迈向高可信数据资产（第四期）

（来源：德勤微信公众号）

前言

上篇文章，德勤从《数据安全法》的重点关注内容以及数据资产全生命周期的安全保护出发，讲述了高可信数据资产的治理手段。企业需要通过技术手段将个人数据与跨境数据的安全保护以及管理方法落实到操作实务，以此实现高可信数据资产建设的价值。**有效的数据采集是实现高可信数据资产全生命周期的第一步，是实现数据资产的来源可信的有效手段，明确黄金数据源是开展高可信数据资产采集活动的关键所在。根据国标GB/T37988—2019中的数据安全PA体系，明确数据安全分级是数据采集安全的重点关注内容，实现有效的数据安全分级是保护高可信数据安全的奠基石。**

如何理解数据分类分级

数据是指用来记录客观事物或事件的符号，具体来说，是对客观事物或事件的性质、状态以及相互关系等信息记录的物理符号。数据包含任何以电子或者非电子形式对信息的记录。数据分类是数据保护工作中的一个关键部分，是建立统一、准确、完善的数据架构的基础，是实现集中化、专业化、标准化管理的基础。行业机构按照统一的数据分类方法，依据自身业务特点对产生、采集、加工、使用或管理的数据进行分类。数据分级是以数据分类为基础，采用规范、明确的方法区分数据的重要性和敏感度差异，并确定数据级别。数据分级有助于行业机构根据数据不同级别，确定数据在其生命周期的各个环节应采取的数据安全防护策略和管控措施，进而提高机构的数据管理和安

全防护水平，确保数据的完整性、保密性和可用性。

执行数据分类分级的前提条件

1 组织保障——建立可支撑开展数据分类分级的组织保障，组织中应至少明确以下内容：

- 数据分类分级的负责部门；
- 数据分类分级的最高负责人；
- 数据分类分级相关的管理角色和职能；
- 数据分类分级相关的授权机制。

2 制度保障——组织应建立明确的制度，制度中至少包含以下内容：

- 数据分类分级的具体要求；
- 数据分类分级工作中涉及的角色及职责；
- 数据分类分级的相关制度和操作流程的制定、发布、维护和更新的机制以及评审和修订周期；
- 数据分类分级管理相关绩效考评和评价机制；
- 数据分类分级的原则、方法；
- 数据级别的相关变更原则及变更后的通知原则；
- 数据分类分级保护的总体原则和目标；
- 数据分类分级的日常管理流程；
- 操作人员的操作规程。

