御数坊数据安全治理咨询服务白皮书

DGworkshop Data Security Governance consulting service whitepaper

V1.0

御数坊（北京）科技咨询有限公司

编 写 组：刘晨、王少锋、赵佳、马占有、林宇街、
张微、方俊霆、牛畅、郭星、张志和
出 品 方：御数坊（北京）科技咨询有限公司
发布日期：2020年9月 第一版

目录 TITLE

1、企业数据安全治理建设目标

在众多的数据概念当中，我们听到的最多的是数据质量、元数据、数据标准等专业性的名词，这些词语在数据治理领域当中在当今高速发展的互联网时代下，对于企业用户也并不算是陌生，而数据安全对于IT行业尤其是从事网络信息安全行业的从业者来说也有自己的认知和了解。而数据安全治理，对于无论是专业从事数据治理的顾问还是从事网络信息安全的IT安全专家来说，都相对陌生，似乎“数据安全治理”这个名词好像是刚刚出现，但又给人一种很奇怪的感觉，“数据安全治理”这个词好像却又被广为人知。

当前IT领域中，企业的数据安全往往被认为是系统安全，保证了系统安全就保证了数据安全。企业在数据安全的建设道路上，往往希望将数据放在一个封闭的环境中，这种片面的做法只能理解为是一种简单的保证数据的“防窃取”。而当下，数据共享是发展趋势，数据安全应该包括防止数据被窃取、被滥用、被误用，同时充分将数据的“保密性”、“完整性”和“可用性”这三个重要数据指标考虑进去。

我们期望建立一套符合企业内自身的数据安全治理之道，包含组织能力、执行能力、人员能力、技术工具、场景化等要素，通过数据安全管控体系的设计，形成人防与技防，从决策到管理再到执行层级相互结合的立体的管控体系，用以建设并提升企业的数据安全治理能力。

2、企业数据安全治理背景

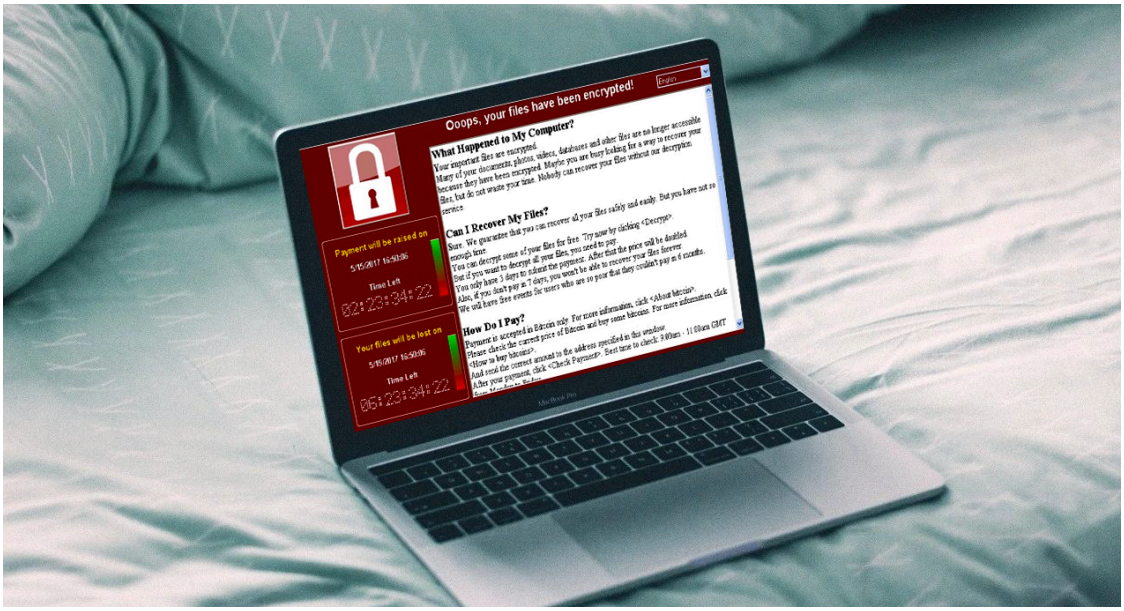
2.1 数据已成为企业生产要素

近日，中共中央、国务院发布**《关于构建更加完善的要素市场化配置体制机制的意见》**中就引导劳动力要素合理畅通有序流动、加快培育数据要素市场、加快要素价格市场化改革等提出“顶层设计”。我们可以看出数据被明确的纳入到生产要素中，数据在经济社会发展中的作用越来越显著和重要。在大数据时代，我们常说数据是互联网时代的“石油”，这并不是夸张，而是事实，毋庸置疑企业的数据资产已经成为企业最具有市场竞争力的资源，谁拥有的数据资源多，谁就会在这个大数据时代拥有更多的市场和用户。大数据正在改变着我们的生活，也在改变着企业的运营模式，这些改变都将成为未来企业竞争的核心商业价值。企业如何在未来的市场竞争中保持竞争力，那么就需要在数据的收集和处理上不断努力，由于数据具有时效性、可再生性，需要通过对数据进行更多的收集和挖掘，寻找数据带给企业的商机。

2.2 数据价值导致数据风险

2.2.1 数据勒索成为风险趋势

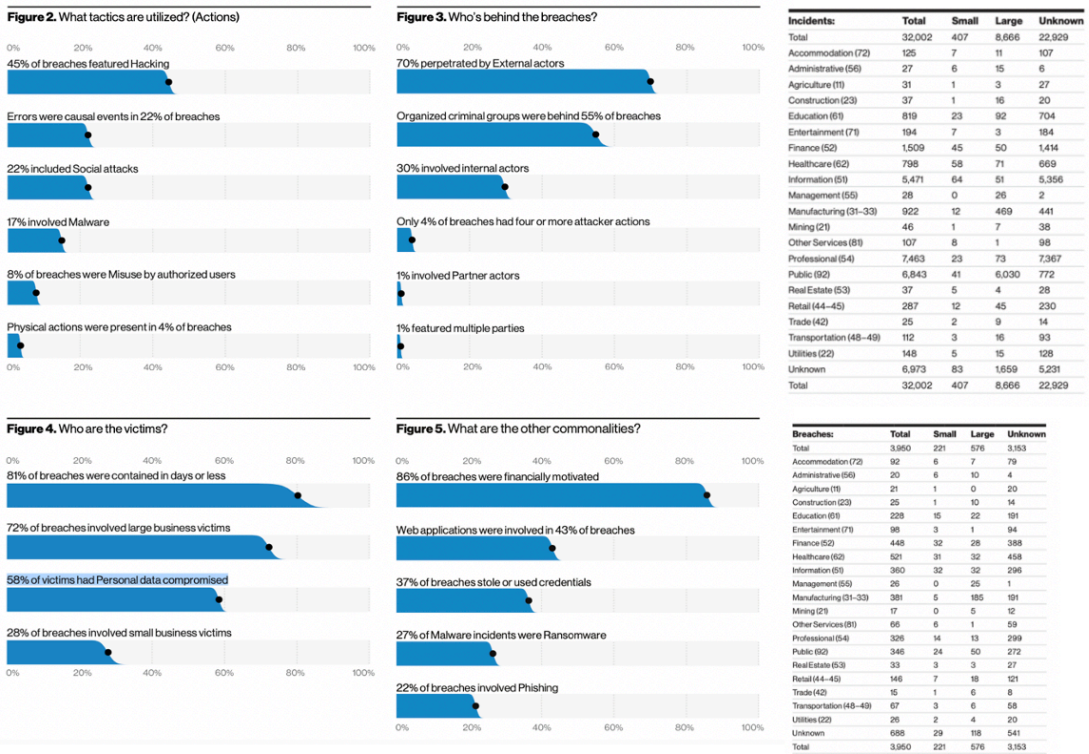
随着企业数据化能力转型工作的开展和推进，企业的数据价值越来越被企业所重视，数据在成为企业核心竞争力资源的同时，也被不法分子或行业竞争对手所关注。



