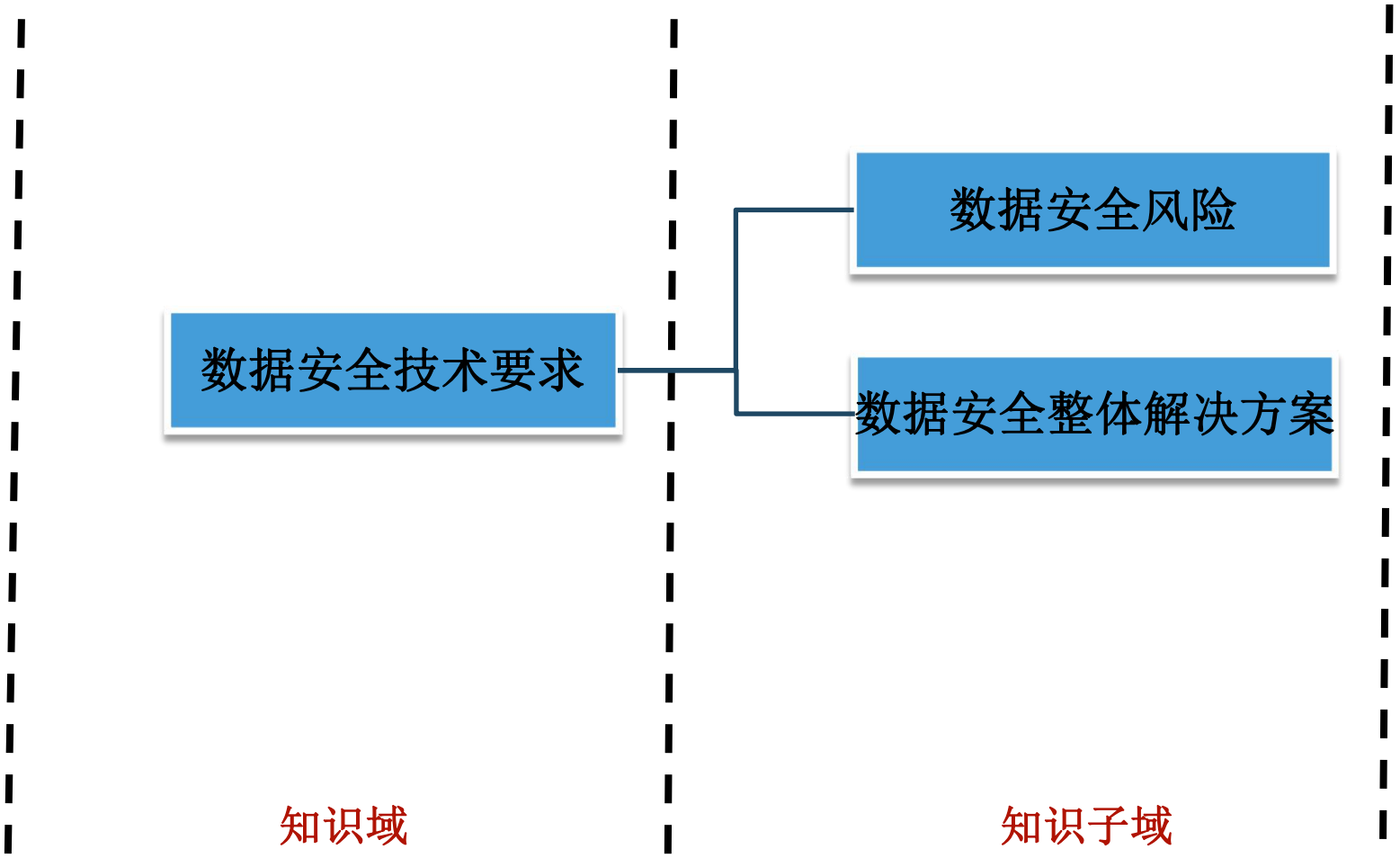
知识子域：数据安全技术要求

- 数据安全技术要求
  - 数据安全风险描述；
  - 了解数据安全技术的定义；
  - 理解数据安全技术的原理及实现；
  - 了解整体数据安全治理方案中数据安全技术的基本概念及对数据安全的作用。

数据安全技术的定义

- 数据安全技术的定义
  - “是指直接围绕数据的安全防护技术，主要是指数据的访问控制、数据防泄漏、加密、脱敏、身份鉴别、行为审计等”。数据安全技术根据数据类型的不同分为针对结构化数据的安全技术和针对非结构化的安全技术。

课程内容



数据安全风险

2017年3月，京东内部员工涉嫌窃取50亿条用户数据
原因：未采取访问权限、身份认证、数据利用的管理

2017年5月，永恒之蓝勒索病毒 WannaCry全球爆发
原因：利用WindowsSMB服务远程溢出漏洞（MS17-010），并搭载NSA制造“永恒之蓝”网络武器，在短短数小时内就发动数万次攻击，袭击了全球数十个国家，而后受害国家增至150多个。

2018年1月，僵尸网络HNS感染逾2万物联网设备（IP摄像机）
原因：僵尸网络HNS通过网络设备漏洞，对诱捕到的物联网设备进行Web开发，包括数据泄露、代码执行和对设备操作的干扰。

2018年8月，华住旗下多个连锁酒店开房信息泄露
原因：公司程序员将数据库连接方式及密码上传到GitHub导致。

数据安全风险–合规性

《中华人民共和国网络安全法》是为保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展制定。由全国人民代表大会常务委员会于2016年11月7日发布，自2017年6月1日起施行。

数据安全风险–合规性

《中华人民共和国网络安全法》

第二十一条 国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改。

第三十一条 国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。关键信息基础设施的具体范围和安全保护办法由国务院制定。

第四十条 网络运营者应当对其收集的用户信息严格保密，并建立健全用户信息保护制度。

第四十二条 网络运营者不得泄露、篡改、毁损其收集的个人信息；未经被收集者同意，不得向他人提供个人信息。但是，经过处理无法识别特定个人且不能复原的除外。

第四十五条 依法负有网络安全监督管理职责的部门及其工作人员，必须对在履行职责中知悉的个人信息、隐私和商业秘密严格保密，不得泄露、出售或者非法向他人提供。

第五十条 国家网信部门和有关部门依法履行网络信息安全监督管理职责，发现法律、行政法规禁止发布或者传输的信息的，应当要求网络运营者停止传输，采取消除等处置措施，保存有关记录；

数据安全风险–合规性

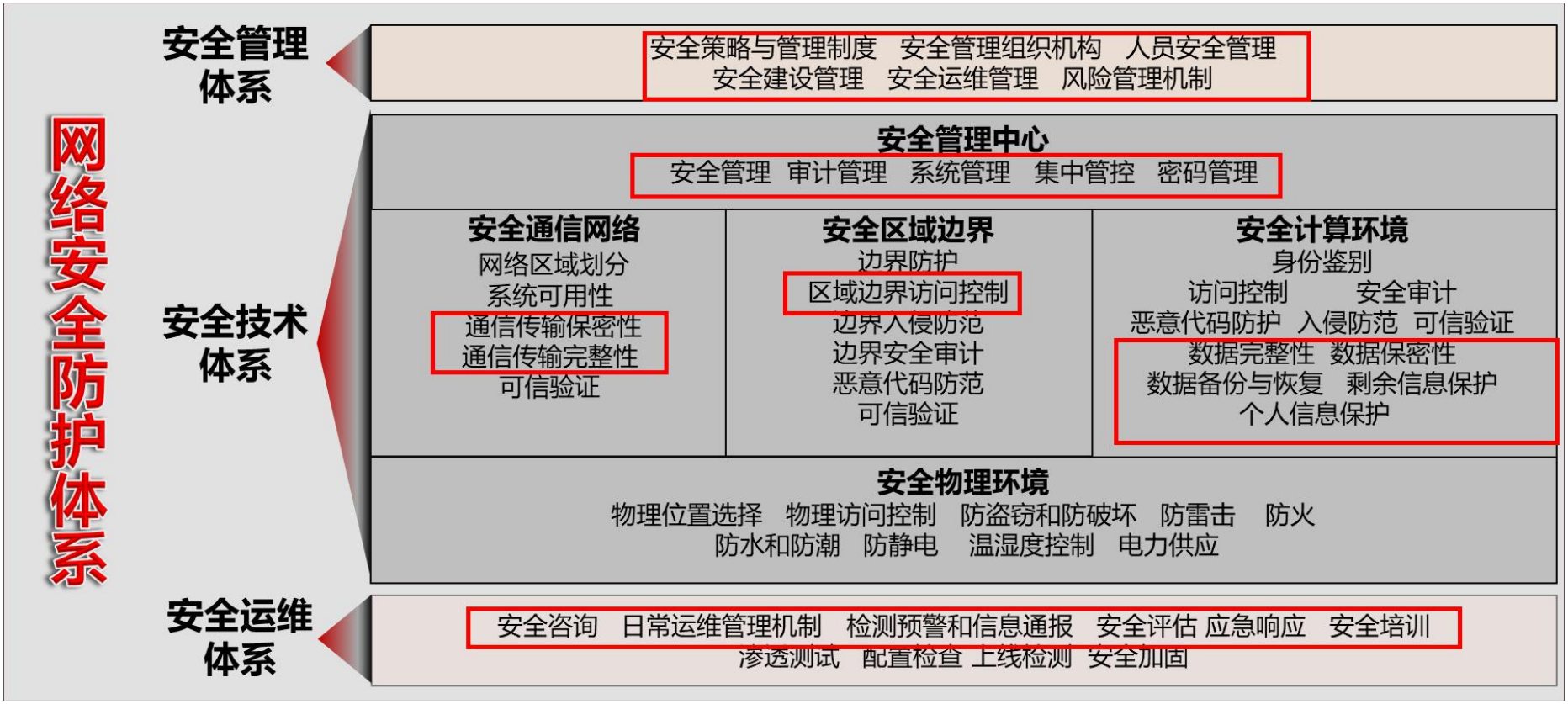
欧盟《通用数据保护条例》（简称GDPR）

最严苛

欧盟《通用数据保护条例》(GDPR)于2018年5月25日正式施行，旨在通过强调数据控制者的透明度、安全性和问责性来规范和加强欧洲公民的数据隐私权。这项新法律具有重大和广泛意义，为数据保护开创了新时代。GDPR扩大了个人控制其个人数据收集和处理方式的权利，并为组织制定了一系列新的义务，要求其更负责地保护个人隐私数据。

