迈向高可信数据资产（第三期）

（来源：德勤微信公众号，2021-09-03）

前言

上篇文章，德勤从高可信数据资产定义出发，讲述了高可信数据资产体系的基本构建方法体系，从数据战略、数据治理、数据信任、数据管理与数据应用五个层面对高可信数据资产的构建方法进行阐述与说明。在前序 1.0 的系列文章中针对高可信数据资产中的数据战略与数据治理已经用了较多的笔墨做了阐述和说明，本篇文章将从数据信任层的数据资产安全保护展开，高可信数据资产与我国最新出台的《数据安全法》中规范数据处理活动、保障数据安全的要求一致。**充分有效的保护数据方可实现数据资产的防线可信与安全可信，得到安全保护的数据方可成为高可信数据资产。数据保护是《数据安全法》的重点关注内容，强化高可信数据资产全生命周期的安全保护更是重中之重。**

如何理解数据安全法中的安全要求

任何组织或个人，在中国境内进行数据处理活动的，都必须遵从《数据安全法》。《数据安全法》从数据安全与发展、安全制度、安全保护义务、政务数据安全与开放四大领域结合整体数字经济的发展提出了发展与安全并重的具体要求。企业应充分开发利用数据资产，建设高可信数据资产安全标准体系，积极研究数据资产安全技术，加强数据资产安全检测评估。

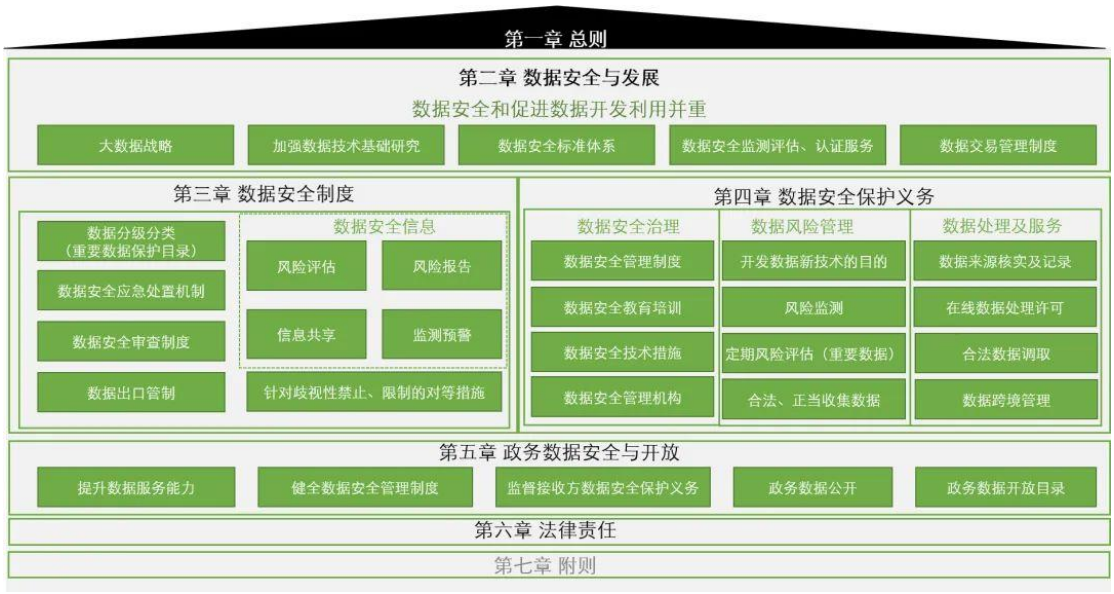

图 1 数据安全法整体框架

企业在开展业务的过程中，面临着数据资产安全管理、数据资产风险管理、个人信息安全管理、数据跨境安全管理等多重挑战。企业应履行数据资产安全保护义务，构筑数据安全治理防线，完善自身数据安全组织运营，并采取相应的技术措施，加强数据资产风险监测，管控数据出口，保护个人信息。