在2017年，一种名为“WannaCry”的勒索病毒袭击全球150多个国家和地区，影响领域包括政府部门、医疗服务、公共交通、邮政、通信和汽车制造业。对于当时的IT从业人员来说，WannaCry勒索病毒的图标让人记忆深刻，也是从那时起，全国IT行业开始对勒索病毒提高关注，数据价值的保护也成为了企业防护的重点；在2018年上半年，我国发生多次勒索病毒事件，该勒索病毒是GlobeImposter家族的变种，该勒索病毒将加密后的文件重命为GOTHAM、.Techno、.CHAK、.FREEMAN、.TRUE、等扩展名，并通过邮件来告知受害者付款方式，使其获利更加容易方便；2020年4月，网络上出现了一种名为“WannaRen”的新型勒索病毒，与此前的“WannaCry”的行为类似，加密Windows系统中几乎所有文件。随着勒索病毒更新迭代速度较快以及不断涌现，勒索病毒已成为不法分子的一份产业，不法分子的勒索代理服务正在变得越来越稳定，甚至走向正规化。同时勒索病毒与挖矿木马混合感染的情况多见，在一些企业内网被入侵攻击的案例中，同时存在挖矿木马感染和勒索病毒感染。

2.2.2 数据泄露防不胜防

在当前的数据世界中，数据价值流动通过采集、流转、汇聚、使用、存储、消费等环节，将二进制数据变成我们可以看懂的文字信息，其中这些信息包含我们的个人信息、企业核心数据、国家机密数据等，但是我们会常常看到互联网上相关的数据泄露的报道，这些数据泄露的事件中，小到以MB为计量单位，大道以TB为计量单位，这些数据泄露事件损害了个人的隐私、企业的商业利益以及国家的机密数据。



Incidents:	Total	Small	Large	Unknown
Total	32,002	407	8,666	22,929
Accommodation (72)	125	7	11	107
Administrative (56)	27	6	15	6
Agriculture (11)	31	1	3	27
Construction (23)	37	1	16	20
Education (61)	819	23	92	704
Entertainment (71)	194	7	3	184
Finance (52)	1,509	45	50	1,414
Healthcare (62)	798	58	71	669
Information (51)	5,471	64	51	5,356
Management (55)	28	0	26	2
Manufacturing (31–33)	922	12	469	441
Mining (21)	46	1	7	38
Other Services (81)	107	8	1	98
Professional (54)	7,463	23	73	7,367
Public (92)	6,843	41	6,030	772
Real Estate (53)	37	5	4	28
Retail (44–45)	287	12	45	230
Trade (42)	25	2	9	14
Transportation (48–49)	112	3	16	93
Utilities (22)	148	5	15	128
Unknown	6,973	83	1,659	5,231
Total	32,002	407	8,666	22,929

Breaches:	Total	Small	Large	Unknown
Total	3,950	221	576	3,153
Accommodation (72)	92	6	7	79
Administrative (56)	20	6	10	4
Agriculture (11)	21	1	0	20
Construction (23)	25	1	10	14
Education (61)	228	15	22	191
Entertainment (71)	98	3	1	94
Finance (52)	448	32	28	388
Healthcare (62)	521	31	32	458
Information (51)	360	32	32	296
Management (55)	26	0	25	1
Manufacturing (31–33)	381	5	185	191
Mining (21)	17	0	5	12
Other Services (81)	66	6	1	59
Professional (54)	326	14	13	299
Public (92)	346	24	50	272
Real Estate (53)	33	3	3	27
Retail (44–45)	146	7	18	121
Trade (42)	15	1	6	8
Transportation (48–49)	67	3	6	58
Utilities (22)	26	2	4	20
Unknown	688	29	118	541
Total	3,950	221	576	3,153

Verizon 2020 Data Breach Investigations Report

2020年5月，美国公司Verizon发布了2020年数据泄露调查报告（DBIR），其中有超80个国家参与此次数据泄露的调研，该报告总共收集了近16万的数据泄露事故和近11万的数据使用违规事件，其中这些事件中有10万多个事件是由云服务或者是银行用户的凭证漏洞导致个人用户的信息泄露；在数据泄露事件中，有55%的泄露事件和有组织犯罪相关，外部攻击占70%，企业内部攻击占30%；涉及个人数据泄露占58%，72%的受害者为大型企业。

2.3 数据平台安全风险加剧

大数据平台多基于开源技术栈进行搭建，各组件自身的安全机制较薄弱，同时系统以及平台的集成缺乏连贯的安全机制，容易产生安全漏洞。

大数据应用使用开放的分布式计算和存储框架来提供海量数据分布式存储和计算服务。数据平台的技术发展速度较快，如何保证在使用新技术、新架构的同时防止新型攻击手段给企业保证数据安全带来挑战，在保证数据平台或数据中台的安全基础上应该采用什么样的防护手段或其应具备什么样的防护能力也是企业需要在设计数据平台之初就应该考虑的内容。

纵观国内大数据平台的架构设计，大多采用像Hadoop、MPP、Hive、Spark、HDFS等生态组件，在设计初期对用户身份鉴别、访问控制、密钥管理、安全审计等方面考虑较少，并且这些应用中多采用第三方开源组件，如容器、微服务等，对这些组件缺乏严格的测试管理和安全认证。

同时，数据通过数据采集、传输、存储、共享、使用和销毁的过程中，每个环节在数据平台当中应该怎样去保证其安全性，也是企业需要考虑的重要问题。

此外，随着企业应用部署在云端已成为必然的趋势，云环境中存在企业用户数据所有权和管理权分离的特点，对被存储在云端的数据，用户是否可以控制其数据的“保密性、完整性、可用性”特点。

2.4 来自合规的监管要求

由于各行各业对数据价值的重视程度越来越大，一旦数据风险出现，不论是对企业还是个人都会造成一定的威胁，我们最常见的就是数据风险导致大量个人信息泄露，这对企业和国家社会安全的防控带来了不小的考验；还有我们经常听说基于苹果手机用户的消费者和安卓手机用户的消费者，通过APP购买产品或获取服务时，需要付费的价值是区别对待的，这种典型的数据滥用导致用户资金消费被区别对待的“杀熟”行为也体现出了当前社会对数据正确使用的迫切需求。因此为了保证大数据时代的稳定发展，世界各国相继颁布了对个人、社会和国家层面的关于数据安全保护的相关法律法规。

我国在2016年颁布了**《中华人民共和国网络安全法》**，在2017年6月1日正式生效，**《中华人民共和国网络安全》**法中明确地对个人隐私数据和国家重要数据提出了保护要求，其中包含一些具体化的措施要求。

在2019年12月1日我国正式实行**GB/T 22239-2019《信息安全技术网络安全等级保护要求》（简称等保2.0）**，为了贯彻落实《中华人民共和国网络安全法》，适应云计算、移动互联、物联网、工业控制和大数据等新技术、新应用情况下网络安全等级保护工作。明确提出了对数据审计、用户访问身份鉴别等要求，企业数据安全建设同样需要参照等保的相关规定和要求。

针对于个人信息的保护，我国早在2017年就颁布了**《信息安全技术 个人信息安全规范》**主要针对个人信息面临的安全问题，规范了个人信息控制者在收集、保存、使用、共享、转让、公开披露等信息处理环节中的相关行为，旨在遏制个人信息非法收集、滥用、泄露等乱象，最大程度地保障个人的合法权益和社会公共利益。而即将在2020年10月1日生效的新版**GB/T 35273-2020《信息安全技术 个人信息安全规范》**中，添加了新的技术变化，如“征得授权同意的例外”、“用户画像的使用限制”、“个人信息主体注销账户”等内容，更加完善了个人信息的保护。