数据安全风险–合规性

等保2.0网络安全防护体系框架

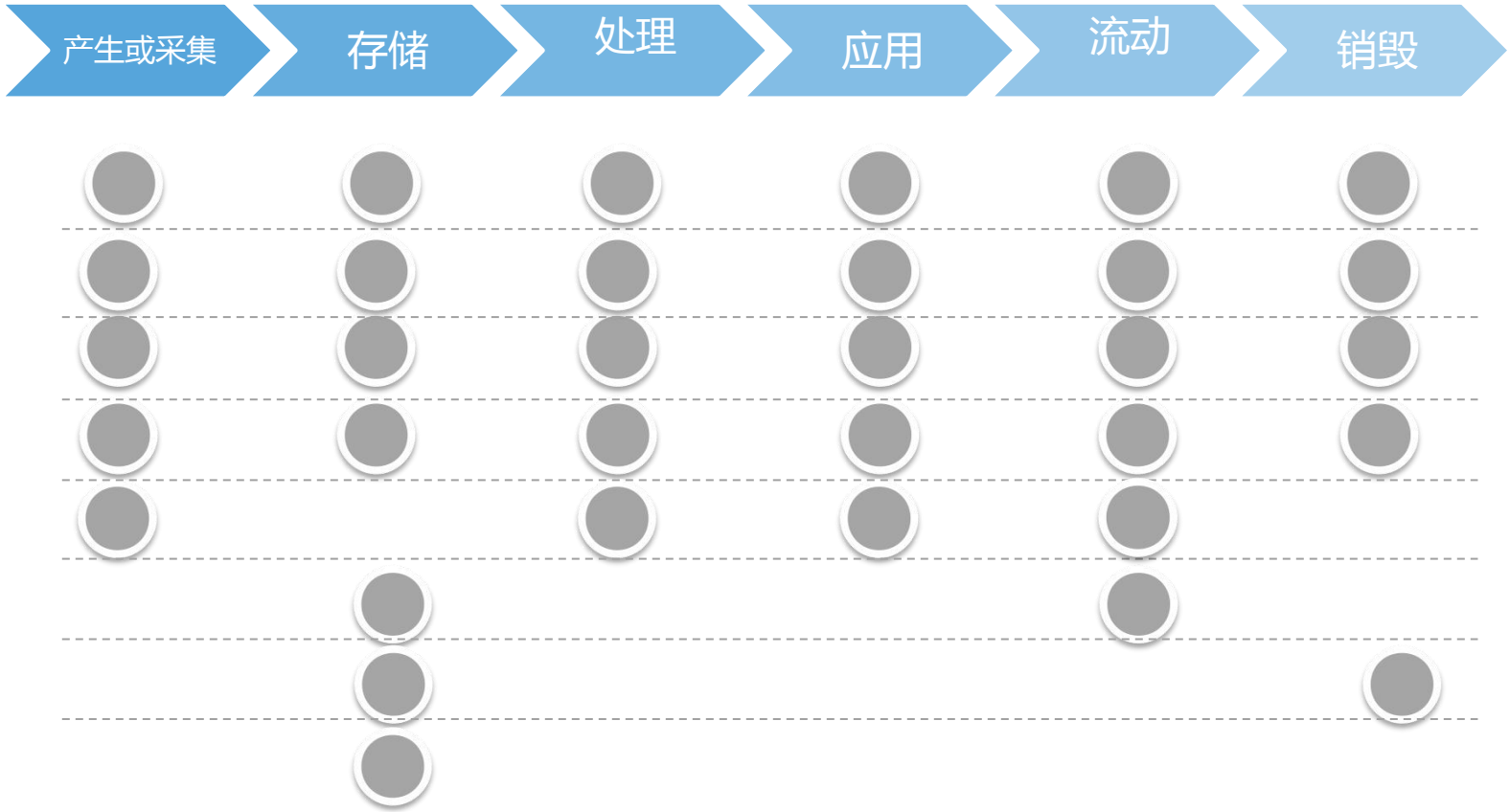


数据安全风险-需求

- 需要识别大量的，各种类型的复杂数据
- 在众多数据资产中确定关键、敏感数据
- 全面掌握数据所处生命周期状态及流动情况

- 以通用安全措施应对复杂的数据安全问题
- 在多变的数据使用场景保持统一的安全策略
- 数据安全面对高级的可持续攻击

数据安全风险-应对措施



数据安全整体解决方案-设计思路

数据安全整体解决方案-结构化数据

产生 → 存储 → 流转（内部） → 应用 → 流转（外部） → 销毁

数据脱敏
- ✓ 数据识别
- ✓ 数据变换

存储DLP
- ✓ 数据库扫描
- ✓ 自动分级分类

备份容灾
- ✓ 数据备份
- ✓ 数据恢复

数据库安全网关
- ✓ 访问控制
- ✓ 操作审计

应用DLP
- ✓ Web下载监控
- ✓ 文件泄漏阻断
- ✓ 页面泄漏脱敏
- ✓ 泄漏审计

终端DLP
- ✓ 终端监控
- ✓ 泄露阻断
- ✓ 泄露审计
- ✓ 文件扫描
- ✓ 安全擦除

网络DLP
- ✓ 网络监控
- ✓ 泄漏阻断
- ✓ 泄漏审计

存储DLP
- ✓ 文件扫描
- ✓ 安全擦除

数据安全交换云
- ✓ 数据导入
- ✓ 安全存储
- ✓ 备份冗灾
- ✓ 共享审核
- ✓ 数据导出

数据安全整体解决方案-非结构数据

终端DLP

- ✓ 文件监控
- ✓ 自动分级分类
- ✓ 智能加密
- ✓ 文件扫描
- ✓ 自动分级分类
- ✓ 智能加密

文档安全管理

- ✓ 线下权限控制
- ✓ 外发审核
- ✓ 域外权限控制
- ✓ 限次销毁

存储DLP

- ✓ 文件扫描
- ✓ 自动分级分类
- ✓ 智能加密

终端DLP

- ✓ 终端监控
- ✓ 泄露阻断
- ✓ 泄露审计
- ✓ 文件扫描
- ✓ 安全擦除

数据安全交换云

- ✓ 安全检查
- ✓ 安全存储
- ✓ 备份冗灾
- ✓ 使用权限设定
- ✓ 共享审核
- ✓ 线上权限控制
- ✓ 下载赋权

网络DLP

- ✓ 网络监控
- ✓ 泄漏阻断
- ✓ 泄漏审计

存储DLP

- ✓ 文件扫描
- ✓ 安全擦除

数据安全整体解决方案-大数据

采集 → 存储 → 处理 → 应用 → 流动 → 销毁

大数据安全网关

- 采集：
  - ✓ 授权许可
  - ✓ 访问控制
  - ✓ 安全审计
  - ✓ 溯源审计
  - ✓ 数据脱敏
- 存储：
  - ✓ 访问控制
  - ✓ 安全审计
  - ✓ 属地限制
  - ✓ 数据加密
- 处理：
  - ✓ 授权许可
  - ✓ 访问控制
  - ✓ 安全审计
  - ✓ 溯源审计
  - ✓ 属地限制
  - ✓ 数据脱敏
- 应用：
  - ✓ 授权许可
  - ✓ 访问控制
  - ✓ 安全审计
  - ✓ 溯源审计
  - ✓ 属地限制
  - ✓ 数据脱敏
- 流动：
  - ✓ 授权许可
  - ✓ 属地限制
- 销毁：
  - ✓ 授权许可
  - ✓ 安全审计
  - ✓ 安全擦除

