

大数据安全标准解读 与测评实践

公安部信息安全等级保护评估中心 赵泰



大数据等级保护对象



大数据的定级



大数据的安全保护



大数据基本要求



大数据测评

大数据等级保护对象

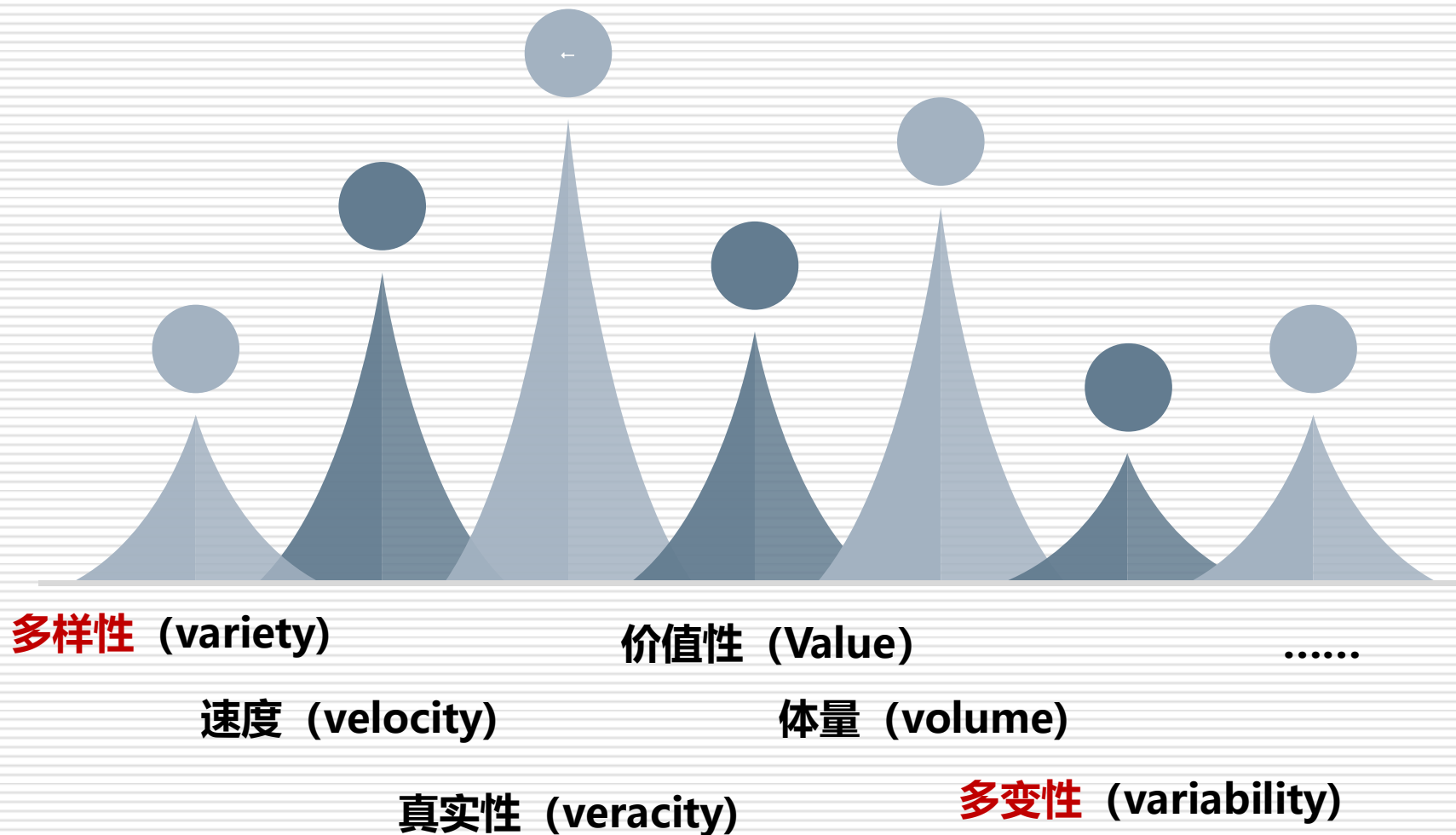


具有V特征的数据资源

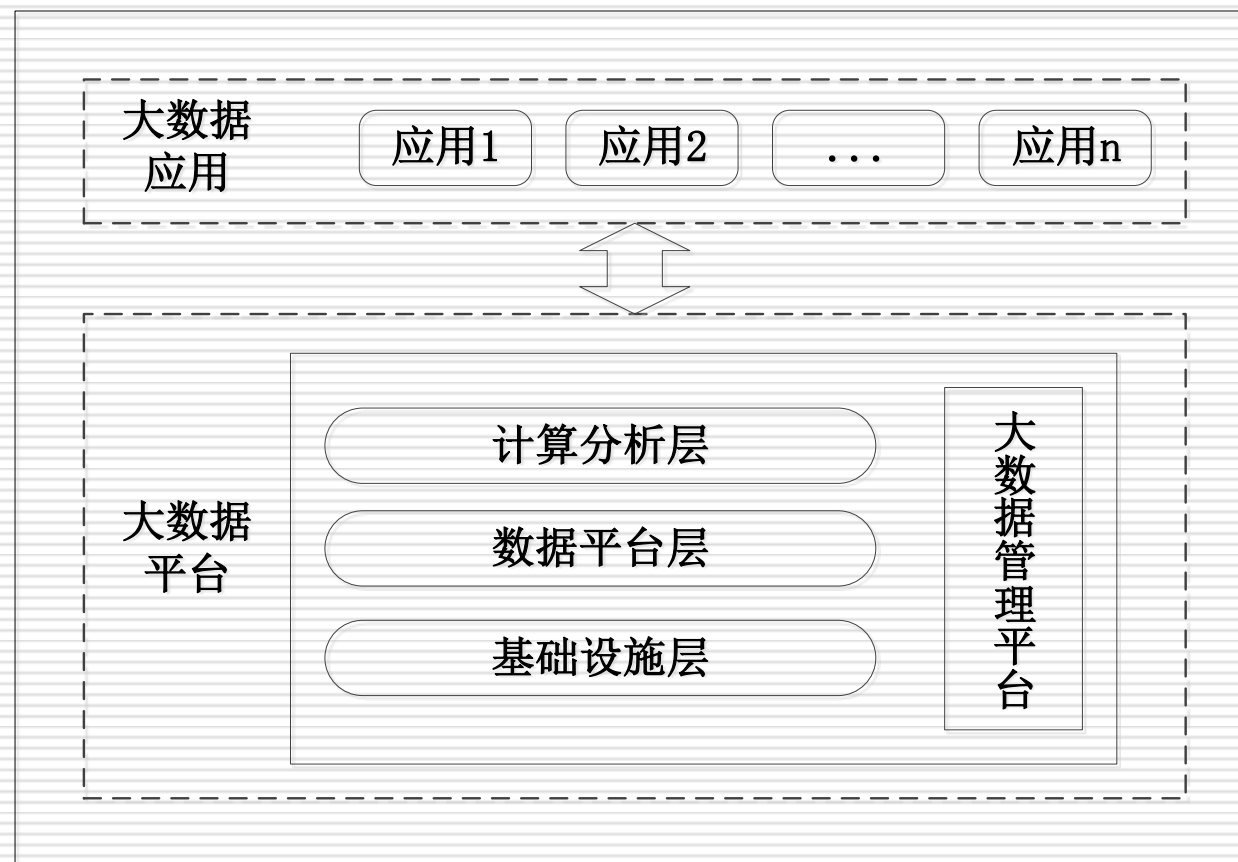







新的数据处理模式

大数据等级保护对象



大数据等级保护对象



-  **大数据等级保护对象**
-  **大数据的定级**
-  **大数据的安全保护**
-  **大数据基本要求**
-  **大数据测评**

大数据的安全保护等级

业务信息	业务信息安全被破坏时所侵害的客体	对相应客体的侵害程度		