在2019年10月1日正式实行的**《儿童个人信息网络保护规定》**针对中华人民共和国境内通过网络收集、存储、使用、转移、披露不满十四周岁的儿童个人信息进行规范。保证了儿童个人信息的权益。

2018年5月25日，欧盟出台了**《通用数据保护条例》**，简称GDPR，该条例的适用范围极为广泛，任何收集、传输、保留或处理涉及到欧盟所有成员国内的个人信息的机构组织均受该条例的约束，并且条例中明确指出了企业如何收集、使用和

处理个人信息，并对违法该规定的企业进行相应的处罚。该条例的颁布，促进了我国对个人信息保护、网络安全的保护法律法规的完善。

3、认识数据安全治理

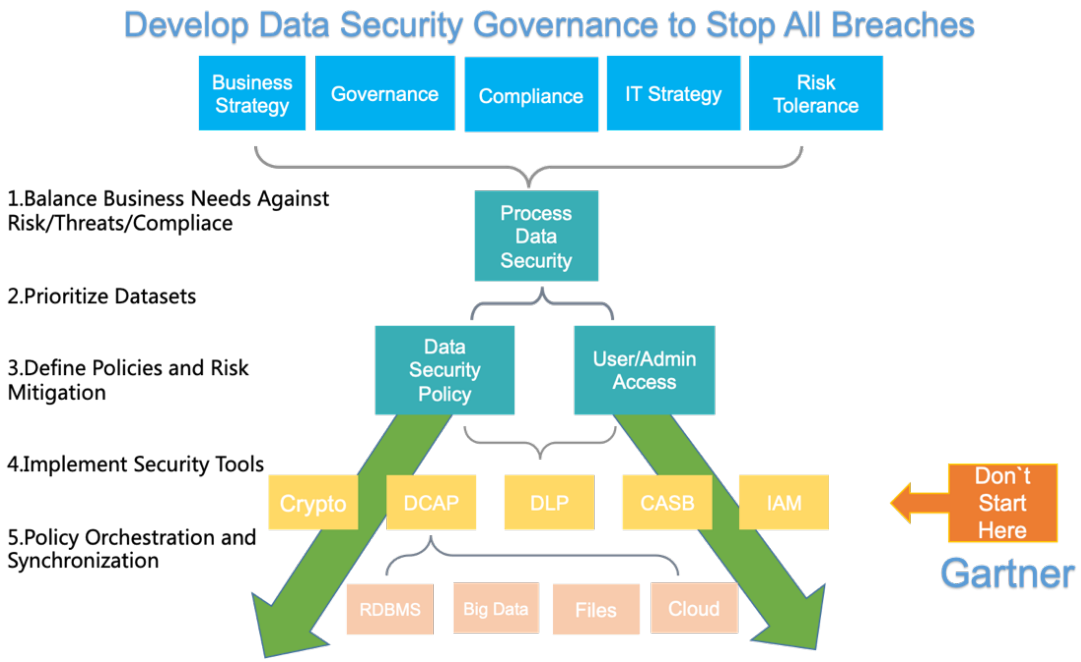
3.1 数据安全治理的方法概述

数据安全治理对于企业和IT从业人员来说算是一个新的名词，企业为了能够保证数据安全往往认为只是使用数据安全相关的工具就可以。而数据安全治理是一个“大范围、复杂而专业”的理念，关于数据安全治理原则与框架，国际研究机构Gartner 对此进行专属领域的研究，提出了数据安全治理框架DSG，该框架提出数据安全治理是一种持续化的工作进程，这正符合同样是Gartner提出的CARTA模型。我国对于企业的数据安全提出了DSMM模型，是围绕数据安全过程维度、安全能力维度以及数据安全能力成熟度等级维度这三个维度，以持续不断的提升组织整体的数据安全能力，以数据为核心的安全框架。在涉及到业务逻辑，业务安全专家需要分析数据流图（DFD图形），从流程，数据存储，数据流和外部实体定义不同的可视表示，从而分析各个环节可能存在的数据安全风险。

3.1.1 Gartner数据安全治理框架DSG

在2018年，全球领先的IT研究和咨询机构Gartner提出安全安全治理框架DSG，该框架的基本思路是对数据全生命周期中的数据进行识别、分类分级，然后根据

响应的数据安全防护策略规则，并采用相应的数据安全防护工具进行部署、策略配置，并根据CARTA模型（持续自适应风险/信任评估模型）定期在发生数据风险的时候调整数据防护工具制定的策略或功能，来阻断或减轻数据所受到的安全威胁，进而保证对敏感信息的保护。



Gartner Data Security Governance框架模型

DSG模型框架主要分为五个部分，其中每个部分的内容如下：

➞ 1. 组织在开展数据安全治理前应统一达成相关目的或共识，并且分析企业经营战略目标、数据安全治理、IT策略与数据风险的容忍度等方面的平衡关系。

➞ 2. 实行全生命周期的数据识别、数据分类与分级。

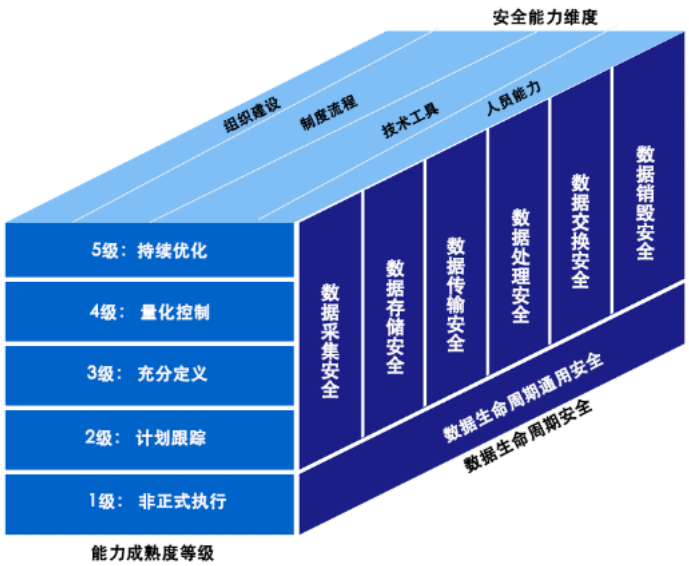
➞ 3. 针对数据分类分级，识别数据风险，并根据数据的分类、数据的级别以及数据面临的风险执行相应的数据安全管控策略。

➔ 4.实施数据安全防护工具，Gartner提供了5种数据安全防护工具，其中涉及到数据加密、以数据为核心的数据审计、数据防泄漏、云访问安全代理网关、身份识别与访问验证系统等。

➔ 5.根据数据安全防护的需要，对不同的工具进行数据安全防护策略。

3.1.2 企业数据安全能力成熟度模型DSMM

有过数据治理的经验的相关人士可以看出DSMM借鉴能力成熟度模型（CMM）的思想，将数据按照其生命周期分阶段采用不同的能力评估等级，DSMM一共划分了5个等级，依次为非正式执行级、计划跟踪级、充分定义级、量化控制级、持续优化级；每个等级的能力需要从数据生命周期各个阶段从数据采集安全、数据传输安全、数据存储安全、数据处理安全、数据交换安全、数据销毁安全六个阶段的能力进行评定。DSMM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。该模型形成一个三维立体模型，全方面对数据安全进行能力建设。



DSMM数据安全能力成熟度模型框架

DSMM从组织、制度流程、技术工具、人员描述了企业应具有的数据安全能力，并从全数据生命周期维度强调了数据的安全要求，同时，制定了企业数据安全能力成熟度的等级，为后续企业建设数据安全体系提供给了理论基础和依据。