终端DLP

- ✓ 终端监控
- ✓ 泄漏阻断
- ✓ 泄漏审计

备份系统

- ✓ 数据备份
- ✓ 数据恢复

服务DLP

- ✓ 接口监控
- ✓ 合规审计
- ✓ 泄漏审计

VPN

- ✓ 传输加密

网络DLP

- ✓ 网络监控
- ✓ 泄漏阻断
- ✓ 泄漏审计

备份系统

- ✓ 数据归档

数据安全整体解决方案-技术手段

深度内容数据识别技术

数据安全整体解决方案-技术手段

数据防泄漏技术

Step 1：看

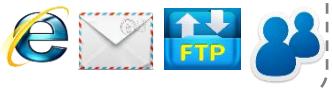
终端

网络

存储

使用中

传输中



存储中

- ✓ 9种终端通道
- ✓ 10+种主流网络协议
- ✓ 50+种主流应用
- ✓ 10+种主流服务器

Step 2：查

+86 136 8987 2019

- ✓ 1000+文件格式识别
- ✓ 5种指纹识别技术
- ✓ 机器智能识别技术
- ✓ 内置40+标识符
- ✓ OCR
- ✓ 10+种异常行为识别

Step 3：防

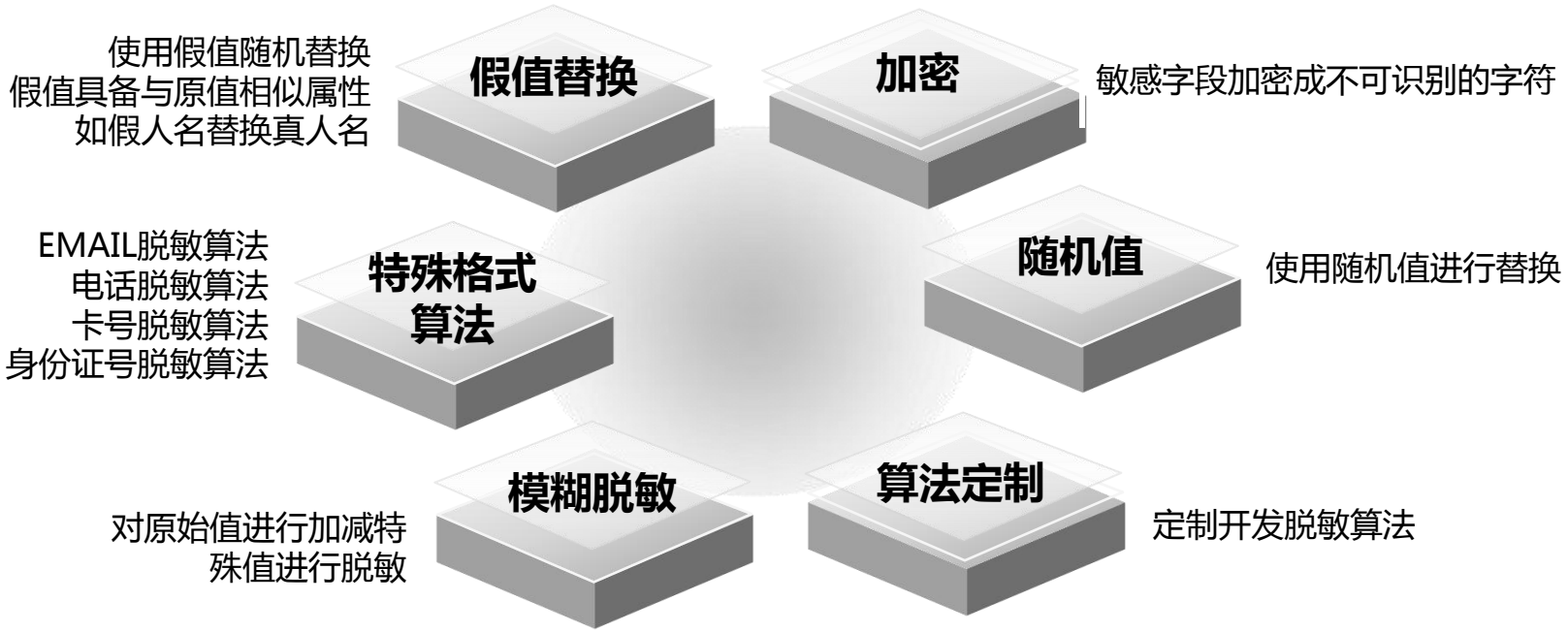
- ✓ 10+种防护手段
- ✓ 网络、存储、终端全面防护

Step 4：审

- ✓ 内置40+种报表
- ✓ 6种报表格式