在完成以上工作的前提下，企业可通过构建数据资产分级分类库和优化数据安全管理体系两方面履行对数据资产保护义务，构筑数据安全治理防线。

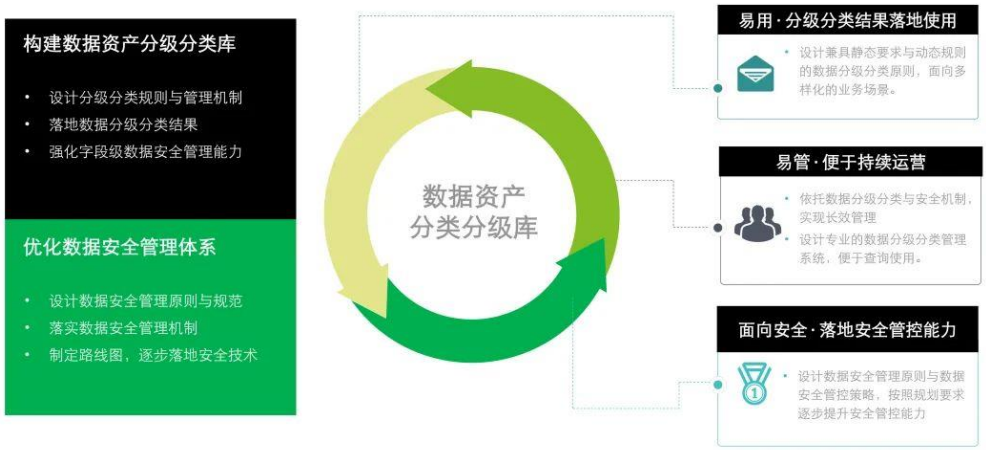

图 1 德勤数据资产分级分类库

数据分类分级宜遵循以下原则

数据分类：

1 系统性原则：数据分类宜基于机构所有数据的考量，建立一个层层划分、层层隶属的、从总到分的分类体系，每一次划分应有单一、明确的依据。数据类目的排列宜依据数据类目主题之间的内在联系，遵循概念逻辑，遵循最大效用原则，将全部类目系统地组织起来，形成具有隶属和并列关系的分类体系，以揭示出机构数据不同类别之间的联系和区别。

2 规范性原则：所使用的词语或短语能确切表达数据类目的实际内容范围，内涵、外延清楚；在表达相同概念时，保证用语一致性；在不影响数据类目涵义表达的情况下，保证用语简洁性。在证券期货行业已有统一数据用语的情况下，使用统一数据用语。

3 稳定性原则：宜选择分类对象的最稳定的本质特性作为数据分类的基础和依据。

4 明确性原则：同一层级的数据类目间宜界限分明。当数据类目名称不能明确各自界限时，可以用注释来加以明确。

5 扩展性原则：在数据类目的设置或层级的划分上，宜保留适当

余地，利于分类数据增加时的扩展。

数据分级：

1 依从性原则：数据级别划分应满足相关法律、法规及监管要求。

2 可执行原则：宜避免对数据进行过于复杂的分级规划，保证数据分级使用和执行的可行性。

3 时效性原则：数据的分级具有一定的有效期。数据的级别可能因时间变化按照一些预定的安全策略发生改变。

4 自主性原则：机构可根据自身的数据管理需要，例如战略需要、业务需要、对风险的接受程度等，按照数据分类原则进行分类之后，按照数据分级方法自主确定更多的数据层级，并为数据定级，但不宜将高敏感度数据定为低敏感度级别。

5 合理性原则：数据级别宜具有合理性，不能将所有数据集中划分一两个级别中，而另外一些没有数据。级别划定过低可能导致数据不能得到有效保护；级别划定过高可能导致不必要的业务开支。