3.1.3 持续自适应风险与信任评估模型CARTA

CARTA（Continuous Adaptive Risk and Trust Assessment）：持续自适应风险与信任评估。强调对风险和信任的评估分析，这个分析的过程就是一个权衡的过程。CARTA模型是一个庞大的体系，其包括大数据、AI、自动化、行为分析、威胁检测、安全防护、安全评估等方面，CARTA模型中的风险是一个持续性的判断过程，对应的防护策略也是需要持续不断的。

CARTA模型可以与数据安全治理进行融合，企业数据面对的数据风险、安全威胁并不是一个持续不变的过程，随着各项新型技术的提出、行业的发展，企业面对的数据风险也一直在变化，对数据的安全防护与安全治理也是一个持续优化的过程。

3.1.4 面向特定场景的风险分析

在分析数据风险的时候，我们经常可以采用数据流图（Data Flow Diagram）的方式对数据风险进行分析，它从数据传递和加工角度，以图形方式来表达系统的逻辑功能、数据在系统内部的逻辑流向和逻辑变换过程，是结构化系统分析方法的主要表达工具及用于表示软件模型的一种图示方法。

我们在软件开发生命周期中的设计阶段，基于数据的安全和业务逻辑，通常会采用基于场景进行威胁建模，通过数据流图的方式从流程，数据存储，数据流和外部实体定义不同的可视表示，从而分析各个环节的安全风险，进而根据风险威胁程度提出解决方法或缓解措施，通过技术手段保证其安全性。

从基于场景的威胁建模进行数据流图的威胁分析，我们得到启示，在数据安全治理的过程中，我们也同样需要考虑在特定场景下的数据风险，并且根据数据使用情况进行场景拆分，制定符合特定场景的数据威胁防护方法，保障数据安全。

3.2 数据安全治理与数据治理

数据治理与数据安全治理是两个很容易让人混淆的名词，对于初次接触这两个名词的人来说可能一时间无法理清两者的关系和区别。对于初次接触数据安全治理概念的人普遍会认为数据安全治理是数据安全加上数据治理的结合体，其实存在本质的不同，如下为各个概念与区别：

数据安全：“国际标准化组织（ISO）对计算机系统安全的定义是：为数据处理系统建立和采用的技术和管理的安全保护，保护计算机硬件、软件和数据不因偶然和恶意的原因遭到破坏、更改和泄露。由此计算机网络的安全可以理解为：通过采用各种技术和管理措施，使网络系统正常运行，从而确保网络数据的可用性、完整性和保密性。所以，建立网络安全保护措施的目的是确保经过网络传输和交换的数据不会发生增加、修改、丢失和泄露等。

数据治理：是组织为实现数据资产价值最大化，所展开的一系列持续工作过程，明确数据相关方的权责、协调数据相关方达成数据利益一致、促进数据相关方采取联合数据行动。

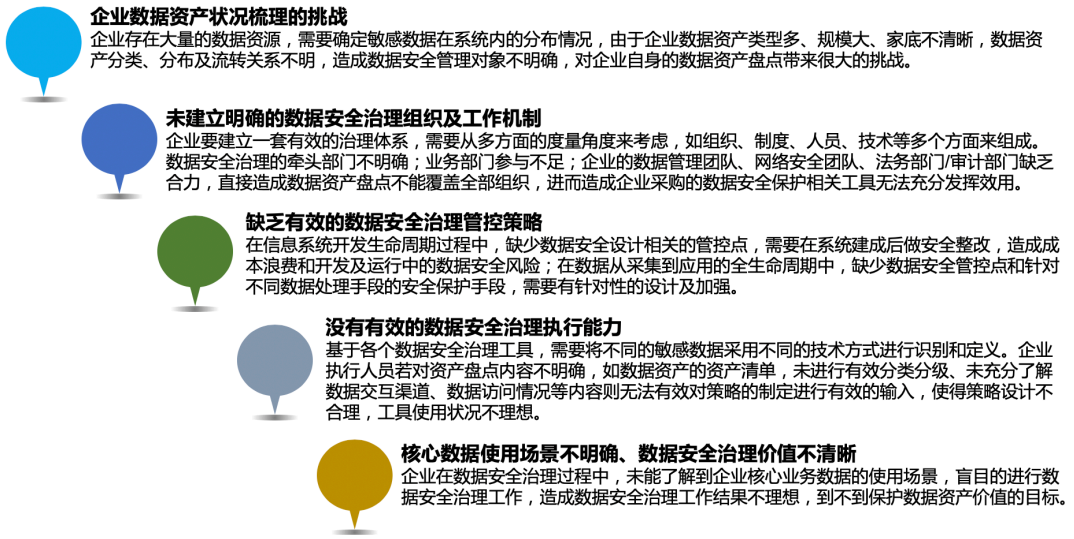
数据安全治理：数据安全治理是安全领域的框架集合，该集合包括数据、业务、安全、技术、管理等多个方面。数据安全治理属于数据治理体系中的一个过程（一部分），从组织、制度流程、技术工具、人员等维度形成自上而下全方位安全防护体系。其主要区别如下表：

区别	数据安全	数据治理	数据安全治理
三者关系	数据安全是一个广泛的定义，强调数据的保密性、完整性、可用性	数据治理包含数据安全治理	是数据治理的一部分，但是强调采用数据安全防护工具保证数据安全使用
目的不同	以网络与威胁为中心，对系统及自身数据进行保护	管理企业的数据资产，提升数据的价值	保证数据安全的使用
参与部门不同	多由IT部门独立承担，业务部门参与度较低	主要由IT部门发起、业务部门协同配合	主要由IT部门、法律部门、风险合规等部门发起、业务部门协同参与
核心不同	主要以技术驱动数字信息化；有明确的网络边界；注重技术流程，管理与技术分离明显	提升数据质量，保证数据规范	保证数据安全的使用，强调数据识别并进行分类分级，从而基于安全工具的策略进行有针对性的防护
产出不同	主要为各技术工具的数据防护策略	主要为元数据管理， 赋予数据上下文和含义的参考框架	数据资产清单，数据进行数据分类分级、敏感梳理数据分布情况、敏感数据资产的访问及控制情况等

数据安全、数据治理与数据安全治理区别对比

4、企业数据安全治理现状洞察

我们通过多年的数据治理工作，对所服务的企业客户数据安全治理挑战得出以下洞察：



5、数据安全治理原则

5.1 以数据为中心

以数据为中心，是保证企业数据安全的核心技术思想。

以数据为中心的安全，通过数据链作为主线，在数据的生命周期内各个不同数据处理环节所涉及的业务系统、运行环境、业务场景和人员等作为围绕数据安全保护的支撑。基于数据链，数据通过采集、流转、汇聚、存储、使用、销毁的各个阶段中数据面临的安全威胁以及对应的防护手段有可能很不一样。例如，在数据采集

阶段，我们应该对采集的数据进行识别，并对数据进行分类分级，同时还应考虑第三方数据提供源的身份验证等问题；在数据传输阶段，数据可能存在敏感信息在传输过程中数据泄露的情况；在数据存储阶段可能会因为数据访问权限控制不精确，导致未授权的用户访问到企业的敏感数据，或者存储设备丢失导致数据泄露等。企业应当考虑数据的不同阶段，从不同角度并全面的考虑企业数据面临的风险，建立强调整体数据安全而不是某个环节的数据安全能力。