		一般损害	严重损害	特别严重损害
	公民、法人和其他组织的合法权益	---	第二级	第三级
	社会秩序、公共利益	第二级	第三级	第四级
	国家安全	第三级	第四级	第五级

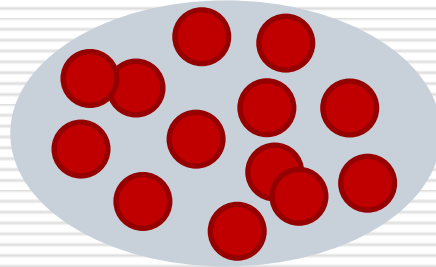
系统服务	系统服务安全被破坏时所侵害的客体	对相应客体的侵害程度		
		一般损害	严重损害	特别严重损害
	公民、法人和其他组织的合法权益	第一级	第二级	第三级
	社会秩序、公共利益	第二级	第三级	第四级
	国家安全	第三级	第四级	第五级

大数据的定级

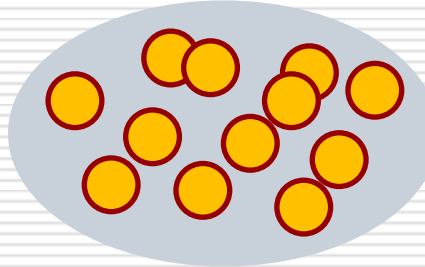
- **数据资源可单独定级**
- **当安全责任主体相同，大数据、大数据平台和应用可作为一个整体对象定级**