6 客观性原则：数据的分级规则是客观并可以被校验的，即通过数据自身的属性和分级规则就可以判定其分级，已经分级的数据是可以复核和检查。

数据分类分级基本流程

第一阶段：业务细分。解决业务分类问题，同时确定数据的管理主体。数据管理主体的确定是数据分类准确性和定级准确性的基本保证。

业务细分的具体方法：

a. 确定业务一级子类——确定基本业务条线

b. 确定每个业务子类的范围下的所有管理主体。

1.管理主体一般是特定的管理组织、部门、岗位；

2.管理主体应可决定管理范围内数据访问的权限；

3.管理主体的确定宜适当，范围过小可能导致对应业务划分颗粒度过细；范围过大可能导致对应业务划分颗粒度过粗，无法区分不同业务。

c.确定每个管理主体对应的管理范围，明确对应关系。

1.管理范围指由业务特点决定的管理内容；

2.业务管理范围之间应相互独立；

3.业务主体和管理范围可为一对多或多对一的方式对应，但应尽量以一对一的方式对应，可适当细化管理主体。

d.对确定的各类业务“管理主体-管理范围”映射关系进行命名，得到业务二级子类的命名。

1.多个管理主体对应的管理范围相同，应视为一个业务二级子类；

2.一个管理主体对应的不同管理范围，应视为多个映射，即多个业务二级子类。

第二阶段：数据归类。在明确数据管理主体和业务分类的基础上，重点解决数据分类问题。

数据归类的具体方法：

a.找到业务二级子类下的全部数据，即确定业务二级子类的管理范围对应的管理对象。

1.管理对象指特定业务管理范围内对应的数据，由一系列数据表、数据项或数据文件等组成；

2.每个业务子类，找到其对应的一系列数据总和。这些“数据总和”应为全部数据的一个个子集；

3.部分数据表、数据项和数据文件可以出现在多个“数据总和”中；

4.得到每个业务子类对应的数据总和，称为“单类业务数据总和”。

b.按照数据细分方法对各个“单类业务数据总和”分别细分，得到数据一级子类。细分方法如下。

1.按照数据性质细分，指划分后的子类之间，数据性质之间有所差异；

2.按照重要程度细分，指划分后的子类之间，重要程度之间有所差异；

3.按照管理需要细分，指因不同的管理目的划分不同子类；

4.按照使用需要细分，指划分后的子类之间，使用范围之间有所差异；

可参选项a-d，选择适当的要素进行细分。

c.命名数据一级子类。即对上一步完成后确定的数据一级子类命名

d.对已划分明确的数据一级子类进一步细分，细分后产生一个或者多个数据子集，为数据二级子类。

需注意在数据归类过程中：

1.每个业务二级子类具有一组数据（数据表、数据项、数据文件等）总和；

2.全部数据可以多个不同组合方式分别隶属于不同的业务二级子类；

3.如有数据无法确定对应业务二级子类，说明业务二级子类划分不完全，需对第一阶段工作进行检验；

4.如有业务二级子类下不存在数据，说明可能存在冗余的业务二级子类或数据资产未厘清。

第三阶段：级别判定。在数据分类基础上，进行数据定级。

1 数据梳理：

第一步：对数据进行盘点、梳理与分类，形成统一的数据清单，并进行数据安全定级合规性相关准备工作。

2 数据安全定级准备：

第二步：明确数据定级的颗粒度（如库文件、表、字段等）。

第三步：识别数据安全定级关键要素。

3 数据安全级别判定：

第四步：按照数据定级规则，结合国家及行业有关法律法规、部门规章，对数据安全等级进行初步判定。

- 一般数据安全级别判定条件示例

客户数据(C)	客户可公开数据 (简称C1)	客户可共享数据 (简称C2)	客户隐私数据 (简称C3)	客户机密数据 (简称C4)
业务数据(S)	业务可公开数据 (简称S1)	业务内部数据 (简称S2)	业务保密数据 (简称S3)	业务机密数据 (简称S4)
公司数据(B)	公司可公开数据 (简称B1)	公司内部数据 (简称B2)	公司保密数据 (简称B3)	公司机密数据 (简称B4)
一般数据(L)	公开数据(简称L1)	内部数据(简称L2)	保密数据(简称L3)	机密数据(简称L4)

- 金融行业数据安全级别判定条件示例

最低安全级别参考	数据定级要素		数据一般特征
	影响对象	影响程度	
5	国家安全	严重损害/一般损害/轻微损害	• 重要数据，通常主要用于金融业大型或特大型机构、金融交易过程中重要核心节点类机构 的关键业务使用，一般针对特定人员公开，且仅为必须知悉的对象访问或使用。 • 数据安全性遭到破坏后，对国家安全造成影响，或对公众权益造成严重影响。
5	公众权益	严重损害	
4	公众权益	一般损害	• 数据通常主要用于金融业大型或特大型机构、金融交易过程中重要核心节点类机构的重要 业务使用，一般针对特定人员公开，且仅为必须知悉的对象访问或使用。 • 个人金融信息中的 C3 类信息. • 数据安全性遭到破坏后，对公众权益造成一般影响，或对个人隐私或企业合法权益造成严 重影响，但不影响国家安全。
4	个人隐私	严重损害	
4	企业合法权益	严重损害	
3	公众权益	轻微损害	• 数据用于金融业机构关键或重要业务使用，一般针对特定人员公开，且仅为必须知悉的对 象访问或使用。 • 个人金融信息中的 C2 类信息。 • 数据的安全性遭到破坏后，对公众权益造成轻微影响，或对个人隐私或企业合法权益造成一般影响，但不影响国家安全。
3	个人隐私	一般损害	
3	企业合法权益	一般损害	
2	个人隐私	轻微损害	• 数据用于金融业机构一般业务使用，一般针对受限对象公开，通常为内部管理且不宜广泛 公开的数据。 • 个人金融信息中的 C1 类信息。 • 数据的安全性遭到破坏后，对个人隐私或企业合法权益造成轻微影响,但不影响国家安全、 公众权益。
2	企业合法权益	轻微损害	
1	国家安全	无损害	• 数据一般可被公开或可被公众获知、使用。 • 个人金融信息主体主动公开的信息。 • 数据的安全性遭到破坏后，可能对个人隐私或企业合法权益不造成影响，或仅造成微弱影 响但不影响国家安全、公众权益。
1	公众权益	无损害	
1	个人隐私	无损害	
1	企业合法权益	无损害	