5.2 面向组织全局

面向组织为全局，是数据安全治理的核心管理思想。

以组织为全局的数据安全治理，这个组织要对数据安全负责。不论数据在这个组织中的生命周期涉及多少产品业务或人员，单个系统、业务的安全问题不能足以衡量这个组织的数据安全。一个组织的数据安全水平，可以作为其是否符合法律要求、特定事件中具备怎样的责任、面向用户赢取信任、面向行业适合处理的数据类型和规模等的参考依据。政府或者行业可以以组织为单位进行数据安全管理，而不是某个产品的安全，一个组织要证明的是自己整个组织的数据安全水平，而不是自己的某个应用的安全。

5.3 能力建设为基础

数据安全能力成熟度是一种能力提升的方法。

评价一个组织的数据安全防护能力的高低，取决于该组织数据安全治理工作的各项工作的完成度，该完成度是建立在一个组织的数据安全能力成熟度等级基础之上的。

数据安全能力成熟度从组织建设、制度流程、技术工具及人员能力四个方面进行安全保障。同时根据数据生命周期安全中的7个数据过程共30个过程域来保证和促进企业数据安全能力等级的建设。结合数据安全能力成熟度的等级可以帮助企业结合本行业的数据敏感度特点决定哪些数据类型或者多大的数据规模需要建立在什么等级的数据安全能力水平，从而实现本行业的数据安全与发展的平衡；在数据开放环节中，数据拥有者有义务要求数据接收者提供等同于甚至高于数据拥有者自身数据安全防护等级的技术手段，从而避免数据在流动过程中未进行有效的数据保护，减少数据开放中的数据泄露风险等问题；组织也可以通过评估自己的数据安全能力成熟度水平，让组织了解自身的数据安全防护薄弱点，并进行能力提升，既可以建设更高的数据安全防护等级，同时也可以让消费者用更加客观量化的方法衡量自己是否值得信任。

5.4 场景化实施落地

以数据使用场景的数据安全是切入点。

我们在进行数据安全治理工作的时候，往往不知道从什么角度进行出发，以什么样的切入点进行数据安全治理工作，数据在整个生命周期中，每个数据流转的信

息系统、业务等过程均不相同，我们可以根据不同角色在不同业务场景下，研究主要的数据使用需求；在尽可能满足数据被正常使用的目标下，完成相应的安全要求和安全工具的选择。

比如在企业中，接触数据等人员可能是研发人员使用敏感信息进行开发测试，也可能是与外部合作机构进行数据共享，也可能是业务人员导出数据报表进行数据统计等，针对于这些不同的数据使用场景我们可以制定核心的数据安全防护策略，对于开发测试的研发人员，可以考虑对数据的脱敏；对于数据共享可以考虑对共享组织机构的身份验证、合同约束；对统计性人员可以考虑数据访问的身份验证、权限控制以及导出数据时敏感信息加密或脱敏等防护手段。

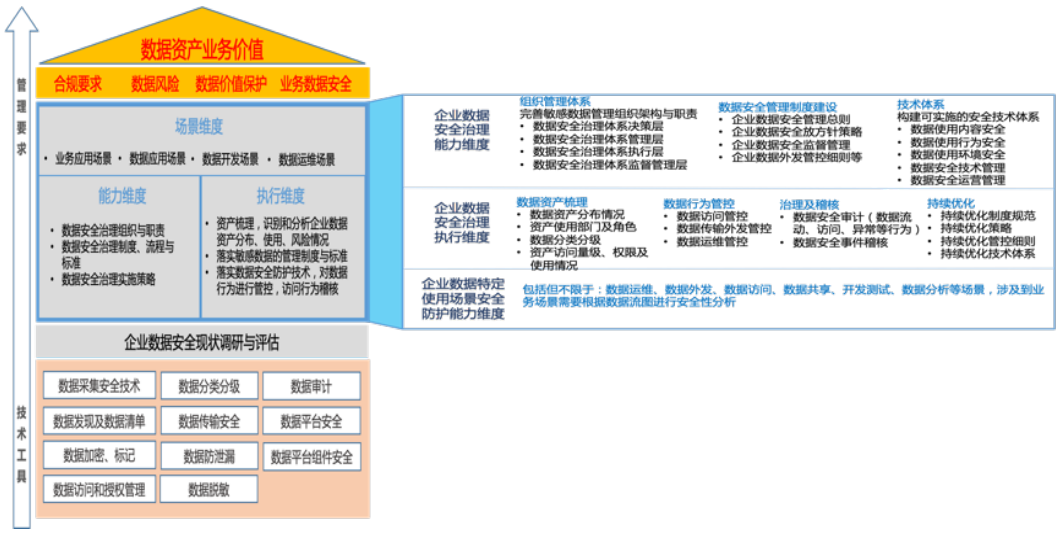
6、御数坊企业数据安全治理咨询服务

6.1 整体数据安全治理咨询服务

御数坊针对于企业数据安全治理的建设提供咨询服务，通过多年的协助企业用户进行数据治理工作，并结合长期从事网络安全、信息安全、数据安全领域从业人员，整合出一套适用于企业数据安全治理能力建设并可落地的一套咨询方案。

御数坊数据安全治理咨询服务旨在为企业用户建立并提升数据安全能力，我们通过多年的数据治理经验，参考数据治理模型如DAMA、DMM等模型并结合Gartner的

数据安全治理框架DSG、数据安全能力成熟度模型DSMM、持续自适应风险与信任评估模型CARTA、与基于场景下的数据流图的治理理念和启示，总结了符合企业数据安全治理建设的咨询方案，分为企业数据安全能力维度、企业数据安全治理执行维度、企业数据特定使用场景的安全防护能力维度。



御数坊数据安全治理体系框架

6.1.1 企业数据安全治理能力维度

6.1.1.1 数据安全能力现状调研与分析

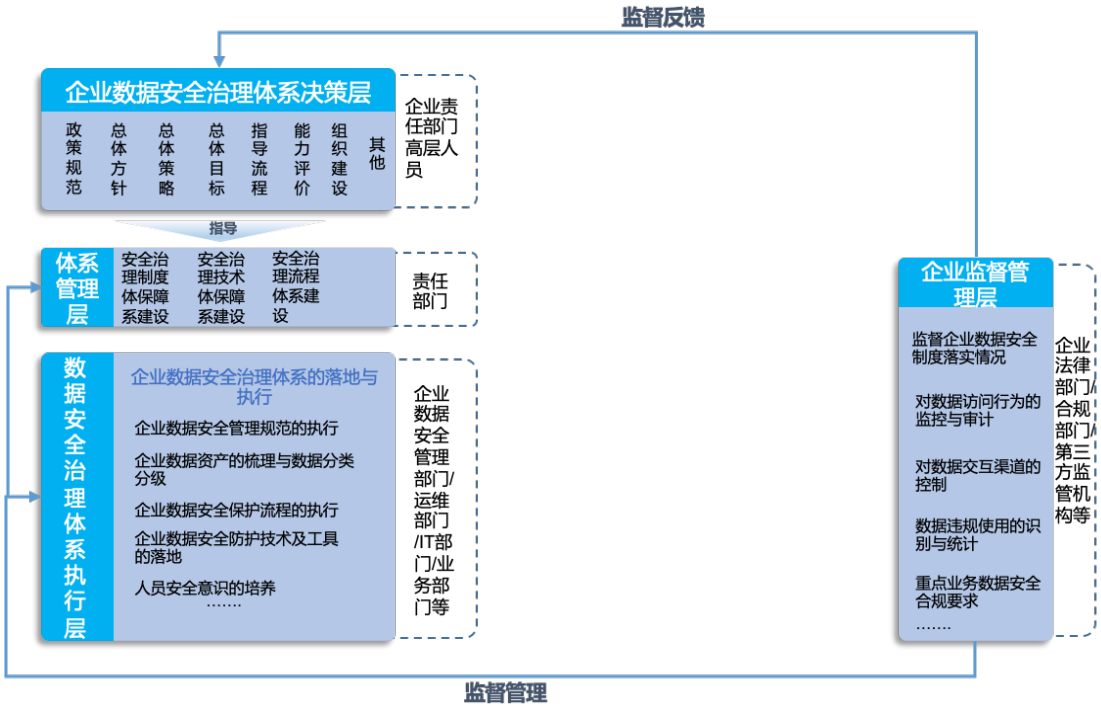
企业现状数据安全管理能力：对于企业数据安全管理能力的现状评估，主要从组织建设和安全运维管理两个方面进行。组织建设评估的内容，通过对现有数据安全部门组织结构、管理制度、流程、人员的解读，梳理出相关制度的缺陷并进行评估；安全运维层面从相关运维流程、数据备份流程、应急响应等内容进行综合评估及解读。