数据保护作为数据资产管理安全信任防护体系的一道防线，是高可信数据资产建设的信任基础。企业应从数据供应端、数据中介机构、数据消费端等业务流程视角充分梳理自身业务流程和相关数据资产，并结合数据全生命周期的理念充分保障数据资产安全，实现企业数据资产的安全可信。

如何进行数据资产生命周期安全保护

《GB/T 37988-2019 数据安全能力成熟度模型》中将数据生命周期分为数据采集、数据传输、数据存储、数据使用、数据交换、数据销毁六个阶段，并从组织建设、制度流程、技术工具、人员能力四个安全能力维度的建设进行综合考量。企业基于自身管理现状和基建完

善程度，在数据生命周期内的六个阶段选取合适的环节进行发力，能够在保证重要数据资产安全的情况下，充分降低安全和业务的沟通成本。

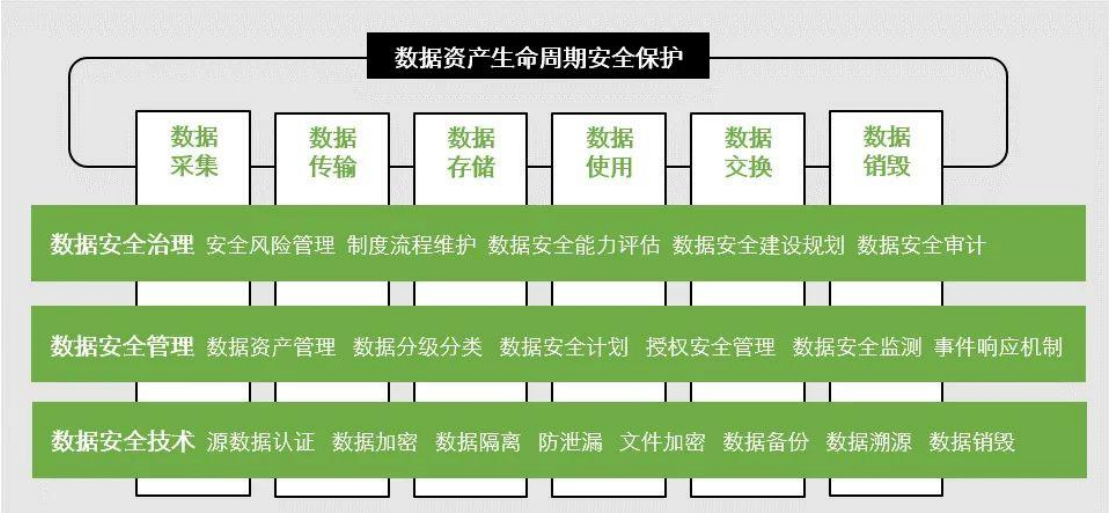

图 2 数据资产生命周期安全保护

数据资产生命周期内的不同阶段存在不同的安全风险，企业只有针对不同阶段内的风险制定相应的保护措施，才能有效的解决数据资产安全问题。

1 **数据采集阶段：**数据分类分级、数据采集告知同意、数据源鉴别及记录、数据质量管理

2 **数据传输阶段：**数据传输加密、网络可用性管理

3 **数据存储阶段：**存储介质安全、逻辑存储安全、数据备份和恢复

4 **数据使用阶段：**数据脱敏、数据分析安全、数据正当使用、数据处理环境安全

5 **数据交换阶段：**数据导入导出安全、数据共享安全、数据发布安全、数据接口安全

6 **数据销毁阶段：**数据销毁处置、介质销毁处置

如何治理与保护数据资产安全

通过对数据安全法的解读和对数据资产生命周期安全保护的理解，德勤提出高可信数据资产安全保护与治理框架。该框架充分平衡业务需求与数据风险管理，将安全要求贯穿高可信数据资产的应用以及数据资产的全生命周期之中。