数据资源的定级

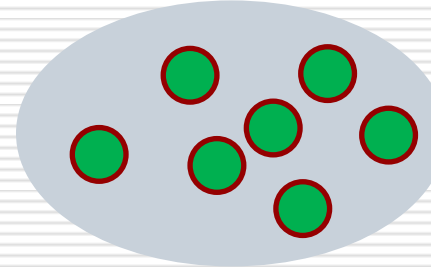
业务系统



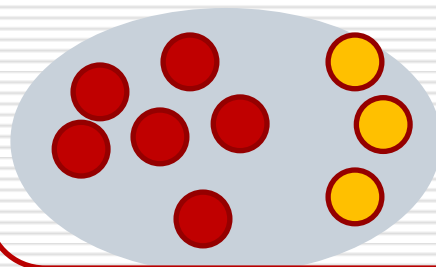
业务系统



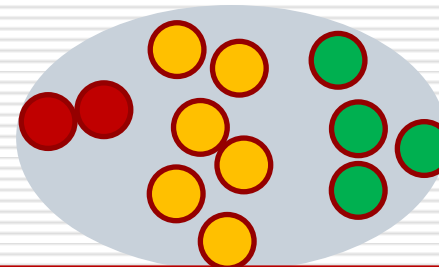
业务系统



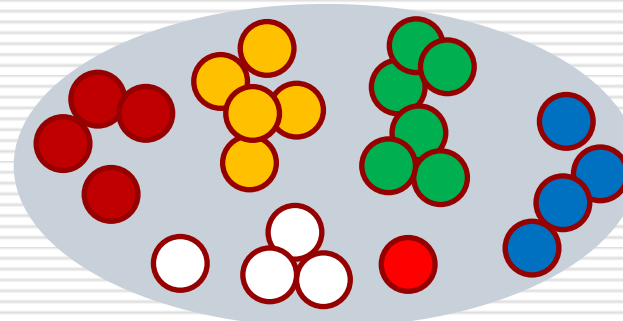
大数据应用



大数据应用



大数据应用



大数据系统的定级

组件

责任主体

大数据

数据所有者

大数据应用

大数据应用服务提供者

大数据平台

大数据平台服务提供者

基础设施






基础设施提供者

组件单独或组合可以构成定级对象，当涉及不同责任主体时，应当分别定级。

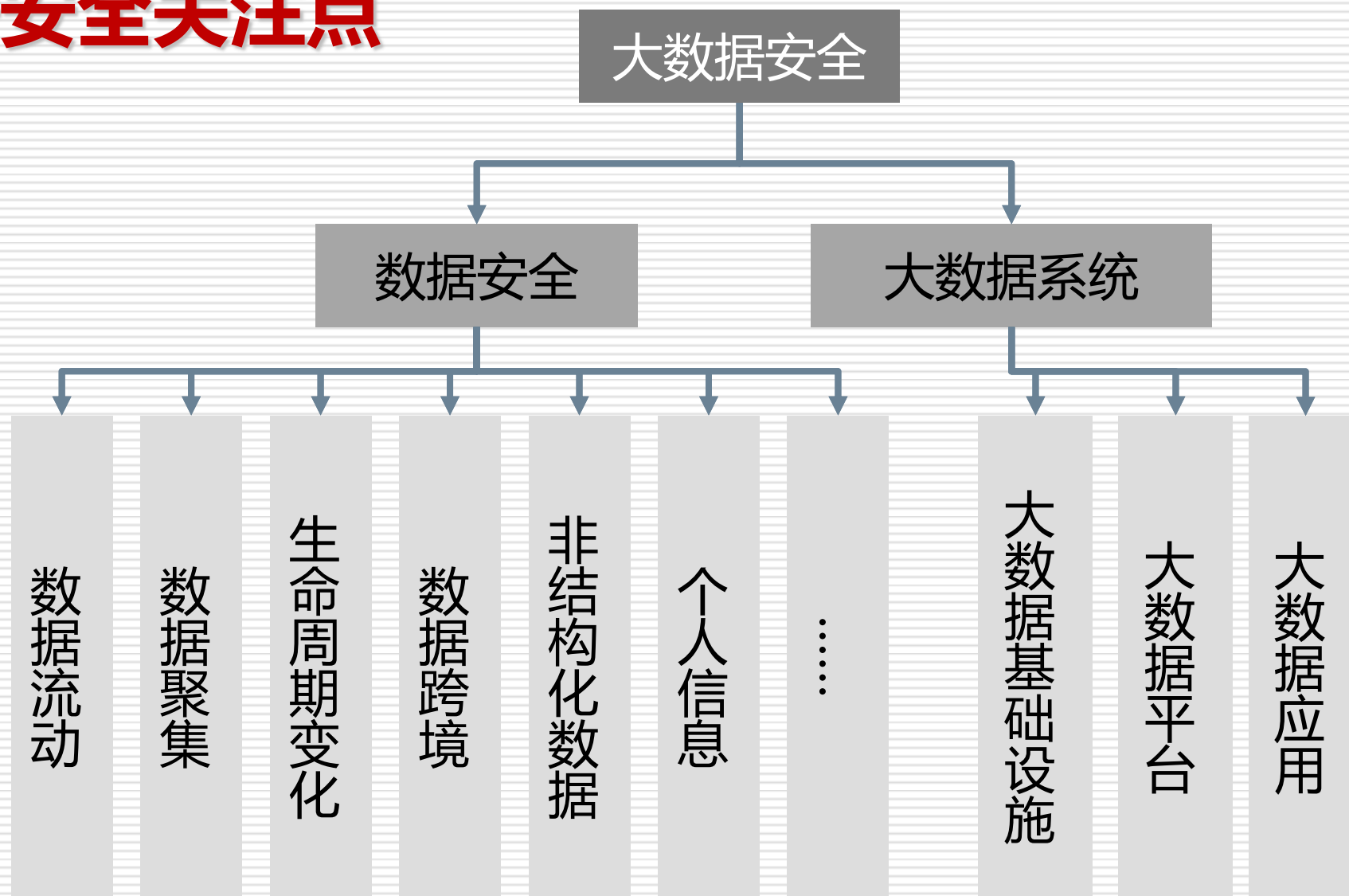
大数据的定级