企业数据安全防护技术：从企业数据安全风险的范围进行评估，每个风险范围对应的数据安全防护技术不同，分为数据边界、物理边界、数据交互边界、人员管理边界、业务逻辑边界等，从每个边界采用的数据安全防护技术角度出发，综合考虑数据的安全风险。

企业数据使用场景：对于企业数据的使用场景，主要采用核心业务场景为主，通过对业务数据的流向、权限、使用场景的识别的拆解、并识别出数据使用场景的风险和脆弱性，根据风险点、数据泄露严重程度等内容进行综合考量，为后续制定合理的数据安全管理制度和数据防护技术工具的选型提供依据。

6.1.1.2 组织管理体系建设

数据安全组织管理体系主要从整个数据安全治理体系的建立角度出发，建立一套自上而下，从决策层到各部门的数据安全管理能力。



数据安全治理体系职能架构

御数坊为企业构建一套适用于企业自身的数据安全治理组织管理体系，自上而下分为决策层、管理层、执行层以及独立的监督管理层，从多维度保障数据安全治理的工作落实。

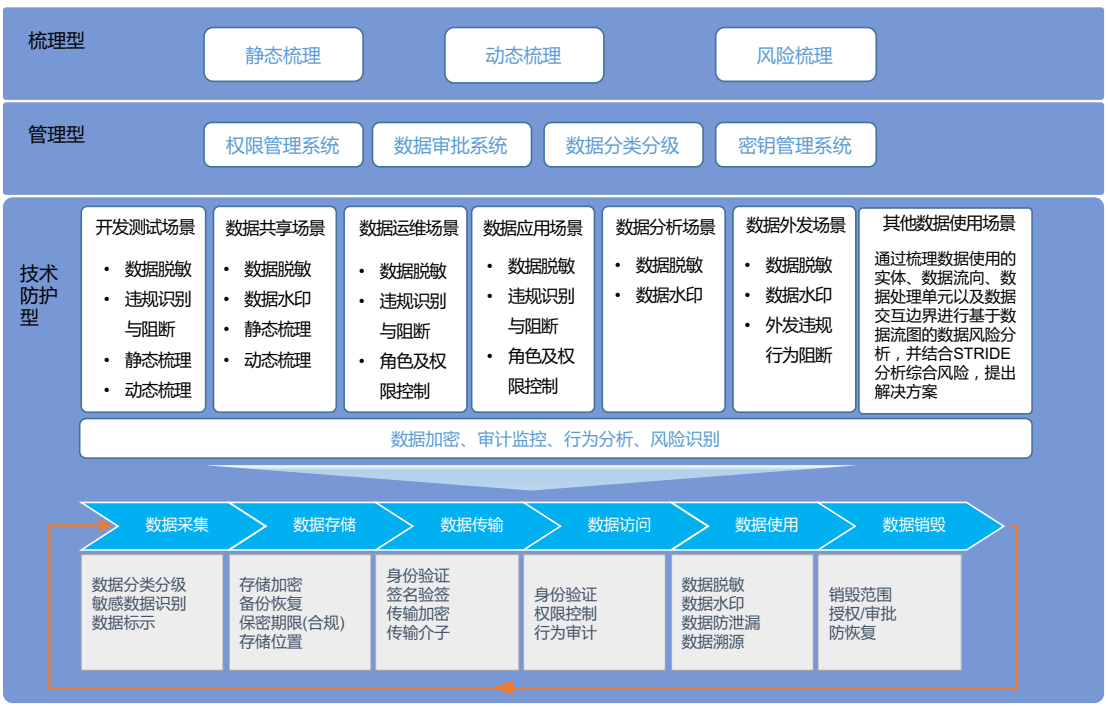
6.1.1.3 管理制度建设

通过之前对企业数据安全防护能力的现状评估、企业数据安全防护技术以及数据数据使用场景的识别、拆分，结合企业数据安全防护总体方针、策略制定相应的数据安全管理制度，并制定出对应的流程规范，如下：

安全策略类	数据安全风险防控要求
	数据安全保障总体策略
安全管理类	数据安全管理要求
	数据分类分级管理规范
	数据安全定级规范
数据安全运营类	数据安全运营要求
	数据安全事件应急响应
数据安全防护技术类	数据安全防护技术要求
	数据安全脱敏技术要求
合规测评类	数据安全运营管理合规性要求
	数据安全技术合规测评要求

6.1.1.4 技术体系建设

企业数据安全治理强调的是数据防护技术的运用，而不是不同产品的堆积和数据平台的建设，数据安全治理应将数据安全防护工具融入到数据使用场景中为目标，根据不同的数据使用场景采用对应的数据安全防护技术。



场景化的企业数据安全防护技术体系框架

6.1.2 企业数据安全治理执行维度

6.1.2.1 数据资产梳理

企业或单位在进行数据安全建设时，面临着企业数据资产分布状况不清、数据资产使用状况不明、数据资产安全状况未知这三大问题，这使企业数据安全防护部门无法开展行之有效的安全建设，也无法制定具有针对性的规章制度。

通过对企业数据资产的分布情况、数据资产使用情况、数据资产安全状况的了解，从而了解数据资产的分布情况、数据资产的访问及权限情况，并对数据资产进行分类分级。

6.1.2.2 数据分类分级

针对企业数据资产的梳理结果形成数据资产分类分级清单。对敏感数据的防护和管控应根据数据的使用角色、数据分类分级、数据的操作行为进行管控，其中：

数据使用角色：企业数据的角色管控应根据数据资产的使用角色、业务场景以及数据使用权限进行角色的划分，通过详细的、规范的角色定义，配合合理的数据权限，保证数据的安全性。

数据分类分级：通过之前的数据资产的梳理工作，充分了解企业的数据的资产分布、数据流转、数据访问情况等，对企业数据进行科学有效的数据分类分级，并结合企业的数据使用及开放标准，对各类别数据、各级别数据进行有效的管理策略。

6.1.2.3 治理稽核

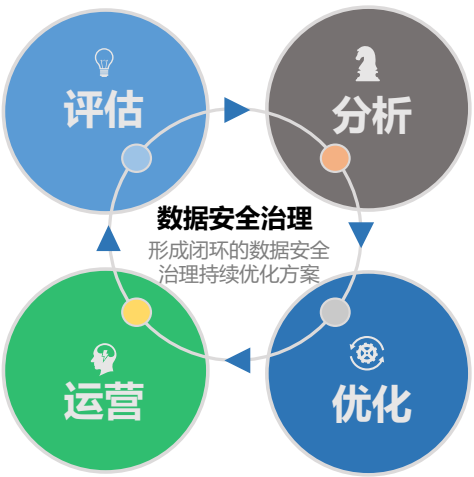
为保证企业数据安全治理工作的顺利进行，御数坊为企业用户建立了由数据安全治理权责机制、数据安全治理审查稽核机制组成的完善的数据安全治理质量保证方案。