- ✓ 任意定制报表内容
- ✓ 多种关联分析方法

数据安全整体解决方案-技术手段

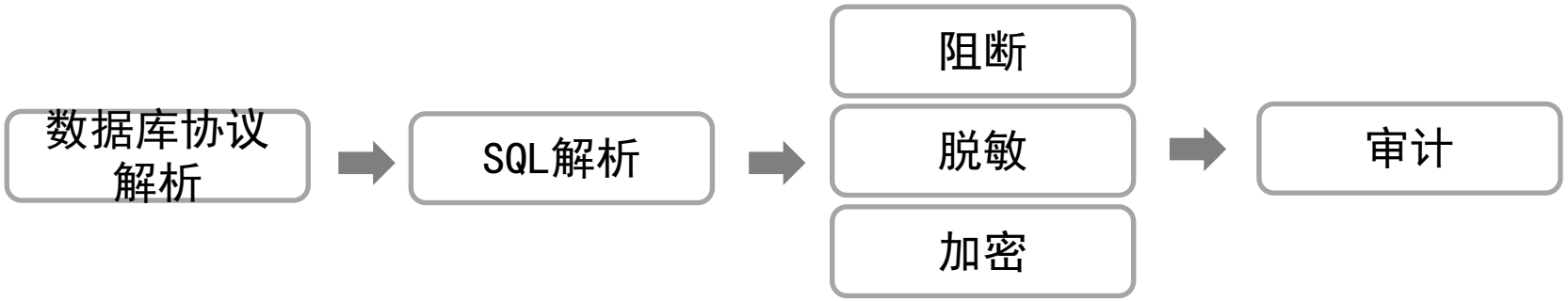
数据脱敏技术



符合《个人信息去标识化指南》要求

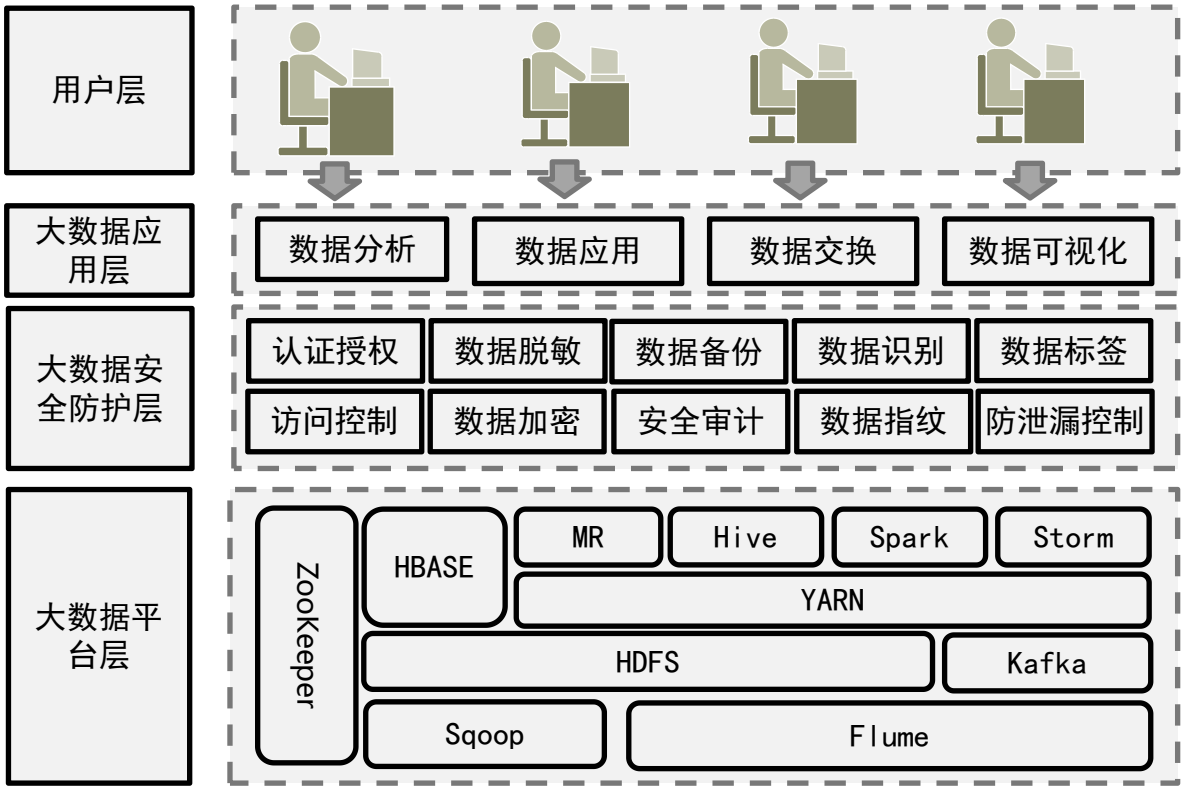
数据安全整体解决方案-技术手段

数据库安全防护技术



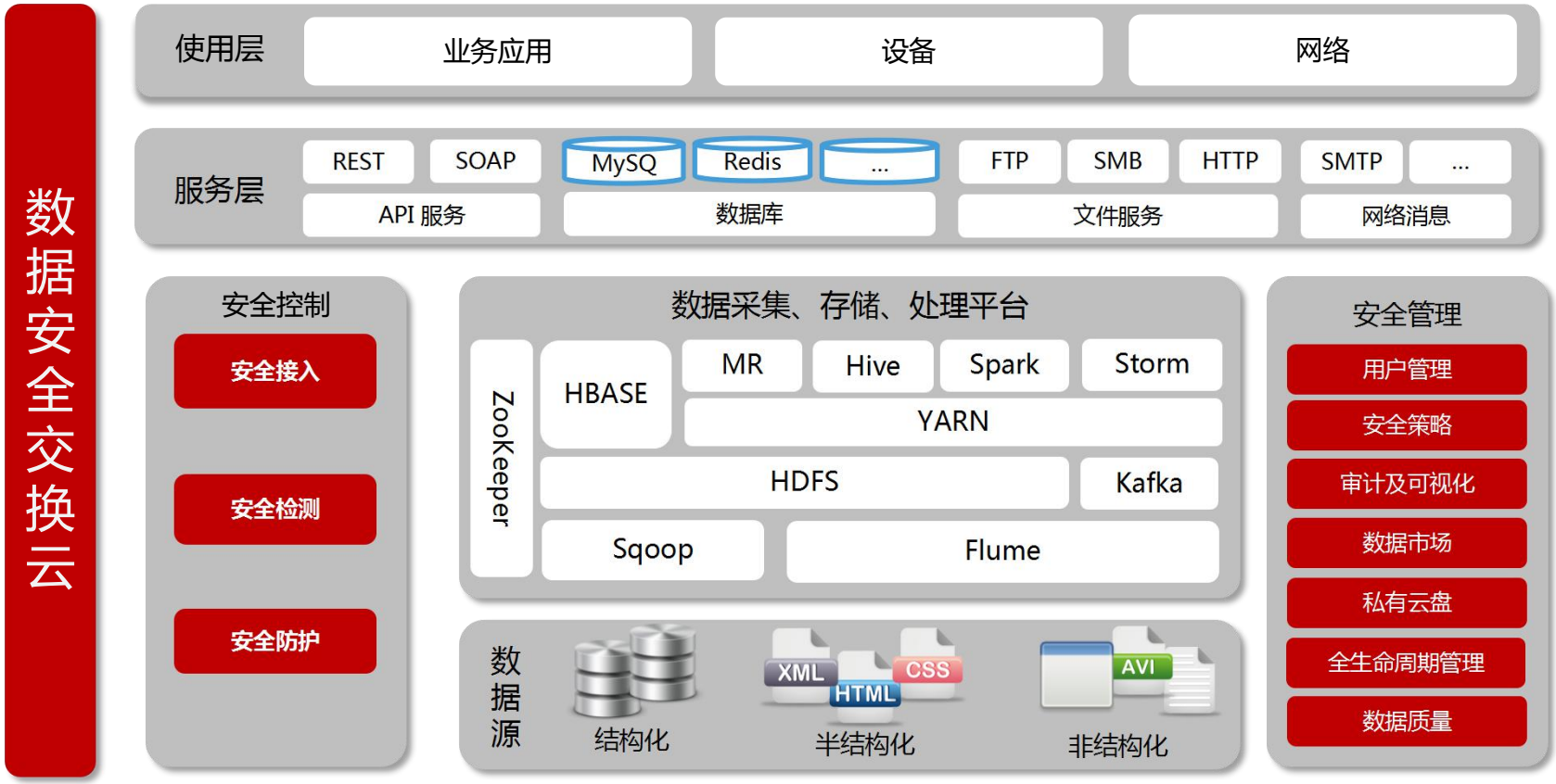
数据安全整体解决方案-技术手段

大数据安全防护技术



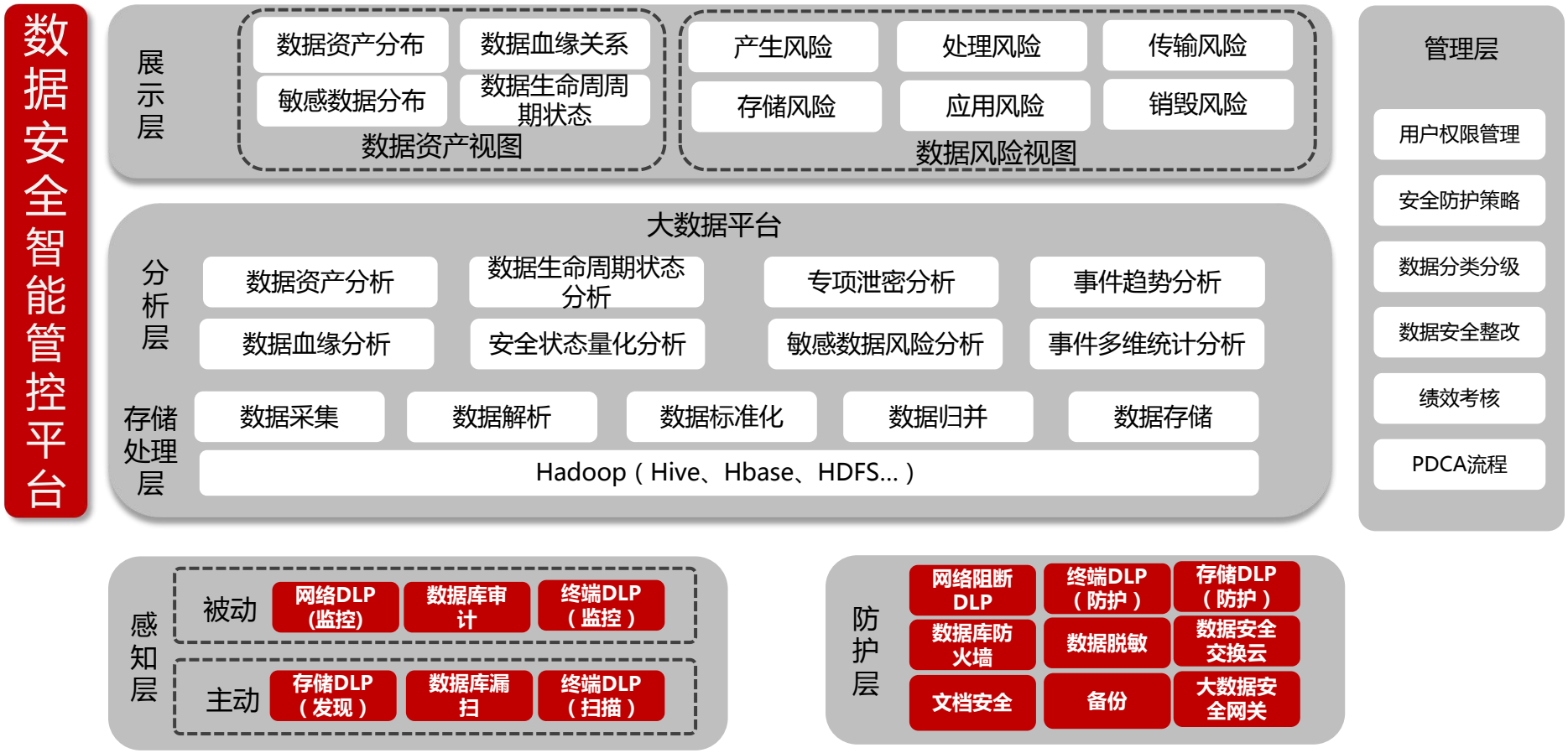
数据安全整体解决方案-技术手段

一体化数据安全交换技术



数据安全整体解决方案-技术手段

统一数据安全智能管控技术



数据安全整体解决方案-技术手段

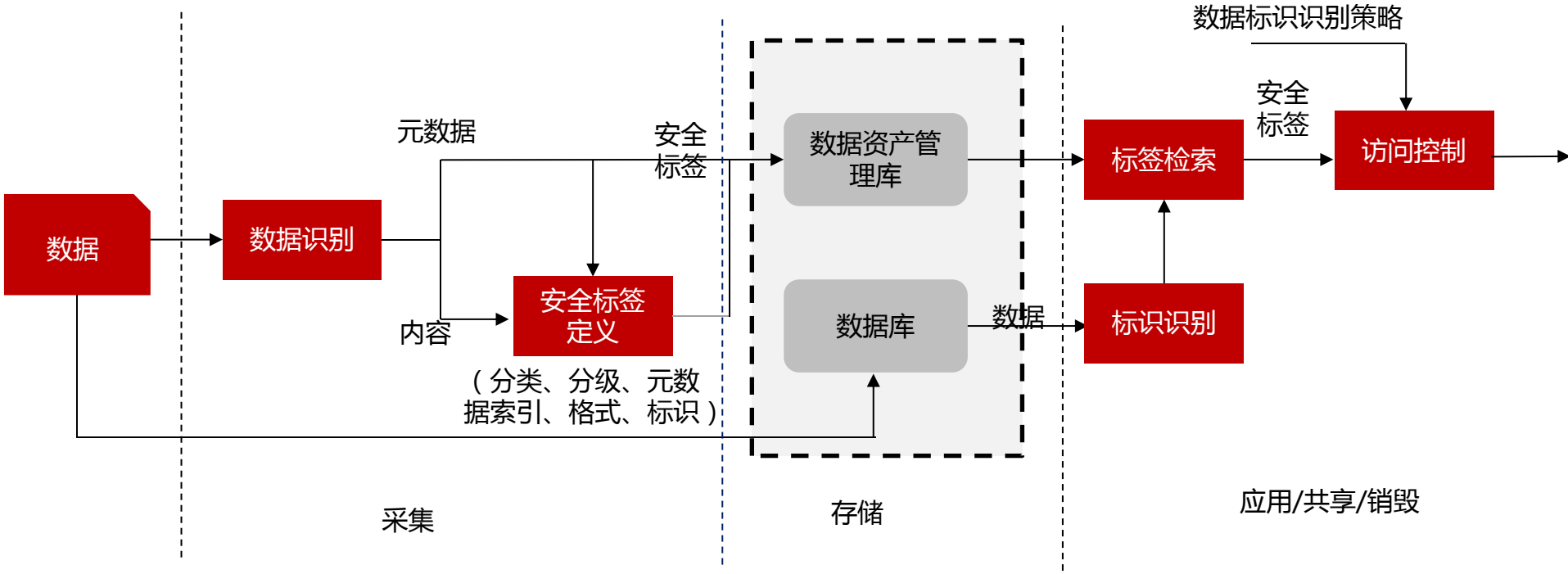
数据安全整体解决方案-技术手段

当数据所有者创建、分类和分级数据时，需要为数据分配标签。

数据所有者 基于角色	时间信息 创建、处理、销毁	机密等级	操作指导
传播发布	访问限制	数据源	合规要求 管辖权、法规

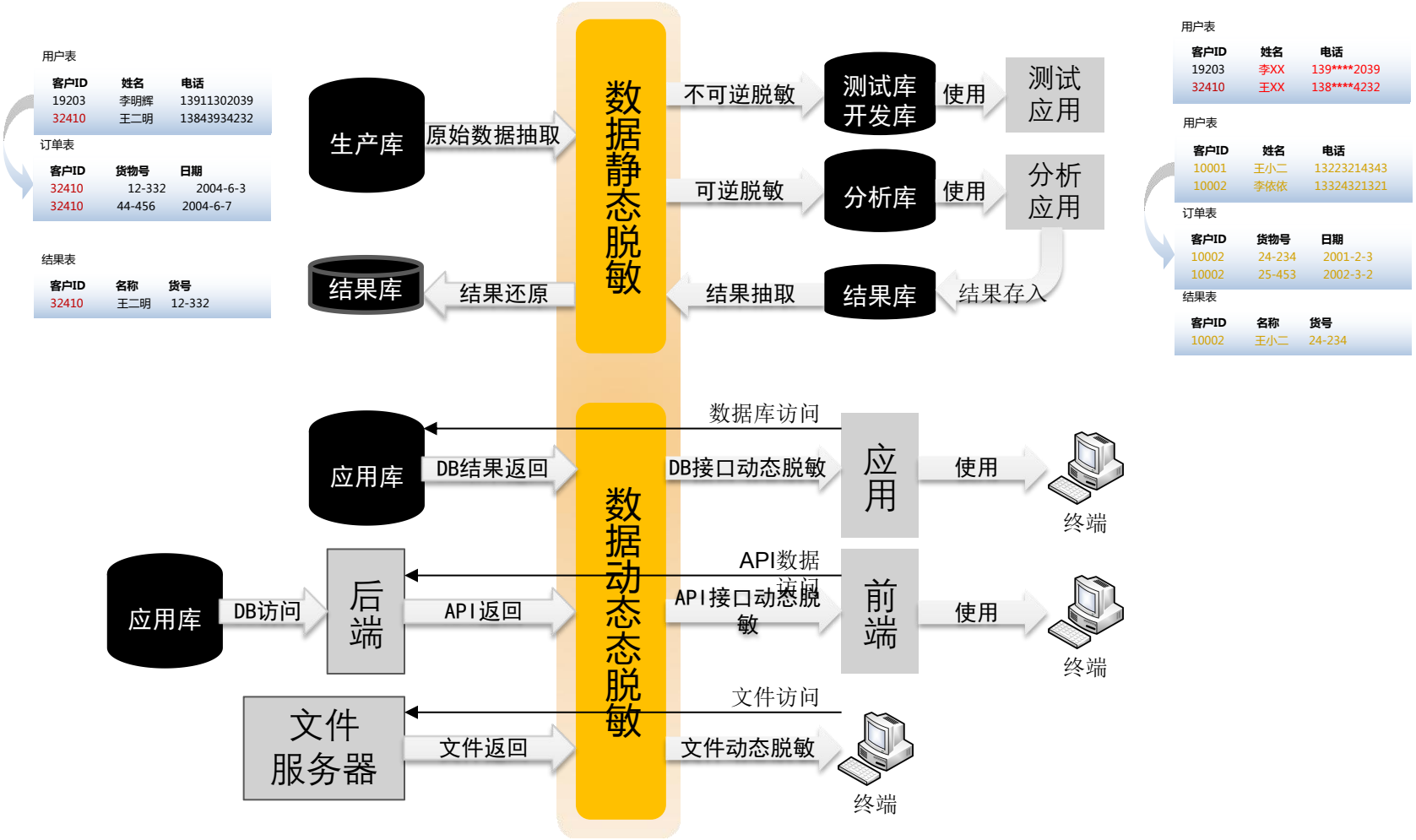
数据安全整体解决方案-技术手段

