

| 证券研究报告 |

数据安全框架报告

安全产业研究 框架系列之一：

2024.2.18

分析师：苏仪
执业证书编号：S0740520060001
Email: suyi@zts.com.cn

摘要

- 在国家政策引领、地方试点推进、企业主体创新等多方合力下，我国数据要素市场不断探索和创新，AIGC对数据的需求快速增长，共同驱动数据安全市场规模持续扩大，竞争格局多元化发展。
 - ✓ 近些年，我国数据安全法治治理体系建设取得重要进展，数据安全治理进入“标准化”法治时代，利好政策不断；
 - ✓ 多省级数据局开年密集揭牌，数据安全产业作为配套工程乘风提速；
 - ✓ 预计到2025年，我国数据安全产业规模超过1500亿元，年复合增长率超过30%。
- 当前，AIGC的海量数据需求为数据安全合规治理带来新变化、新需求。数据脱敏、身份认证与访问控制等技术常用于保护隐私信息不被泄漏，以确保数据的安全性和合规性。
- 展望未来，数字经济推动数据价值释放、数据量激增与AIGC跨越式发展均对数据安全提出了更高的要求，我国将持续构建更加科学的数据安全合规治理制度体系，切实筑牢数据安全屏障，数据安全产业将得到进一步发展。
- **风险提示：**AI进展不及预期带来下游需求不及预期的风险；市场竞争加剧的风险；政策落地不及预期的风险；研究报告中使用的公开资料可能存在信息滞后或更新不及时的风险等。



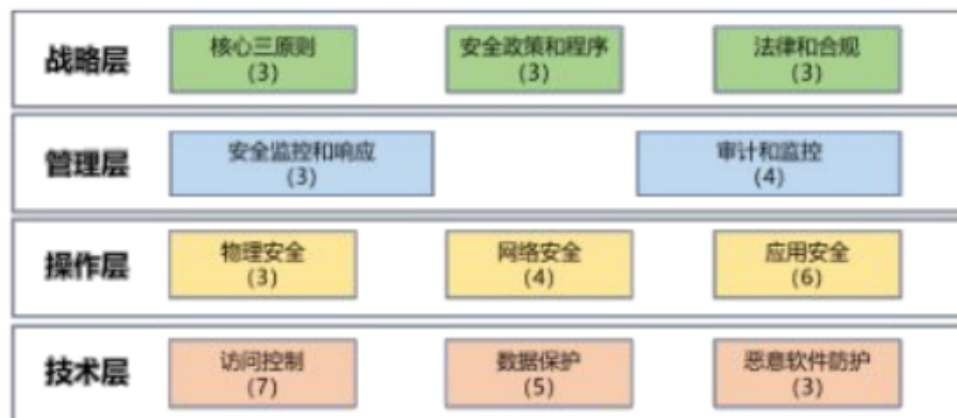
1

数据安全概述

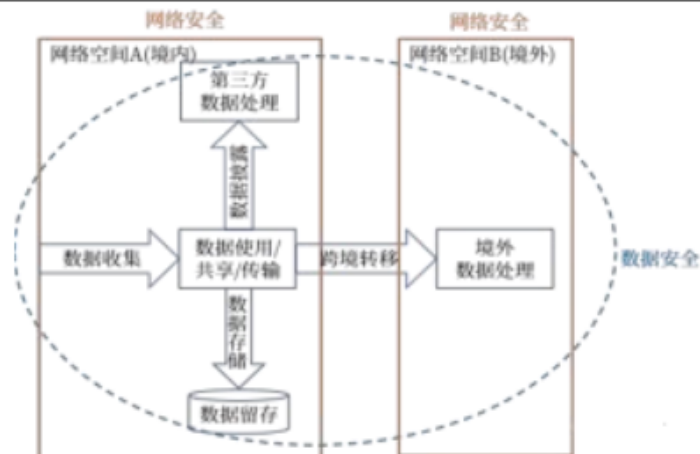
1.1 数据安全/网络安全/信息安全/数据资产安全的定义及关系

- **数据安全**：指保护数字数据免受未经授权访问、泄露、破坏或丢失的过程和技术，包括一系列的措施、策略和程序，旨在保护数据的保密性、完整性和可用性，侧重于数据的全生命周期内的安全与合规。
- **网络安全**：一个网络系统不受任何威胁与侵害，能正常地实现资源共享功能，侧重于计算的资源与环境，具有边界。
- **信息安全**：强调信息本身的安全，以信息的机密性、完整性、可用性（CIA）三大基本属性为保护核心，辅以信息的不可否认性（抗抵赖性）、真实性、可控性等扩展属性等保护，侧重于保护一切有价值的信息。
- **数据资产安全**：数据安全3.0时代进入到体系化数据安全治理时代，数据上升到资产，基础设施层面。数据资产的安全重点转为保护具有业务价值的数据；面向数据资产的保护意味着面向企业业务的保护。
- **关系**：数据安全是信息安全的核心，可将网络安全理解为手段，数据安全和信息安全理解为目标。