数据治理认责机制：数据安全治理需要从更顶层的战略决策、更合理的认责安排及更严密的认责机制。企业应将参与数据要素市场的各方主体，包括但不限于主管部门、行业相关企业或组织、行业数据拥有者等，在治理体系中明晰的权利和责任作为企业数据安全治理体系框架的主线。

数据安全治理审查稽核机制：主要活动为对数据安全治理体系设计、建设和运行情况的监督、审计和评价，包括了监管部门的监督管理工作，安全审计部门的专项审计以及第三方机构的安全评估工作等，并向决策层、管理层按流程反馈体系运行情况及执行层的数据安全治理需求等，促进整个体系的持续优化。

6.1.2.4 持续优化

由于数据具有时效性，数据的保护策略也应与数据的生命周期进行绑定，一旦数据的重要性质的时效性已经消失，那么相应的防护策略也应进行调整。因此，数据安全治理体系的建设也并非一次可以完成，需要根据信息化建设的变化和政策的要求持续不断的完善，来应对可能发生的数据安全风险，满足政策的要求。



我们可以通过以下的优化过程来满足持续优化的要求，分别为“评估”、“分析”、“优化”、“运营”四个环节，形成闭环的数据安全治理持续优化方案。

6.1.3 企业数据待定使用场景的安全防护能力维度

企业在数据安全治理过程中，为了使数据安全治理工作结果理想化，应充分了解到企业核心业务数据的使用场景，不盲目的进行数据安全治理工作，应以完成保护数据资产价值为目标。对于数据的使用场景，应对核心业务场景进行识别，通过了解业务场景中的数据使用情况、数据流转情况、数据防护现状，然后对数据业务场景进行拆分，充分对数据的流转情况和使用情况进行风险的识别，最后再制定出对应的数据安全防护策略或技术工具的使用。

6.2 专项咨询服务

6.2.1 数据防泄漏专项

6.2.1.1 企业数据防泄漏误区

越来越多的企业对自身的数据安全逐步开始重视起来，已经有很多企业购买了数据防泄漏（DLP）产品，但是很少有企业将DLP产品用起来或者有效的用起来。我们经过调查和研究发现企业数据防泄漏产品使用效果不理想的原因主要有如下5点：

(1) 未建立明确的数据防泄漏治理体系

(2) 未建立明确的数据防泄漏管理矩阵

(3) 未对数据进行有效的分类分级

(4) 终端数据交互场景不清晰

(5) 未进行持续的优化改进

6.2.1.2 企业数据防泄漏治理过程

终端数据防泄漏咨询项目主要关键的实施阶段分为4个阶段，包括：企业数据防泄漏现状评估、企业终端数据资产梳理、企业数据防泄漏运营体系建立、数据防泄漏产品策略落地实施等。

6.2.1.3 御数坊数据防泄漏治理服务优势

多方人员参与，建立数据防泄漏治理体系：执行层和高级管理层的参与，以确保从数据防泄漏项目一开始就能保持一致的理解和认可，并对风险偏好有清晰的定义；业务和信息所有者参与验证数据防泄漏相关的制度和流程，将确保业务的稳定运行。法务部门的参与将确保遵循隐私相关要求。

专业人士的参与，明确数据防泄漏管理矩阵：针对于数据防泄漏专项治理项目成员御数坊聘用了拥有经验丰富的数据防泄漏厂商专家以及多年从事数据安全治理的专业顾问，梳理终端数据交互渠道，制定数据分类分级规范，制定数据防泄漏数据交互管理矩阵。

终端数据资产梳理，形成交互场景与分类分级资产清单：通过对数据防泄漏产品的深入了解，对企业各部门终端数据资产进行调研、收集，形成涵盖数据类型、级别、交互渠道、控制意见为一体的数据资产清单。

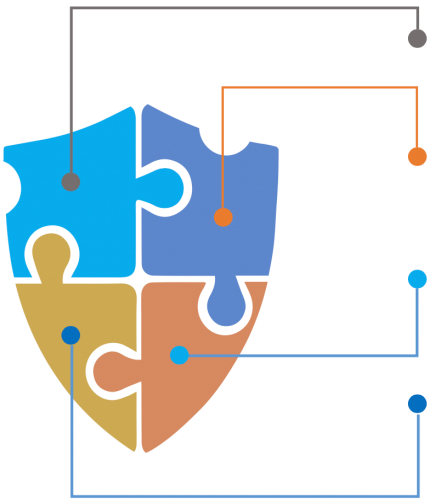
制定有效的数据防泄漏策略：制定有效的数据安全防护策略可以有效的保证数据安全，策略应根据数据的分类和级别、交互渠道、例外情况、控制措施进行有效的设定。

采用成熟的项目管理方法：御数坊有一套成熟的项目管理方法论，通过控制项目时间、降低项目成本、促进达成共识来降低项目的风险；保证数据标准与数据质量管理咨询项目的成功。我们通过期望值管理、风险及问题管理、项目成果管理、绩效指标管理、质量交流计划、质量审核程序和持续提高来保证项目质量，不断引导项目朝着客户的期望发展。

6.2.2 企业数据平台安全设计专项

随着数字化转型战略的启动，越来越多的企业采用构建属于自己的数据平台、数据中台来支撑企业自身的业务，而伴随着国家对于数据安全的法律法规的发布，逐步完善了对企业数据以及个人隐私数据的防护，这也就导致了企业在构建自身的数据平台时需要重点考虑数据的安全性。企业数据的安全保障目标是保护数据权属性、保密性、完整性、可用性、可追溯性，实现数据“可管、可控、可信”。保障对象为公司各领域数据资产（含数据资源、所涉及的数据中台及关联的数据处理设备）及用户隐私。

对于企业数据平台的安全能力设计，御数坊为企业用户从以下四个维度为用户的数据平台的安全能力做设计。



数据平台整体安全

构建数据平台系统安全体系架构可从平台网络域的角度划分为三个层次，由内而外分别是：平台台自身安全防护、系统内部安全防护和系统外部安全防护。

数据平台组件安全

在数据平台安全自身防护的基础上，增加安全的配置、安全组件和安全监控等，来增强对数据中台自身的安全防护能力，其中组件安全主要从数据采集组件、数据处理组件、数据存储组件等基于数据的采集、数据处理、数据存储、能力开放等环节进行安全考虑。

数据生命周期安全

数据平台上的数据安全需要根据数据生命周期进行安全管理，从数据采集、数据传输、数据存储、数据共享、数据使用、数据销毁的每个阶段提出安全防护需求。

核心业务场景数据安全

企业在构建数据平台时，应了解到企业核心业务数据的使用场景，并制定数据流图模拟数据流转方向，针对核心数据产生的业务价值考虑对应的数据安全方案，达到保护数据资产价值的目标。

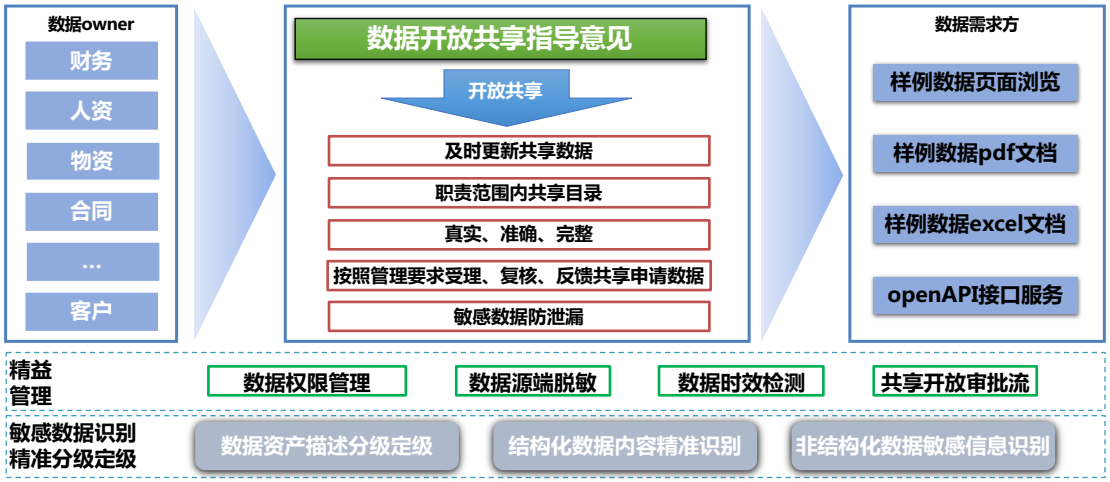
7、企业客户实践案例介绍

7.1 数据安全等级与数据共享-某国企

□ 项目概况

通过数据安全分级定级的实施，实时的监控并对大数据中心的结构化与非结构化数据进行数据安全等级的判定，结合数据权限的定制化落地形成了以数据安全分级为管理核心的数据运营平台。