大数据基础设施、大数据平台、大数据应用的安全保护等级**一般**由其所**承载、处理或产生的大数据的信息安全保护等级**决定。

如果大数据基础设施、大数据平台、大数据应用为不同的定级对象，下层定级对象的安全保护等级应**不低于**其承载的上层定级对象的等级。

-  **大数据等级保护对象**
-  **大数据的定级**
-  **大数据的安全保护**
-  **大数据基本要求**
-  **大数据测评**

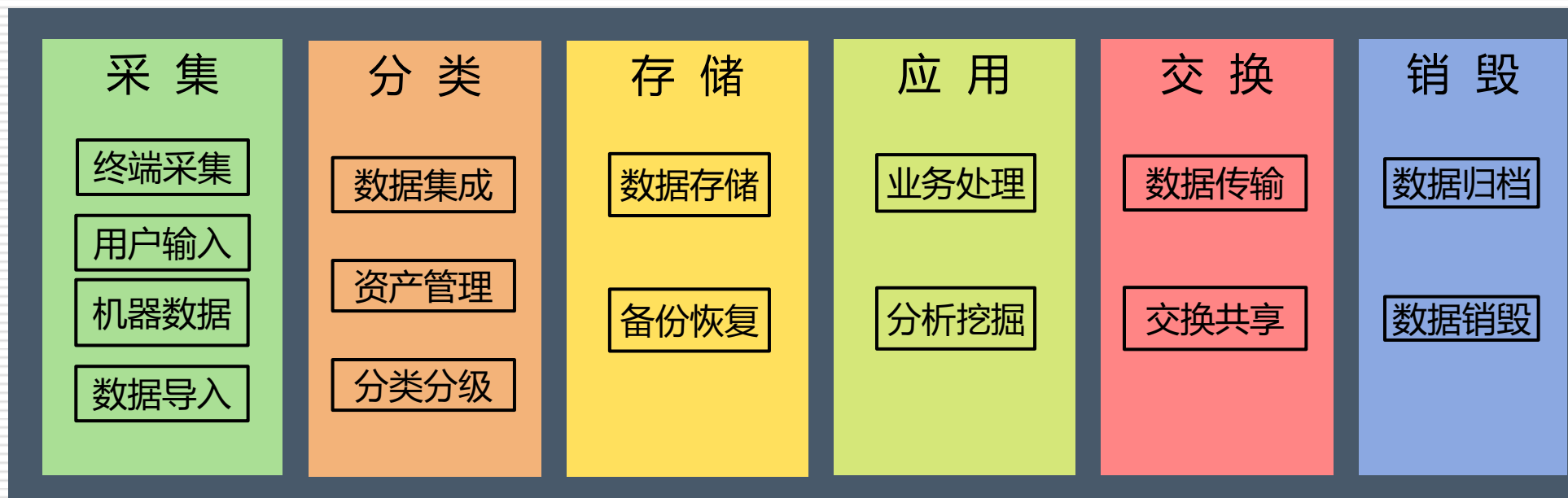
大数据安全关注点



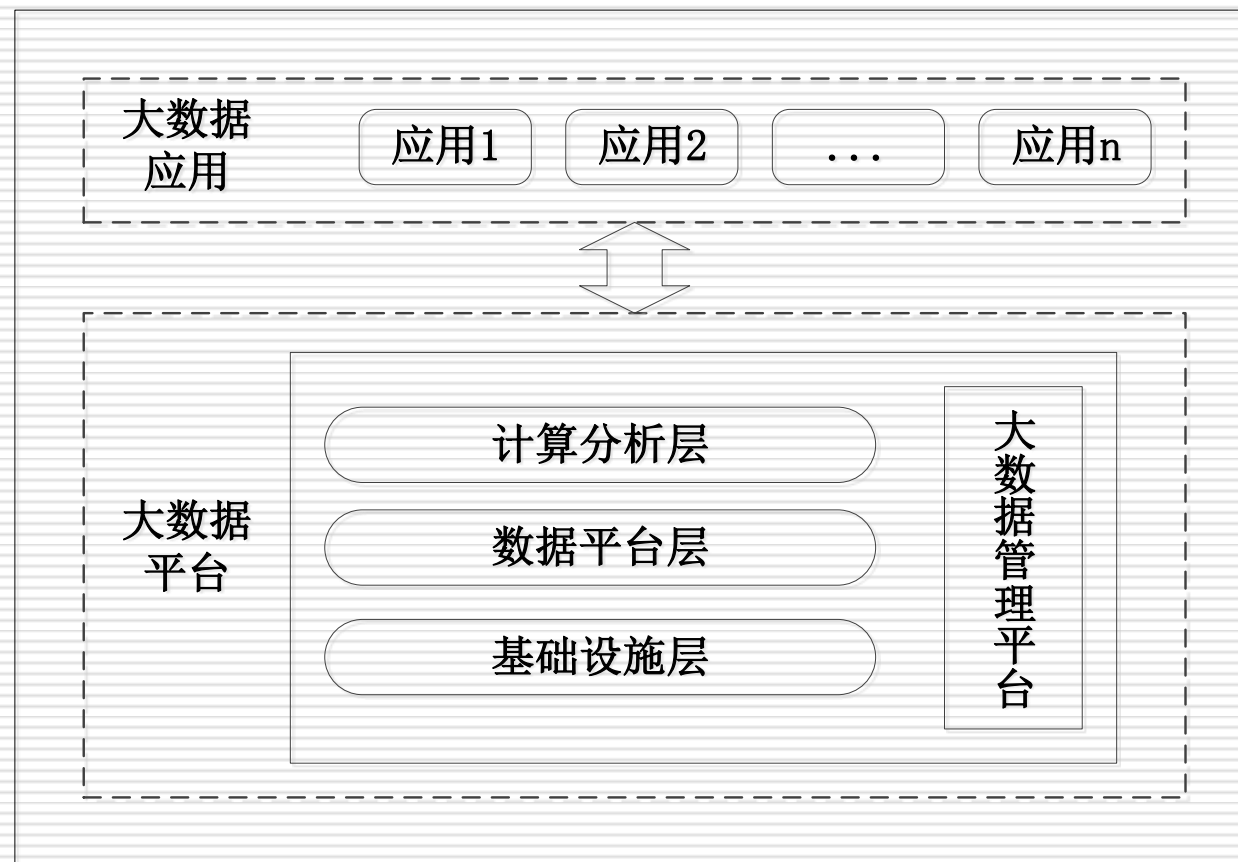
大数据安全的特点

- ◆ 关注大数据生命周期
- ◆ 关注生态角色职责
- ◆ 关注数据流动的安全

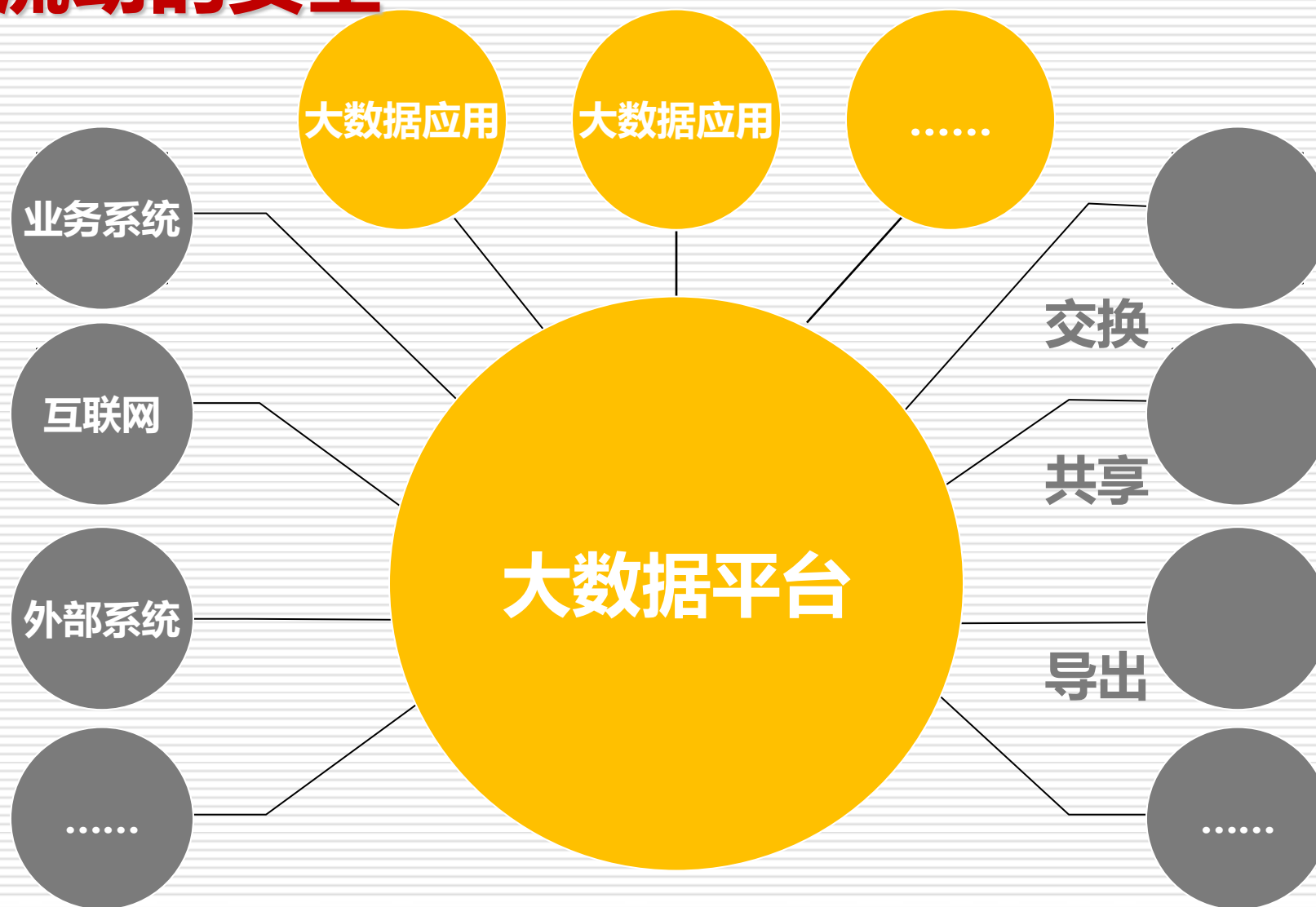
数据生命周期的安全








生态角色职责



数据流动的安全



-  **大数据等级保护对象**
-  **大数据的定级**
-  **大数据的安全保护**
-  **大数据基本要求**
-  **大数据测评**

大数据基本要求

附录 H（资料性附录）大数据应用场景说明

H.1 大数据概述

▷ H.2 第一级可参考安全控制措施

▷ H.3 第二级可参考安全控制措施

▲ H.4 第三级可参考安全控制措施

H.4.1 安全物理环境

H.4.2 安全通信网络

H.4.3 安全计算环境

H.4.4 安全建设管理

H.4.5 安全运维管理

▷ H.5 第四级可参考安全控制措施

大数据基本要求-物理环境

- 第一级：无要求
- 第二级：设备机房位于中国境内
- 第三级：与第二级要求相同
- 第四级：与第二级要求相同

大数据基本要求-通信网络

- 第一级：要求平台不承载高于其安全保护等级的大数据应用
- 第二级：与第一级要求相同
- 第三级：在第一级基础上，增加管理流量与系统业务流量分离的要求
- 第四级：与第三级要求相同