基于分类分级标识的访问控制策略

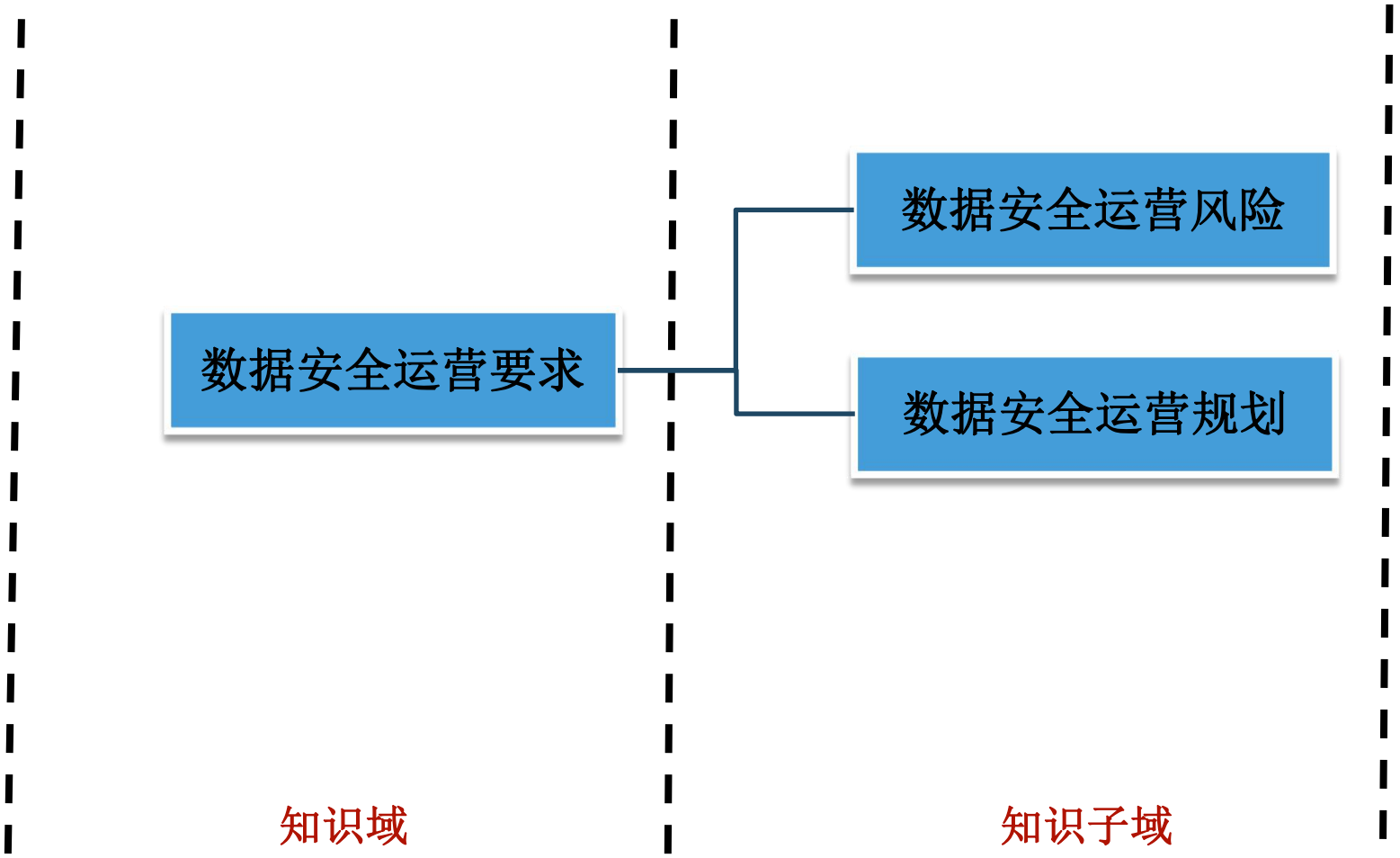


数据安全整体解决方案-技术手段

基于分类分级标识的访问控制策略



课程内容



数据安全运营风险

数据安全运营主要关注信息环境中数据风险的安全保护及控制，主要有如下关键主题：

维护弹性运营

- 涉及日常活动，组织需要关键业务具备弹性，当负面事件影响到组织的时候，运维人员需要确保减轻组织活动的破坏，余姚预计数据风险破坏并确保关键系统的部署和维护以保持连续性。运维人员需要确保实时监测和相应的维护流程。

保护有价值的数据资产

- 安全运营过程中需要提供对各种数据资源的日常维护，包含人力和虚拟数据资产，至少需要维持已被用于保护敏感和关键数据资源免于破坏的控制。

数据安全运营风险-数据存储风险

- 数据的存储解决了数据保存的问题。那么我们就需要考虑数据存储的风险。
- 数据丢失风险
- 数据存储访问风险
- 敏感数据泄露风险
- 数据随意使用风险

数据安全运营风险-数据存储防护

- 采用数据备份、数据归档等手段保障数据完整性
- 采用日志审计等手段对存储访问行为进行记录审计
- 采用敏感数据加密、脱敏手段解决敏感数据泄露
- 通过访问控制（账号管理、认证管理、授权管理、权限管理）降低数据滥用风险。