第五步：综合考虑数据规模、数据时效性、数据形态（如是否经汇总、加工、统计、脱敏或匿名化处理等）等因素，对数据安全级别进行复核，调整形成数据安全级别评定结果及定级清单。

4 数据安全级别审核：

第六步：审核数据安全级别评定过程和结果，必要时重复第三步及其后工作，直至安全级别的划定与本机构数据安全保护目标一致。

5 数据安全级别批准：

第七步：最终由数据安全管理最高决策组织对数据安全分级结果进行审议批准。

数据资产分类分级的应用

随着《数据安全法》落地，建立数据分类分级保护制度、实行分类分级保护等规定逐渐渗透到了日常的数据管理中。企业在完成数据分类分级工作后，可以更好地实现内容可信的高可信数据资产的构建。数据分类分级的应用场景举例：

- 企业用户的使用场景：企业用户做数据安全建设工作：首先梳理企业数据资产、分类分级，根据分类分级结果制定数据管控策略，实施管控措施，全景展示数据安全态势，持续运营改进。开放 API 接口，允许其他数据安全防护设备读取敏感数据信息，进行数据安全防护策略的配置和部署；
- 高校用户使用场景：专业数据分类分级设备由学校的网管中心统一负责维护，具体敏感数据识别业务则由各个学院自行完成，各学院数据互相隔离。
- 云端用户使用场景：业务系统部署在云环境，支持云端数据资产分类分级。

- 监管机构的使用场景：监管机构需要对大数据企业/单位做综合数据安全风险评估，包括数据资产识别、数据分类分级、平台组件安全扫描等。

数据分类分级价值

1 数据资产清查：帮助企业对数据资产进行全面清查、摸排，构建企业级的数据资产目录，为之后数据资产管理和数据安全体系建设打好基础。

2 满足企业合规需要：帮助企业满足合规的需要，既能够应对国家层面的法律法规，亦能满足行业法规的要求。例如敏感数据分类分级相关监管合规要求：

图 2 数据分类分级的最佳实践

3 数据资产化：帮助企业更好实现数据资产化，使企业从安全分级角度明确哪些数据在哪里、哪些数据可以使用、哪些数据要受控使用、哪些数据可以直接对外开放，利用数据分类分级的结果指导不同等级的数据在不同应用场景下在多类型安全设备中构建安全策略的部署与实施，实现数据安全治理。

结语

高可信数据资产的安全分类分级是管理体系合理规划、数据安全

合理管控、人员精力及力度合理利用的基础，是组织内部管理体系编写的基础、是技术支撑体系落地实施的基础、是运维过程中合理分配精力及力度的基础。下期文章我们将从数据监管体系展开，重点介绍监管对数据治理的要求与合规检查，敬请关注。

为更深入地阐释数据治理领域的理论体系与实践成效，探索数据治理进阶之路，德勤将邀请**国际数据管理协会中国（DAMA - CHINA）**与业内理论与实践应用专家参与此次数据治理 2.0 系列文章的编撰，邀请**微众银行**的数据及建模专家分享在数据模型应用、算法实践等领域经验。如果您对数据治理 2.0 系列文章有任何问题或意见，敬请联系：

文章作者：德勤中国风险咨询合伙人何晓明，德勤中国风险咨询经理崔英俊；德勤中国风险咨询副总监何向飞，德勤中国管理咨询副总监张华，国际数据管理组织协会中国理事郑保卫审阅编著。

原文链接：https://mp.weixin.qq.com/s/2uwGLBo5Icv4CqtCyxkEhg ，转载请注明。