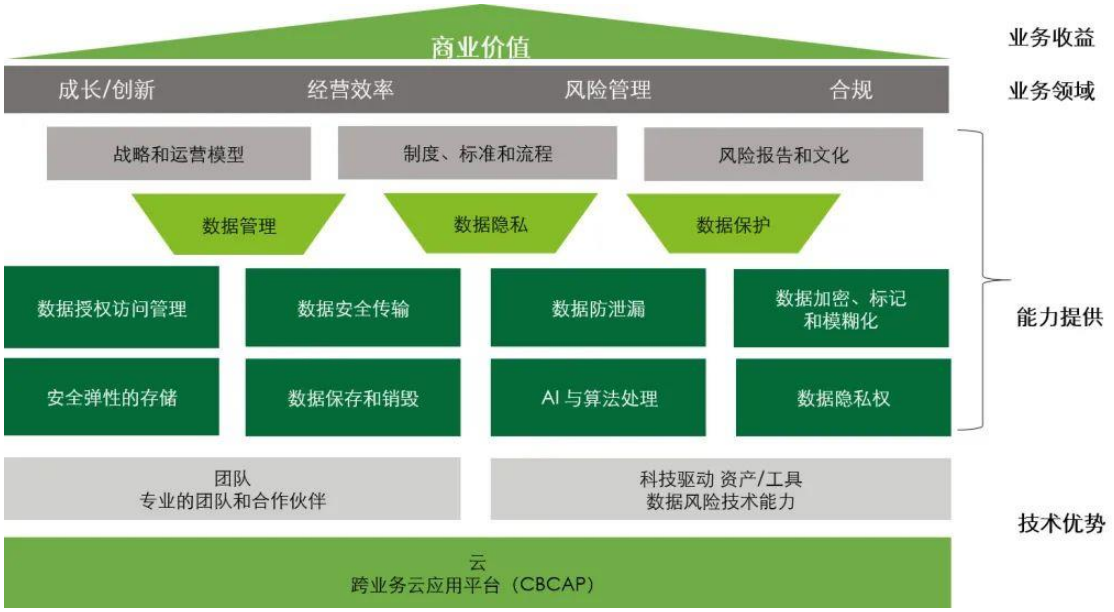

图 3 德勤高可信数据资产安全保护与治理框架

德勤高可信数据资产安全保护与治理框架从业务收益、业务领域、能力提供以及技术优势四个层面明确了数据资产安全保护的整体管理要求，以对数据资产的安全保护和管理体系进行标准处理，从而最大限度的减低因数据资产保护不善而给企业带来的风险，提高企业使用数据资产取得竞争优势的能力。企业应在数据战略和数据治理的层面之上，建立相关系统、流程和结构以在数据资产的整个生命周期内对其管理并满足适用的商业、法律和监管要求。

如何有效保护个人信息

个人信息无疑是高可信数据资产的关键组成部分，当前个人信息保护的监管重点主要集中在违规收集个人信息、过度索取权限、用户

权限保障不足、非法用户画像和广告推广、未成年人保护失效以及违规使用个人信息等方面。《个人信息保护法（草案）》明确了个人**具有知情权、决定权、查阅复制权、更正补充权、删除权**等权利，并对基于个人同意以外合法处理个人信息的情形作了规定。

同时，《个人信息保护法（草案）》完善了处罚条款，规定可对违法企业处五千万元以下或者上一年度营业额百分之五以下的罚款。为满足监管要求、降低个人信息泄露风险，企业应从个人信息保护组织技术管理要求、个人信息收集、个人信息保存、个人信息使用、个人信息共享等方面提高管控水平。