数据安全运营风险-数据处理风险

- 数据或数据库处理过程中需要了解的风险？
- 相关的数据策略及数据所有权是什么？
- 访问数据的权限及级别是否不同？
- 数据在处理中的法律问题？多用户访问权限？
- 敏感数据国际法律的不同等？

数据安全运营风险-数据处理防护

- 建立敏感数据标记、处理的过程。
- 分级分类数据的机密性、完整性、可用性分类
- 物理及逻辑控制
- 存储介质需要进行敏感标签，明确是否加密、联系人、保存时间等。
- 只有经过授权的人才可以访问数据，定义相关的策略、流程、步骤。

数据安全运营风险-数据共享风险

- 数据或数据库共享过程中遇到的风险？
- 权限管理是否有越权行为？
- 数据流向是否有追踪溯源？
- 多用户访问权限管理？
- 共享数据范围界定？
- 数据使用是否安全？
- 敏感数据违规传输？

数据安全运营风险-数据共享防护

- 采用共享审核机制保证安全共享
- 数据共享过程中采用细粒度华权限控制
- 数据传输采用内容检查
- 数据冗余及数据备份
- 数据标签追踪溯源
- 日志审计及记录

数据安全运营风险-数据销毁风险

- 是否明确数据存储的期限？
- 是否及时清理超过生命周期的数据？

数据安全运营风险-数据销毁防护

- 制定数据使用生命周期。
- 定期清理超过期限数据
- 采用技术手段进行销毁，例如软擦除、物理销毁等。

数据安全运营规划-数据运营制度

- 建立数据运营制度。对在数据的生命周期的过程中进行操作使用制度。主要任务是建立、鉴权和完善数据安全运行环境。确保业务系统中各类信息数据的安全、可靠及完整，防止违规操作，避免因误操作而导致数据丢失、数据损坏、数据泄漏等行为。保证发生故障时能够及时发现、及时纠正、及时恢复。

数据安全运营规划-数据运营制度

- 上机运行系统的规定：
- 1. 系统管理员、系统操作员、系统维护员、数据录入员及经系统管理员批准的有关人员有权上机操作。
- 2. 非指定人员不能上机运行系统。
- 3. 商机人员必须使用其真实身份，操作密码注意保密，一旦出现问题，操作人员和系统管理人员有不可推卸的责任。
- 4. 上机人员必须按照各自的操作权限进入，不得越权，上机人员操作完毕后，必须退出系统。
- 5. 应及时做好各自的备份工作，以防意外事故发生。

数据安全运营规划-数据运营制度

- 上机使用人员职责和权限
- 1. 系统管理员
- 2. 系统维护人员
- 3. 系统操作人员
- 4. 数据录入人员
- 5. 数据审核人员
- 6. 业务审计人员
- 7. 档案管理人员

数据安全运营规划-数据运营制度

- 运营保障制度
- 1. 建立硬件、网络、系统及应用日常数据位数流程机制。
- 2. 建立故障应急处理流程机制。
- 3. 建立数据保护保障机制
- 4. 建立版本管理机制

数据安全运营规划-数据运营制度

- 故障处理相应及要求
- 1. 一般故障
- 2. 次要故障
- 3. 重大故障

数据安全运营规划-数据运营制度

- 安全要求制度
- 1. 定期对系统进行风险评估
- 2. 对信息系统进行7*24小时安全检测，发现问题及时记录并处理
- 3. 每周至少一日信息系统安全巡检。