图表：数据安全基本概念框架图



图表：网络安全和数据安全的范围



1.1 2023年最具影响力的十大网络安全事件

■ 信息化浪潮席卷全球的背景下，全球网络安全事件频发。2023年发生的创记录的数据泄露、勒索软件、零日漏洞、间谍软件和供应链攻击事件为2024年全球网络安全威胁态势定下了主旋律和基调，同时也为网络安全专业人士制定风险管理策略和目标提供重要参考。

图表：2023年最具影响力的十大网络安全事件

序号	事件性质	事件	事件概述
1	杀伤半径最大的供应链攻击	MOVEit Transfer数据盗窃攻击	攻击者利用MOVEit Transfer服务器曝出的漏洞入侵并下载用户存储的数据。
2	技术最复杂的间谍软件攻击	三角测量	针对苹果iPhone设备的间谍软件活动，利用了多达四个零日漏洞。
3	金融业最具影响力的安全事件	工商银行美国子公司被LockBit勒索软件攻击	攻击导致部分系统中断，攻击者可能利用了未及时修补的Citrix Bleed漏洞。
4	最严重的医疗数据泄露事件	23andMe数据泄露	基因检测提供商23andMe遭遇撞库攻击，导致重大数据泄露。
5	最严重的云数据安全事故	丹麦云服务商丢失所有用户数据	丹麦托管服务商被勒索软件攻击加密了大部分客户数据且数据恢复不成功。
6	最严重的游戏业网络安全事件	GTA5源码泄露	Lapsus\$入侵了Rockstar游戏，获得了对Rockstar内部Slack服务器和Confluencewiki的访问权限，并窃取了大量机密数据。
7	对科技行业威胁最大的DDoS组织	匿名苏丹	“匿名苏丹”黑客组织的DDoS攻击瘫痪了多家全球科技巨头的网站和服务。
8	影响最大的在线金融服务数据泄露事件	PayPal撞库攻击	撞库攻击：黑客收集大量网络上已经泄露的某网站的用户名和密码去登陆另一个网站。
9	最严重的博彩业黑客攻击	米高梅度假村网络攻击导致IT系统关闭	BlackCat附属机构在事件期间对100多个ESXi虚拟机管理程序进行了加密。
10	影响最大的军工企业安全事件	波音遭LockBit勒索软件攻击	LockBit在数据泄露站点发消息声称窃取了波音的大量敏感数据。

资料来源：清华大学智能法治研究院公众号，中泰证券研究所

1.2 数据安全的原则

■ 根据DAMA，数据安全的原则包括 6 个方面：

- **协同合作：**数据安全是一项需要协同的工作，涉及IT安全管理员、数据管理专员/数据治理、内部和外部审计团队以及法律部门。
- **企业统筹：**运用数据安全标准和策略时，必须保证组织的一致性。
- **主动管理：**数据安全管理的成功取决于主动性和动态性、所有利益相关方的关注、管理变更以及克服组织或文化瓶颈，如信息安全、信息技术、数据管理以及业务利益相关方之间的传统职责分离。
- **明确责任：**必须明确界定角色和职责，包括跨组织和角色的数据“监管链”。
- **元数据驱动：**数据安全分类分级是数据定义的重要组成部分。
- **减少接触以降低风险：**最大限度地减少敏感/机密数据的扩散，尤其是在非生产环境中。

图表：侧重于数据本身的安全属性时数据安全的原则（CIA数据安全三要素模型）



1.3 数据安全活动的目标&数据安全的主要活动

■ 根据DAMA定义，数据安全活动目标主要包括三个方面：

- 支持适当访问并防止对企业数据资产的不当访问。
- 支持对隐私、保护和保密制度、法规的遵从。
- 确保满足利益相关方对隐私和保密的要求。

■ 数据安全的活动包括六个阶段：识别数据安全需求、制定数据安全政策、定义数据安全标准、评估当前安全风险、实施数据安全控制、实施数据安全审计。

图表：数据安全的六大主要活动



1.3.1 数据安全的主要活动——识别数据安全需求、制定数据安全政策

- **识别数据安全需求：**降低风险和促进业务增长是数据安全活动的主要驱动因素。
 - 确保组织数据安全，可降低风险并增加竞争优势。
 - 全面了解组织的业务需求是在组织内实施数据安全的第一步，组织的业务需求、使命、战略和规模以及所属行业，决定了所需数据安全的严格程度。
- **制定数据安全政策：**数据安全政策是组织为保护其数据资产而制定的一系列正式文档，定义了组织如何管理、保护和处理数据，包括对员工的行为规范、技术控制措施、以及对违反政策行为的处理方式。