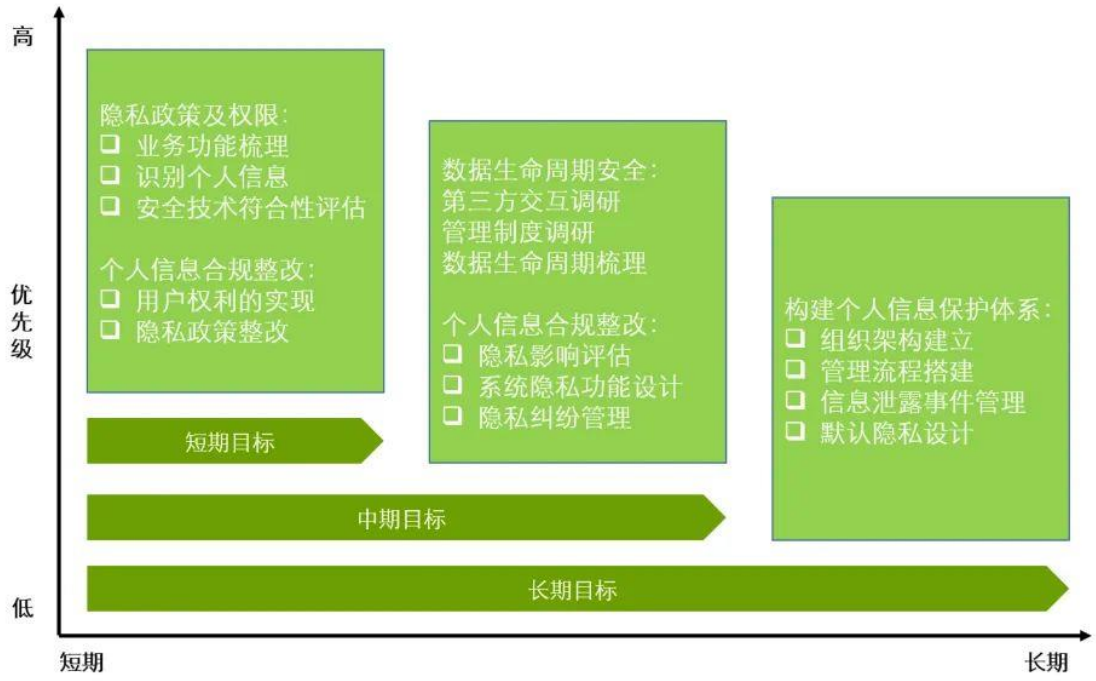

图 4 个人信息保护方案建设目标

我们建议企业立即开展相关工作，充分识别企业持有的个人信息，确认个人信息的业务使用场景，开展个人信息风险评估，落地整改方案并追踪改进效果。企业可根据自身情况设计个人信息保护短中长期建设目标，在满足国内外合规要求的前提下，保护数据资产生命周期安全，构建个人信息保护体系，最终实现个人信息的安全保护。

如何实现数据跨境安全

《数据安全法》第 25 条规定，国家对与维护国家安全和利益、履行国际义务相关的属于管制物项的数据依法实施出口管制。该项规定与《出口管制法》的规定形成了衔接。《出口管制法》规定了对相关货物、技术、服务等物项，包括物项相关的技术资料等数据的出口管制要求。

据此，如果待出境数据落入出口管制清单，数据出境还应根据《出口管制法》获得国务院、中央军事委员会出口管理部门的许可。此外，《数据安全法》更是规定违法向境外提供重要数据的企业将面临最高一千万人民币的罚款。因此，我们建议企业持续强化数据出境管理，建立数据出境审核机制。