数据安全运营规划-数据安全管控

产生/采集

识别、审计

存储

扫描、加密、隔离、
审计、脱敏、备份

处理

访问控制、加密、
隔离、审计、脱敏

应用

识别、访问控制、
阻断、告警、审计、脱敏

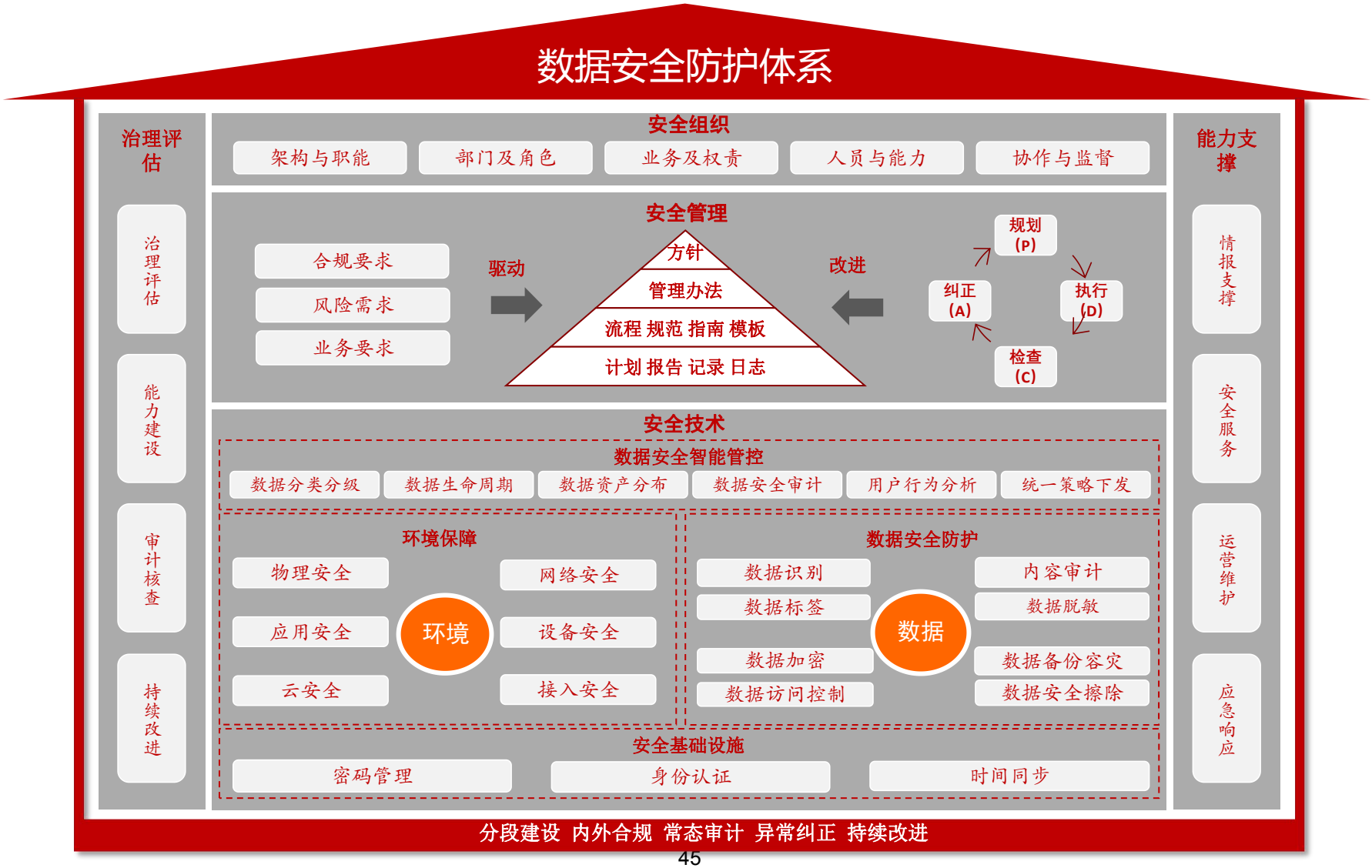
流动、传输、共享

阻断、告警、审计、脱敏

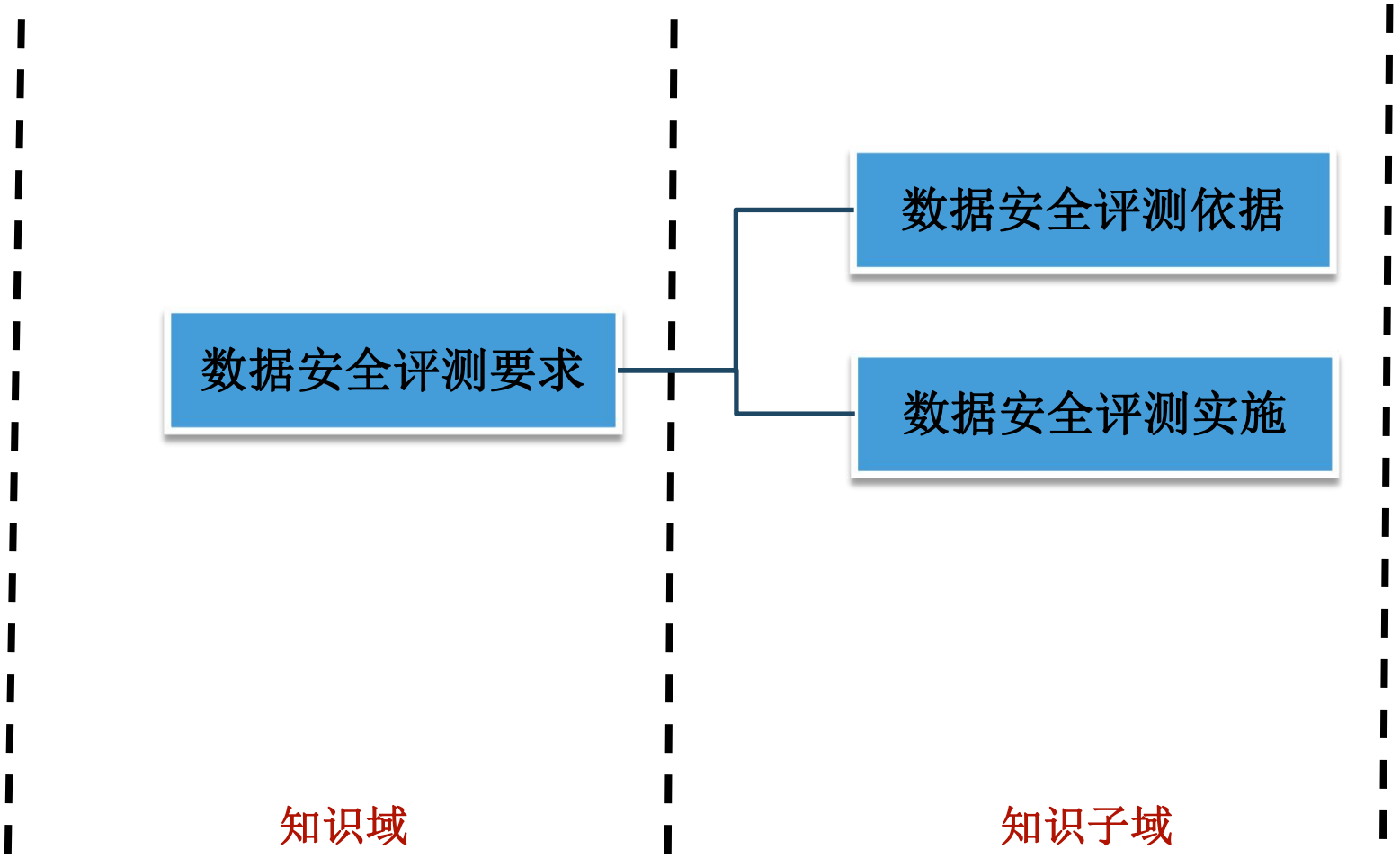
销毁

安全擦除、审计

数据安全运营规划-以数据为中心建设



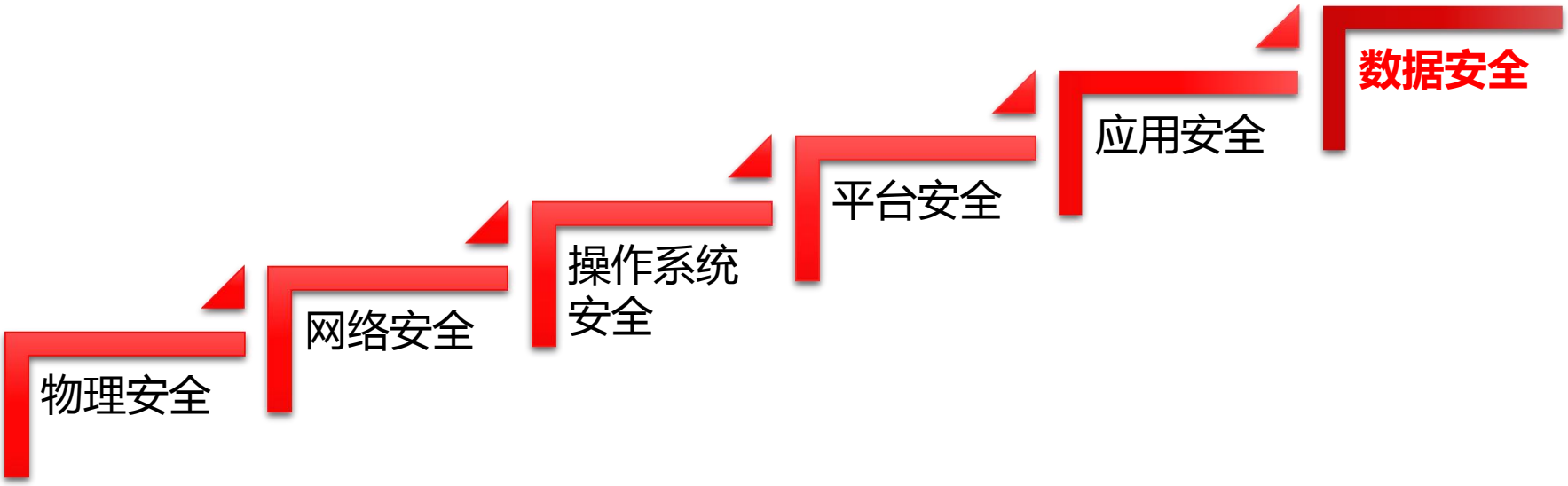
课程内容



数据安全评测依据–合规性依据

《中华人民共和国网络安全法》

网络安全，是指通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。



数据安全评测依据–合规性依据

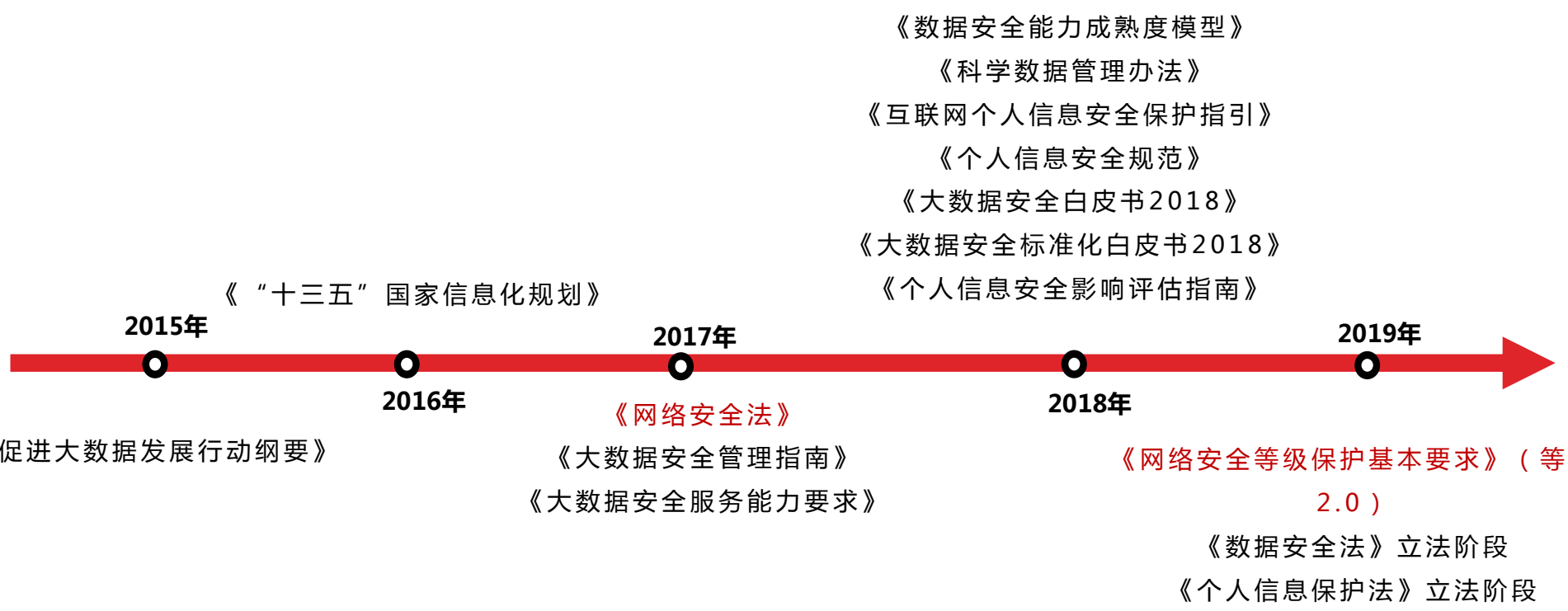
网络安全法

第二十一条	第三十一条	第四十条	第四十二条	第四十五条	第五十条
•国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，**防止网络数据泄露或者被窃取、篡改**。	•国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者**数据泄露**，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。关键信息基础设施的具体范围和安全保护办法由国务院制定。	•网络运营者应当对其收集的**用户信息严格保密**，并建立健全用户信息保护制度。	•网络运营者不得**泄露、篡改、毁损**其收集的个人信息；未经被收集者同意，不得向他人提供个人信息。但是，经过处理无法识别特定个人且不能复原的除外。	•依法负有网络安全监督管理职责的部门及其工作人员，必须对在履行职责中知悉的**个人信息、隐私和商业秘密严格保密**，不得泄露、出售或者非法向他人提供。	•国家网信部门和有关部门依法履行网络信息安全监督管理职责，发现法律、行政法规禁止发布或者传输的信息的，应当要求网络运营者**停止传输**，采取**消除**等处置措施，保存有关记录。