大数据基本要求-计算环境

- 第一级：要求对终端和组件进行身份鉴别
- 第二级：在第一级基础上，增加管理大数据应用、平台服务组件，屏蔽故障资源，提供脱敏和去标识化工具/组件，以及授权使用大数据应用资源的要求
- 第三级：在第二级基础上，增加数据分类分级保护，设置安全标记，接口调用实施访问控制，数据资源隔离的要求
- 第四级：在第三级基础上，增加对不同类别、不同级别数据全生命周期区分处置的能力

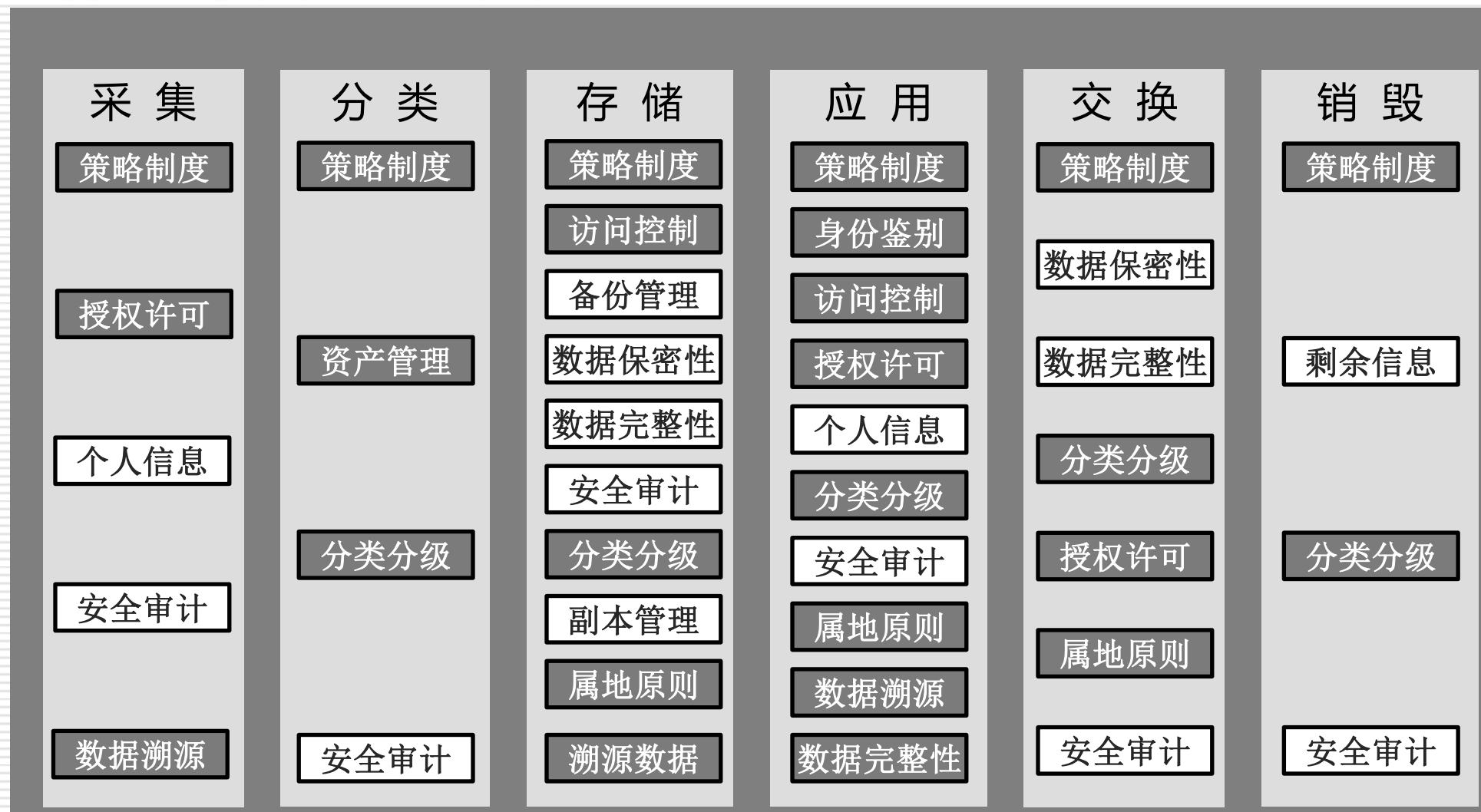
大数据基本要求-安全建设

- 第一级：选择大数据平台的要求
- 第二级：在第一级基础上，增加约定平台提供商权限和职责的要求
- 第三级：在第二级基础上，增加数据交换、共享双方对数据保护责任的要求
- 第四级：与第三级要求相同

大数据基本要求-安全运维

- 第一级：无要求
- 第二级：要求建立数字资产安全管理策略
- 第三级：在第二级基础上，增加数据分类分级保护的策略，重要数字资产的范围确定和相关使用流程，数据类别和级别评审和变更的要求
- 第四级：与第三级要求相同