同时助力客户获得数据治理领域4项大奖，在此领域的管理达到国际领先水平。



该公司数据安全定级和共享分类以业务对象为客体，融合整个企业架构和企业统一信息模型梳理设计的成果，将业务域根据公司数据中心的划分，包含安全、财务、公共、建设、人资、市场、物资、综合等多个域，每个域的数据按照《数据开放共享指导意见》进行安全数据使用，最后呈现到数据需求方。

□ 数据安全分级

- 御数坊通过数据资产梳理工具DGOffice对企业数据资产进行梳理，形成对数据资产的自动分类分级，减少人员参与成本，最终形成数据安全定级、流程与岗位三位一体的认责机制。
- **数据安全等级**：根据公司数据安全分级策略，包含安全一级、安全二级、安全三级、安全四级等4个级别；
- **数据共享类别**：根据公司数据安全共享策略，包含普通可共享、有条件共享、不予共享等3类；

- **数据共享条件**：仅针对有条件共享类，须经过责任部门审批许可后方可共享；
- **依据**：主要是《网络安全法》、《央企商密保护规定》、《消费者权益保护法》等法律法规；
- **责任部门/单位**：数据信息的归口管理业务部门。

☐ 数据安全相关规范

- 《数据安全定级规范》、《数据安全分级定级术语》

根据数据的安全分类定级，与数据共享使用场景进行数据开放使用的标准设定，是规章制度的编写基础。

☐ 实践总结

通过该公司的数据安全定级与数据共享场景的结合，我们可以看到数据的分级是企业数据重要性的直观化展示，是组织内部管理体系编写的基础。其实，数据的分类与分级也是技术支撑体系落地实施的基础，针对不同类型不同级别的数据，采用不同的防护方案，形成细粒度数据的安全管控及防护能力，有助于企业数据的安全保障。

7.2 数据防泄露专项治理-保险行业

☐ 项目背景

为应对日益增长的终端数据泄漏风险，保障某保险集团业务数据的安全、满足外部法律法规监管对数据安全的要求，该保险公司客户数据信息中心已完成数据防泄漏项目一期的实施，一期主要为集团总部数据防泄漏产品的实施部署以及客户端的部署，项目二期涵盖各子分公司层面及覆盖至四级机构，能够覆盖全集团所有数据传输通道，更为全面地监控集团敏感数据泄漏风险，实现对敏感数据外发的告警、阻断与全面管理。此次数据防泄漏咨询服务专项主要为二期项目。

☐ 项目主要内容

1. 开展终端数据防泄漏现状评估：对集团及子公司当前数据防泄漏管理现状开展快速的风险评估，识别集团与子公司层面数据防泄漏管理层面缺失和技术层面的缺陷，为开展子分公司数据防泄漏工作制定详细计划。
2. 执行各子公司数据分类分级：对子公司进行数据分类、分级工作，并将其做为落实数据安全差异化、精细化管控措施的基础。
3. 建立数据防泄漏体系：明确集团针对子分公司数据安全管理职责，建立常态化的监督、检查机制。
4. 协助子公司数据防泄漏产品的落地：配合数据防泄漏产品落地，建立、完善数据防泄漏运维流程。

☐ 项目难点

此次项目主要有两点难点：

1. 终端数据资产收集难度较大
2. 数据防泄漏体系设计缺乏参考

由于数据防泄漏产品的性质，数据资产的收集存在一定的难度，使用自动化收集工具不能有效的收集到终端数据，同时数据防泄漏厂商对于防泄漏产品的实施部署具有丰富的经验，但是由于在行业内未有单独关于数据防泄漏体系的设计，数据防泄漏厂商未能为用户提供相关设计，对于组织建设、流程设计、运维设计缺乏参考性依据。一般咨询公司对于数据防泄漏产品功能特性了解程度较低，不能针对于产品特性进行针对性体系设计。

☐ 项目执行过程及交付物

对于此次该保险行业的数据防泄漏咨询服务专项，御数坊聘用具有丰富经验的数据防泄漏产品厂商的安全专家与多年从事数据治理的专业顾问，结合数据防泄漏产品的特性，制定出终端数据调研表，以部门为单位对终端数据进行收集，重点对终端进行数据资产的收集，对数据交互渠道、数据传输例外、数据访问敏感岗位、以及组织对收集的数据重视程度进行终端数据资产盘点，并进行企业数据防泄漏风险评估工作，为用户建立一套从人员构成、管理规范、制度流程的自上而下的数据防泄漏体系。

☐ **终端数据防泄漏现状评估：**

- 企业数据安全（防泄漏）现状体系评估报告
- 企业敏感数据操作岗位清单
- 企业数据外发例外情况清单
- 各类数据级别数据交互渠道矩阵

☐ **数据分类分级工作执行：**

- 终端数据收集清单
- 数据分类表
- 数据分级表
- 筛查标准、应急预案等

☐ **数据防泄漏体系建立：**

- 数据防泄漏运维组织架构
- 终端数据防泄漏相关管理制度
- 终端数据防泄漏运营状态检查机制
- 数据防泄漏防护策略
- 数据防泄漏平台操作手册

☐ **终端数据防泄漏运维管理：**

- 例外策略流程、权限、策略变更流程、数据外发审批流程等

☐ 实践总结

从数据防泄漏就可以看出有效的数据防泄漏体系包含组织结构、制度规范、管理流程、数据事件筛查与稽核等工作，这进一步体现出了数据安全治理工作需要从组织保障、制度保障、技术保障、人员保障四个维度保证数据安全。

参考文献：

大数据风险：http://www.qianjia.com/zhike/html/2020-01/14_19145.html

数据安全建设思路：https://www.secrss.com/articles/13551

数据安全治理深入业务流程：https://blog.csdn.net/llawliet0001/article/details/88916491

数据安全治理基本思路：http://www.itongji.cn/detail?type=1018

御数坊（北京）科技咨询有限公司

专注于数据治理领域咨询和软件服务机构

以“咨询服务+软件产品”的方案为企业提供全生命周期的数据治理解决方案，以“标准化、智能化、网络化”的理念实现SAAS+AI的数据治理产品创新，打造出拳头产品“DGOffice”，帮助客户真正建立数据治理能力，建立数据资产目录对多源异构数据进行标准化，提高数据中台数据质量，创造数据资产价值。成立5年服务于多家家500强企业，行业覆盖能源、通信、金融、政府等众多领域。

1、数据治理体系规划

2、数据管理能力评估

3、数据管理专项咨询

4、数据专业人才资质认证

联系我们
邮箱：marketing@dgworkshop.com.cn
网址：http://www.dgworkshop.cn
咨询电话：13581752030
地址：北京市海淀区中关村大街甲6号铸诚大厦706室
邮编：100086

御数坊公众号


御数坊
DGWorkshop