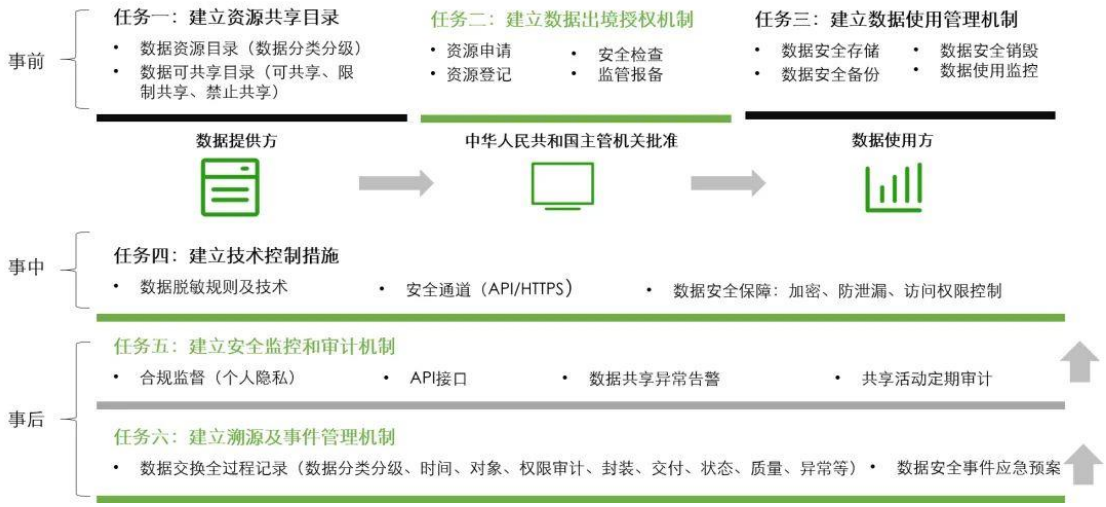

图 5 数据出境安全管控方案

如何使用技术手段保护数据资产安全

前文介绍了企业数据资产安全治理与保护的框架、个人隐私以及数据跨境保护的关注重点。与此同时，企业需要通过技术手段将管理方法落实到操作实务，以真正地实现高可信数据资产安全保护，并且充分实现高可信数据资产建设的价值。从数据资产生命周期安全保护

的角度，企业可采用数据访问控制、数据防泄露、数据库防火墙等多种安全工具组合的方式建设企业数据安全技术防护能力。

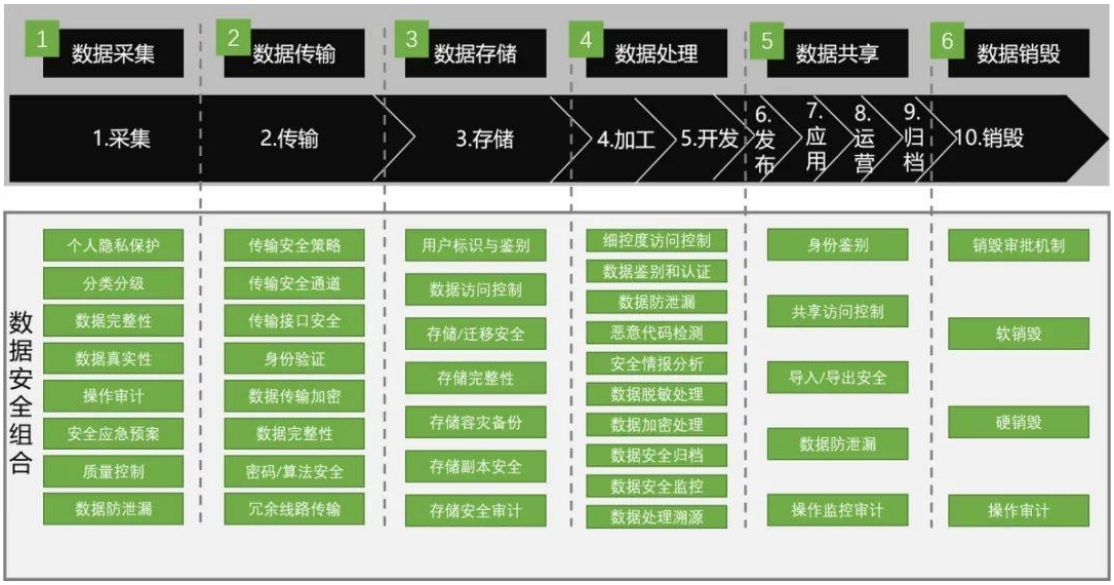

图 6 数据资产安全保护工具概览

在此基础上，企业可以采用如零信任架构、UEBA（用户和实体行为分析）等更加严格与智能的技术手段来实现简单、模块化的数据资产环境，并且直观的管控用户访问和操作行为。