数据生命周期的安全

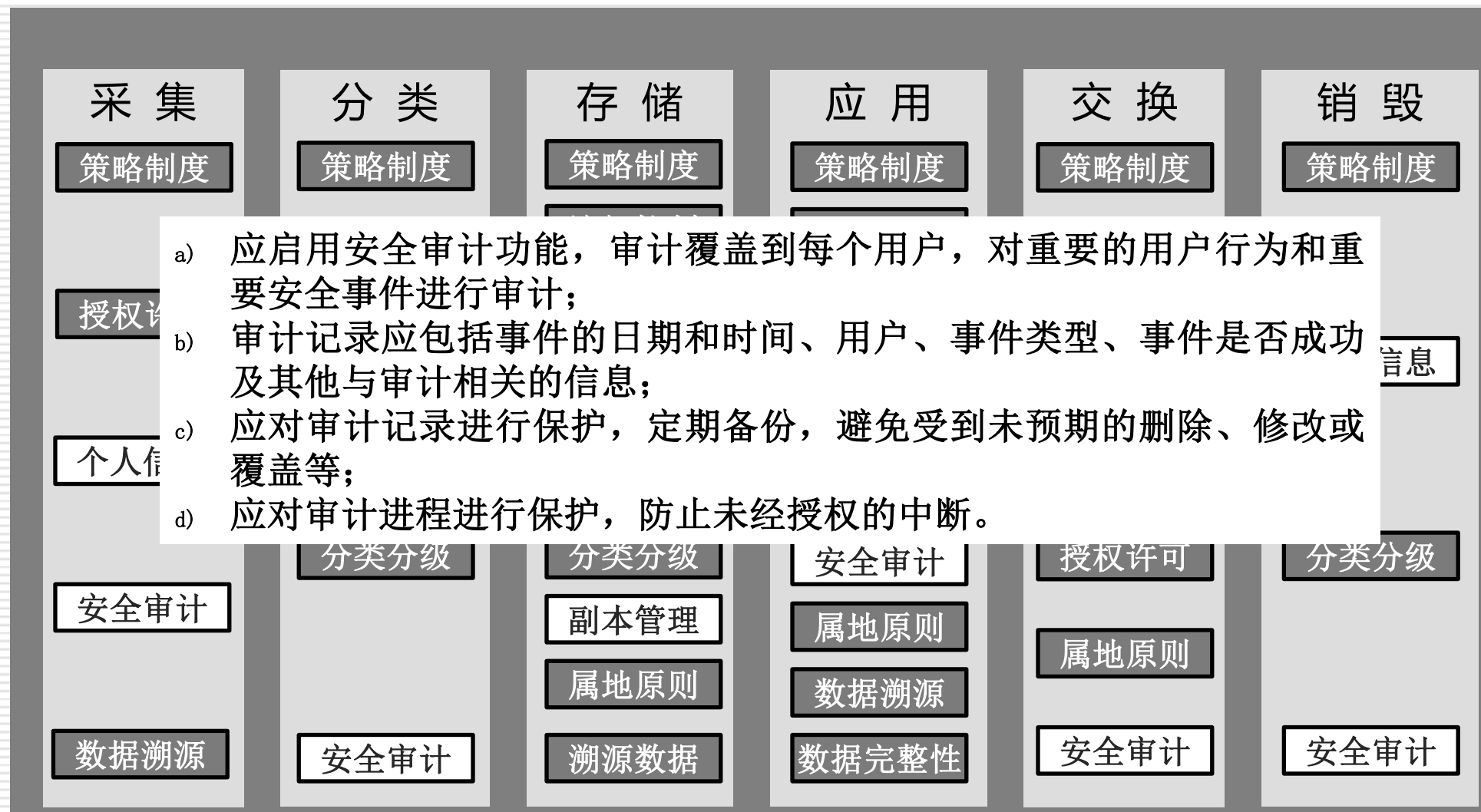


数据生命周期的安全

	采集	分类	存储	应用	交换	销毁
安全物理环境			H.4.1	H.4.1	H.4.1	
安全通信网络						
安全计算环境	H.4.3.a、 H.4.3.h、 H.4.3.j、 H.4.3.k、 H.4.3.m	H.4.3.i	H.4.3.h、 H.4.3.i、 H.4.3.j、 H.4.3.k	H.4.3.f、 H.4.3.h、 H.4.3.i、 H.4.3.j、 H.4.3.k、 H.4.3.l、 H.4.3.m	H.4.3.a、 H.4.3.h、 H.4.3.i、 H.4.3.j、 H.4.3.k、 H.4.3.m	H.4.3.h、 H.4.3.j、 H.4.3.m
安全建设管理	H.4.4.b、 H.4.4.c		H.4.4.b	H.4.4.b	H.4.4.b、 H.4.4.c	H.4.4.b
安全运维管理	H.4.5.a、 H.4.5.b	H.4.5.a、 H.4.5.b、 H.4.5.c、 H.4.5.d	H.4.5.a、 H.4.5.b	H.4.5.a、 H.4.5.b、 H.4.5.c	H.4.5.a、 H.4.5.b、 H.4.5.c	H.4.5.a、 H.4.5.b