图表：数据安全需求的来源



图表：数据安全政策的制定步骤和内容



1.3.2 数据安全的主要活动——定义数据安全标准、评估当前安全风险

- **定义数据安全标准：**政策指导行为准则，但未覆盖所有特殊情况。
 - 标准作为政策的补充，为如何达成政策旨趣提供了更具体的说明。
- **评估当前安全风险：**评估数据安全风险指的是通过系统的方法识别和评价可能威胁组织数据安全的各种因素，以及这些威胁可能导致的后果，此过程包括确定数据资产、潜在的威胁、可能的漏洞及这些因素可能导致的风险水平。

图表：评估当前安全风险的主要步骤

识别和分类数据资产

采用人工梳理或专门的软件扫描整个网络和系统，识别存储的数据。基于重要性和敏感性，对扫描到的数据进行分类标识，可以由人工标识，也可以采用AI自动标识。

资产编号	数据库名称	表名称	字段名称	存储位置	数据类型	敏感性	重要性
DB001T1F1	客户信息系统	客户详情	客户ID	服务器1-数据中心A	整型	低	高
DB001T1F2	客户信息系统	客户详情	客户姓名	服务器1-数据中心A	字符型	中	高
DB002T1F1	员工管理系统	员工个人资料	员工ID	服务器2-数据中心B	整型	低	高
DB002T1F2	员工管理系统	员工个人资料	职位	服务器2-数据中心B	字符型	低	中
DB003T1F1	产品管理系统	产品设计	产品代码	服务器3-数据中心C	字符型	低	高
DB004T1F1	销售数据库	销售记录	销售金额	云存储服务A	浮点型	低	高
DB005T1F1	网站分析工具	访问日志	访问时间	服务器4-数据中心A	日期时间型	低	中

识别潜在威胁

基于数据安全政策和数据安全标准对各类数据的保护要求，对照当前各类数据安全保护的现状，确定组织数据安全在技术、流程和政策上可能存在的弱点，比如通过系统漏洞扫描、web漏洞扫描、数据库漏洞扫描等举措、及时发现存在的问题。

评估影响和可能性

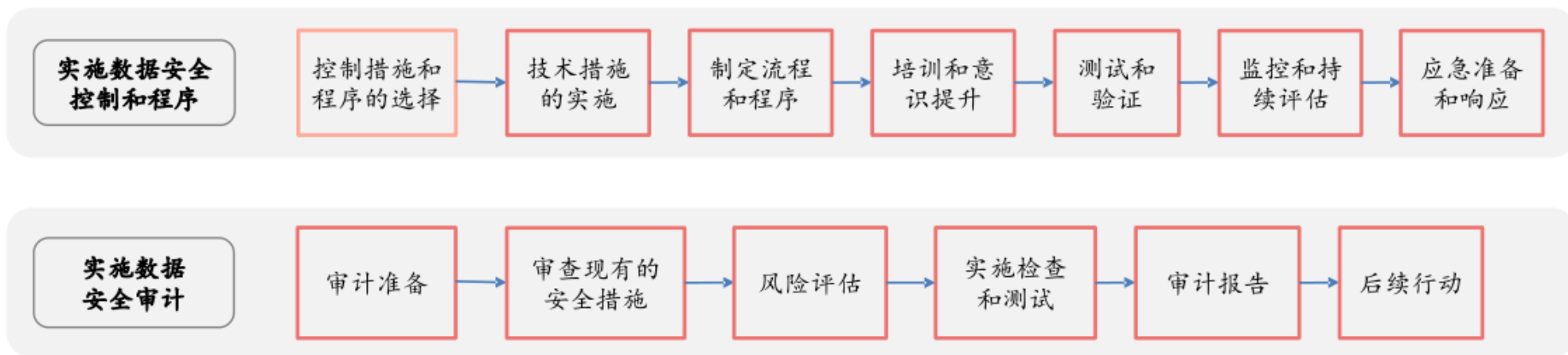
分析数据安全事件发生的可能性和其对组织造成的潜在影响。简化的数据安全风险评估表格样例：