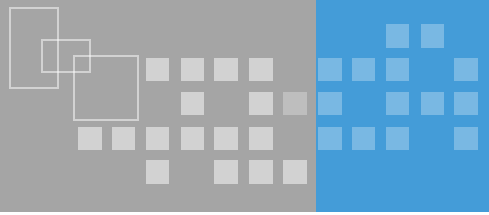
谁主管谁负责、谁运行谁负责、谁使用谁负责

数据安全评测依据–合规性依据

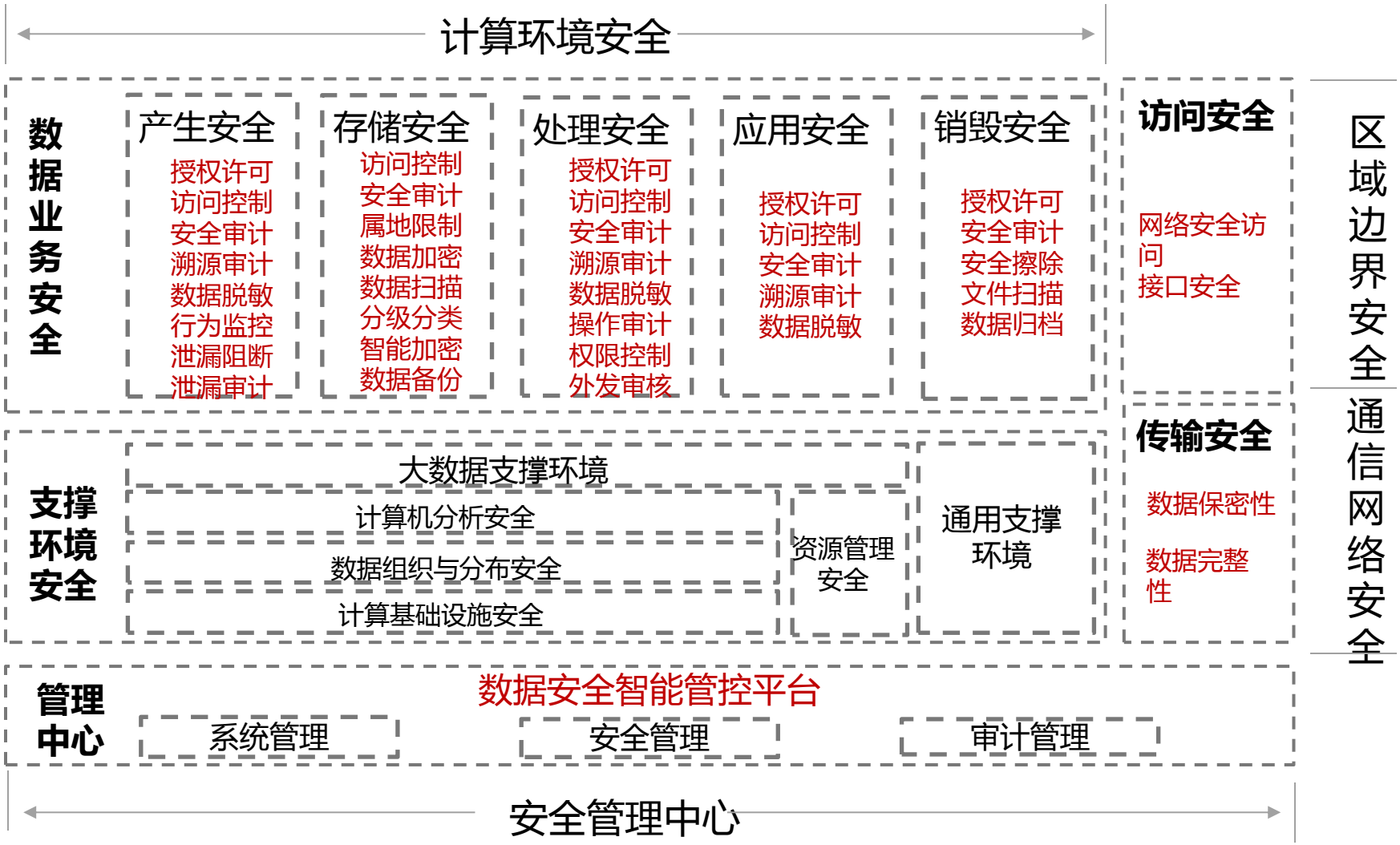
国家法律政策指引



数据安全评测依据-合规性依据



等保2.0

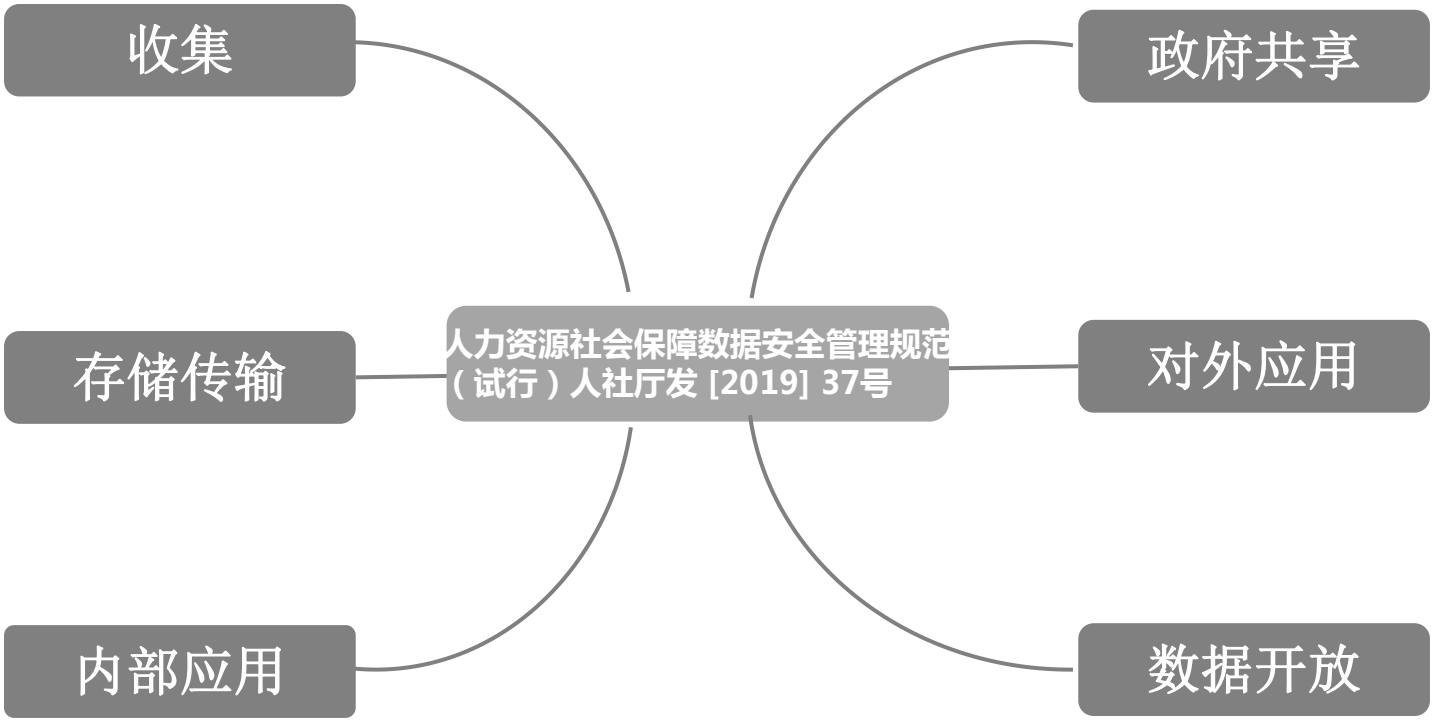


数据安全评测依据–合规性依据

《中国人民银行网络数据安全管理指南》[2019] 7号

数据分级标准	数据安全治理	数据全生命周期防护	数据安全运营
A、B、C、D、E	管理、标记、认证、授权、审计、培训	收集、存储、使用、披露、备份、归档、删除、销毁	监测、检查、评估、审计、应急

数据安全评测依据–合规性依据



数据安全评测依据-技术依据

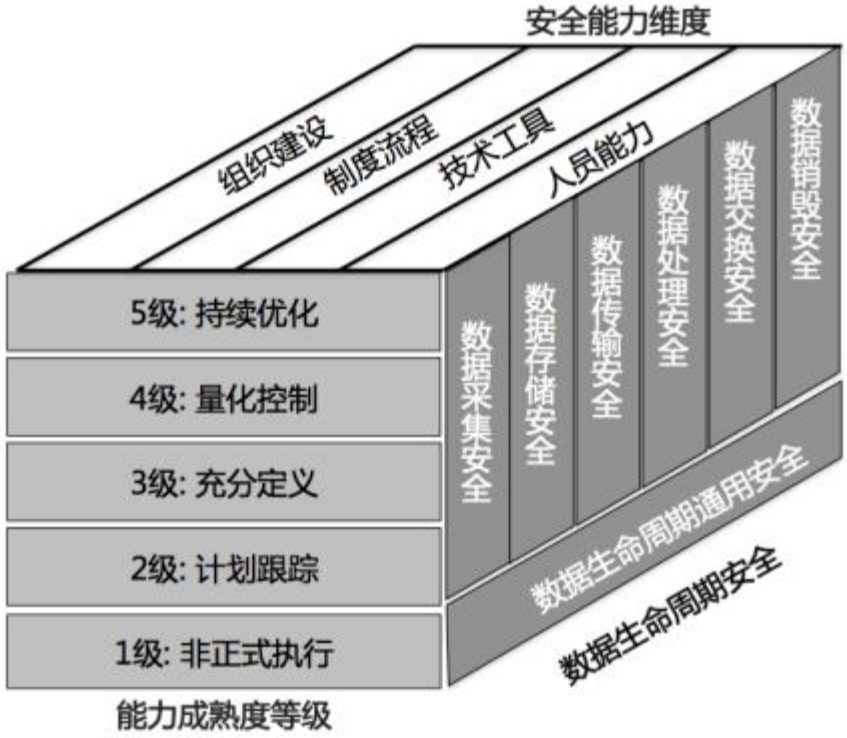


图1　数据安全能力成熟度模型架构

数据安全评测依据-技术依据

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2所示。

图3 数据安全过程域体系

CISP

谢谢，请提问题！