H4.5.a应建立数字资产安全管理策略，对数据全生命周期的操作规范、保护措施、管理人员职责等进行规定，包括并不限于数据采集、存储、处理、应用、流动、销毁等过程；

大数据基本要求



数据分类分级

- 应制定并执行数据分类分级保护策略，针对不同类别级别的数据制定不同的安全保护措施；
- 应在数据分类分级的基础上，划分重要数字资产范围，明确重要数据进行自动脱敏或去标识的使用场景和业务处理流程；
- 应定期评审数据的类别和级别，如需要变更数据的类别或级别，应依据变更审批流程执行变更；
- 大数据平台应提供数据分类分级安全管理功能，供大数据应用针对不同类别级别的数据采取不同的安全保护措施；
- 大数据平台应提供设置数据安全标记功能，基于安全标记的授权和访问控制措施，满足细粒度授权访问控制管理能力要求；
- 大数据平台应在数据采集、存储、处理、分析等各个环节，支持对数据进行分类分级处置，并保证安全保护策略保持一致；

● **保证在机构内部数据分类分级的保护策略保持一致。**

授权许可

- 对外提供服务的大数据平台，平台或第三方只有在大数据应用授权下才可以对大数据应用的数据资源进行访问、使用和管理；
- 以书面方式约定大数据平台提供者的权限与责任、各项服务内容和具体技术指标等，尤其是安全服务内容；
- 明确约束数据交换、共享的接收方对数据的保护责任，并确保接收方有足够或相当的安全防护能力；
- 建立数字资产安全管理策略，对数据全生命周期的操作规范、保护措施、管理人员职责等进行规定，包括并不限于数据采集、存储、处理、应用、流动、销毁等过程；
-

访问控制

- 应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问；-通用安全
- 大数据平台提供设置数据安全标记功能，基于安全标记的授权和访问控制措施，满足细粒度授权访问控制管理能力要求；
- 涉及重要数据接口、重要服务接口的调用，实施访问控制，包括但不限于数据处理、使用、分析、导出、共享、交换等相关操作。

个人信息保护

- 应仅采集和保存业务必需的用户个人信息；通用
- 应禁止未授权访问和非法使用用户个人信息；通用
- 大数据平台应提供静态脱敏和去标识化的工具或服务组件技术；
- 应在数据分类分级的基础上，划分重要数字资产范围，明确重要数据进行自动脱敏或去标识的使用场景和业务处理流程。



大数据等级保护对象



大数据的定级



大数据的安全保护



大数据基本要求



大数据测评

调研环节

- 分类、分级，合理选择测评对象
- 业务数据生命周期流程
- 数据流动的情况（上下游）
- 关注个人敏感信息、出境数据、溯源数据

角色和对象

层面	扩展要求中涉及对象
安全物理环境	大数据平台管理员和大数据平台建设方案
安全通信网络	大数据平台和业务应用系统定级材料，网络架构
安全计算环境	数据采集终端、导入服务组件、业务应用系统、数据管理系统和系统管理软件，大数据平台、大数据应用，辅助工具、服务组件，计算节点和存储节点，设计或建设文档，应急方案或应急处置措施、设计文档和建设文档，审计数据
安全建设管理	大数据应用建设负责人、大数据平台资质及安全服务能力报告，大数据平台服务合同、协议和服务水平协议、安全声明，数据交换、共享策略和数据交换、共享的合同、协议
安全运维管理	数字资产安全管理策略，数据分类分级保护策略，大数据平台建设方案，：数据管理员，数据管理相关制度和数据变更记录表单

测评实践

- 测评指标：大数据平台应提供静态脱敏和去标识化的工具或服务组件技术；
- 测评对象：设计或建设文档、大数据应用和大数据平台；
- 测评实施包括以下内容：
 - 应检查大数据平台设计或建设文档，查看是否具备数据静态脱密和去标识化措施或方案，如核查工具或服务组件是否具备配置不同的脱敏算法的能力；
 - 应检查大数据应用，查看静态脱敏和去标识化工具或服务组件是否进行了策略配置；
 - 应检查大数据平台，查看是否为大数据应用提供静态脱敏和去标识化的工具或服务组件技术；

■ 应测试验证脱敏后的数据是否实现敏感信息内容的脱敏和隐藏，验证脱敏处理是否

“应在数据分类分级的基础上，划分重要数字资产范围，明确重要数据进行自动脱敏或去标识的使用场景和业务处理流程；

测评实践

- **测评指标：**大数据平台应提供数据分类分级安全管理功能，供大数据应用针对不同类别级别的数据采取不同的安全保护措施。
- **测评对象：**大数据平台、大数据应用系统、数据管理系统和系统设计文档等；
- **测评实施包括以下内容：**
 - 应访谈管理员是否依据行业相关数据分类分级规范制定数据分类分级策略；
 - 应核查大数据平台是否具有分类分级管理功能，是否依据分类分级策略对数据进行分类和等级划分；大数据平台是否能够为大数据应用提供分类分级安全管理功能；
 - 应核查大数据平台、大数据应用和数据管理系统等对不同类别级别的数据在标识、使用、传输和存储等方面采取何种安全防护措施，进而根据不同需要对关键数据进行重点防护。

测评实践

- **测评指标：应明确约束数据交换、共享的接收方对数据的保护责任，并确保接收方有足够或相当的安全防护能力；**
- **测评对象：数据交换、共享策略和数据交换、共享合同、协议等；**
- **测评实施包括以下内容：**
 - **应核查是否建立数据交换、共享的策略，确保内容覆盖对接收方安全防护能力的约束性要求；**
 - **应检查数据交换、共享的合同或协议，查看是否明确数据交换、共享的接收方对数据的保护责任。**

问题

- 数据的分级和系统级别的关系
- 测评对象如何选择

非常感谢