数据资产	威胁源	漏洞	影响程度	发生可能性	风险等级	应对措施
客户支付信息	网络黑客攻击	未加密的数据传输	高	中	高	实施端到端加密通讯
员工个人信息	内部数据泄露	弱密码策略	中	高	中	提供培训教育和员工意识
商业机密文档	竞争对手间谍活动	缺乏访问控制	高	低	中	实施严格的访问控制审计
产品设计图纸	物理盗窃	不安全的文件存储	高	低	中	使用物理安全措施

1.3.3 数据安全的主要活动——实施数据安全控制措施和程序、实施数据安全审计

- **实施数据安全控制措施和程序：**在评估了数据安全的风险后，需要将数据安全政策和数据安全标准的要求转化为实际的控制措施和程序。
- **实施数据安全审计：**数据安全审计是一种详细的检查和评估过程，旨在评价组织内的数据保护措施的有效性，确认是否符合特定的安全标准和法规要求，并确保数据安全政策得到妥善执行。
 - 此过程涉及对组织内的数据访问、处理、存储和传输控制的审查，以识别潜在的安全漏洞和不规范操作。

图表：实施数据安全控制和程序、实施数据安全审计的步骤



1.4 数据全生命周期的安全防护实现数据安全治理有效闭环

- **数据安全活动：**宏观层面上对数据安全的管理和控制进行阐述，利于确保数据安全整体策略和流程的连贯性和一致性。
 - 数据安全活动的每一个步骤都可以拆分为数据采集、传输、存储、处理、交换和销毁六个方面来进行阐述。
- **数据全生命周期安全防护：**更为微观，其从数据本身出发，将注意力集中在数据采集、传输、存储、处理、交换和销毁等各个阶段，通过关注数据在其生命周期中的每一步如何被保护，可以提供更细致、更具体的安全措施和实践，有助于确保在数据的每一个环节都实现安全性。
- **两种视角相互补充实现数据安全的持续改进和适应性发展。**
 - 宏观策略为微观实施提供方向和框架，微观实施的反馈和经验可以用来优化宏观策略。

图表：数据全生命周期安全防护的六个阶段及20项内容



1.5 数据安全的检测清单

图表：数据安全的检测清单

	检查项	检查点	检查类别		检查项	检查点	检查类别
1.组织保障	a1.机构职责	a11.明确数据安全管理部门	文档检查	2.制度建设	投诉处理	有效举报线索处置和记录	文档检查
		a12.明确部门管理职责	文档检查			数据安全教育培训制度	访谈、文档检查
	a2.岗位人员	a21.人员配备	访谈、文档检查		教育培训	数据安全教育培训周期	文档检查
		a22.数据安全岗位职责	访谈、文档检查			数据安全教育培训人员	文档检查
		数据分类分级策略和标准	访谈、文档检查			数据安全教育培训内容	文档检查
2.制度建设	分类分级	针对性的安全管理 及技术保障策略	文档检查	3.技术能力	数据加密	数据的传输加密	访谈、文档检查
			登陆检查			数据存储加密	安全测试
	安全评估	数据安全评估整体要求	访谈、文档检查		数据脱敏	数据脱敏处理	访谈
		重点业务评估定期评估	访谈、文档检查			业务系统账号管理	访谈、文档检查
	监测巡查	数据安全日常监测巡查	文档检查		操作权限管理	业务系统访问授权	登陆检查、安全测试
			登陆检查				安全测试
	应急响应	应急预案及演练	访谈、文档检查		业务系统访问授权	业务系统访问授权	访谈、文档检查
		数据安全事件处置	访谈、文档检查			业务系统访问授权	访谈、文档检查
	数据安全监督检查	数据安全监督检查制度	访谈、文档检查		业务系统访问授权	业务系统访问授权	访谈、文档检查
	投诉处理	数据安全投诉处理制度	访谈、文档检查			业务系统访问授权	访谈、文档检查
		公开举报投诉渠道	文档检查			业务系统访问授权	访谈、文档检查