1.零信任架构

在德勤发布的《2021 年技术趋势》报告中，已认为零信任是现代企业环境所需要的一种创新安全保障方法。零信任通过细分资源访问控制防范非法访问和横向移动，以保护资源的安全性为核心目的，以“从不相信、永远验证”为基本理念。

零信任代表安全管理理念上的转变，并且通常需要在企业内进行文化的变革。很多现有的安全技术都可以用来构建零信任架构，在实践过程中，企业应该合理部署安全堆栈，以促进更高效的自动化和排程来保护数据资产安全。

图 7 零信任三要素

2.UEBA

UEBA，即 user and entity behaviour analytics，提供画像及基于各种分析方法的异常检测，通常是基本分析方法（利用签名的规则，模式匹配，简单统计等）和高级分析方法（监督和无监督的机器学习等），用打包分析来评估用户和其他实体来发现与用户或实体标准画像或行为相异常的活动所相关的潜在事件。这些活动包括受信内部或第三方人员对系统的异常访问（用户异常），或者外部攻击者绕过防御性安全控制的入侵（异常用户）。

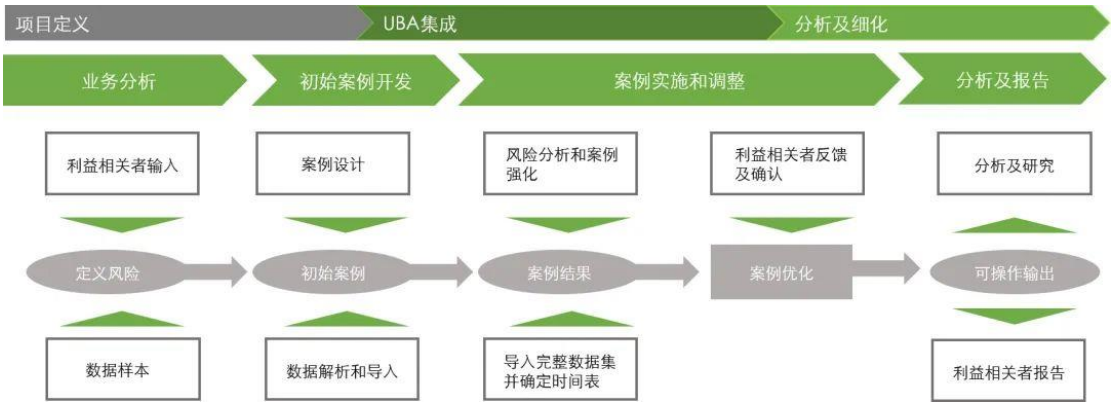

图 8 UEBA 实施方案

UEBA 能够帮助企业精确定位数据资产安全风险较高的业务场景，可以帮助企业发现通过简单统计方法无法捕捉的行为异常，并且便于后期排查与追溯工作的开展。

结语

高可信数据资产安全保护实践，将持续在业务流转中打造数据资产安全实战化防护，提高企业处于各种数据资产安全场景的解决方案

能力。《数据安全法》规定国家建立数据分类分级保护制度，对数据实行分类分级保护，统筹协调有关部门制定重要数据目录，加强对重要数据的保护。下期文章我们将在高可信数据资产保护治理框架下，重点介绍数据资产分级分类保护指引的制定和应用，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。

文章作者：德勤中国合伙人何晓明，德勤中国经理崔英俊，德勤中国副总监何向飞，德勤中国副总监张华，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/mhwxlSljG9We4oluuqeJ3A ，转载请注明。