资料来源：安全架构公众号，中泰证券研究所

1.5 数据安全的检测清单

图表：数据安全的检测清单

	检查项	检查点	检查类别		检查项	检查点	检查类别
3.技术能力	操作权限管理	业务系统访问授权	安全测试	4.重点环节	用户个人信息收集	信息采集合法正当	登陆检查
			访谈、文档检查			信息采集最小化原则	访谈
		运维支撑人员操作权限	登陆检查				安全测试
			安全测试				文档检查
	数据流动	数据流动记录	文档检查			信息采集目的用途	访谈、文档检查
		重点环节日志留存管理	文档检查				登陆检查
	人员操作日志记录	日志记录完整、准确	登陆检查、文档检查				登陆检查
		日志留存时间要求	访谈				访谈
			登陆检查		数据使用	去标识化处理	访谈、登陆检查1
	数据备份与恢复	数据备份和恢复	访谈、文档检查				访谈、登陆检查2
	安全风险监测	企业内部数据安全风险监测	文档检查				登陆检查1
	数据安全事件溯源	数据安全事件溯源记录	登陆检查				登陆检查2
	数据接口安全		访谈、文档检查			敏感数据操作权限	访谈、文档检查
		接口安全	文档检查、安全测试				安全测试
			安全测试				访谈、文档检查
	用户个人信息收集	信息采集合法正当	访谈、文档检查		三方合作	合作方监督管理	登陆检查

资料来源：安全架构公众号，中泰证券研究所

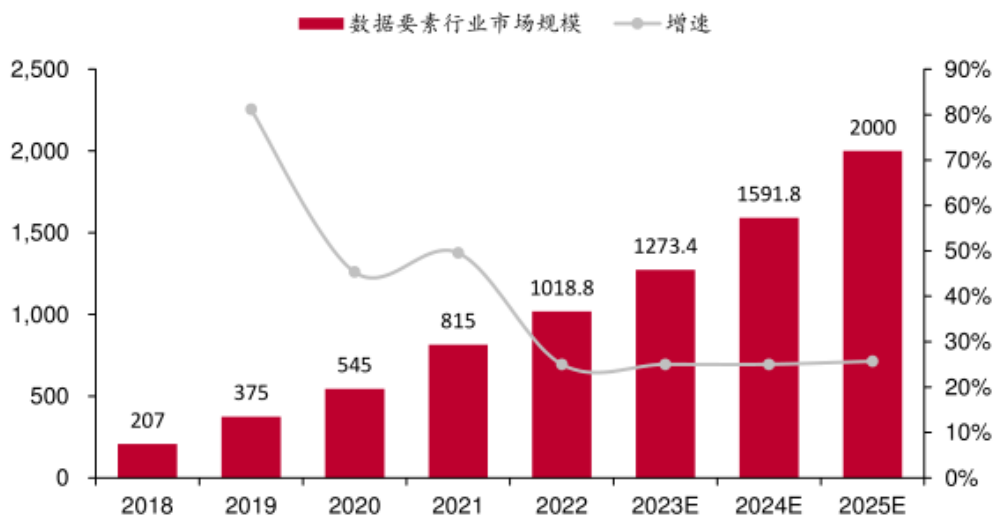
2

数据要素驱动 打造安全合规的数据底座

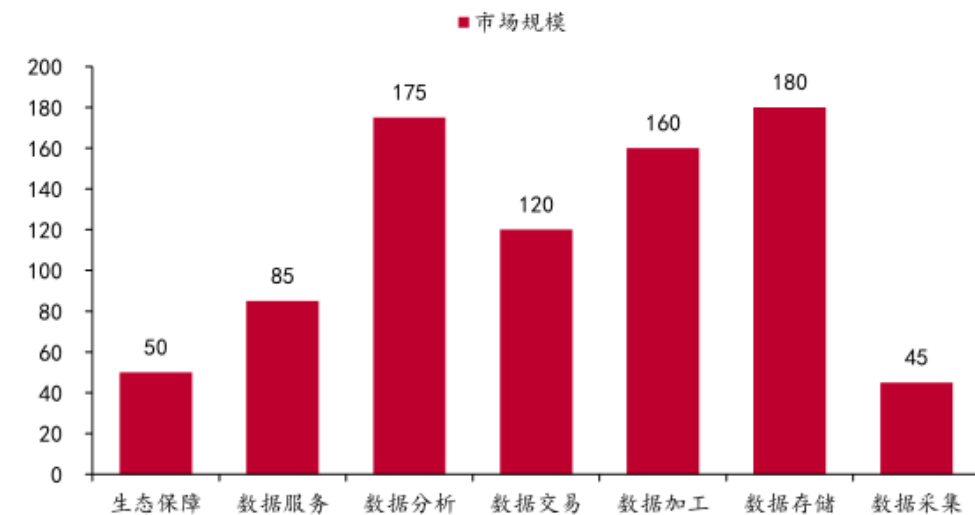
2.1 数据要素市场蓬勃发展，规模持续扩大

- 在国家政策引领、地方试点推进、企业主体创新等多方合力下，我国数据要素流动势能不断积聚，数据基础设施不断完善，数据要素市场不断探索和创新，步入高速增长阶段。2021年我国数据要素市场规模约为815亿元，预计“十四五”期间市场规模复合增速将超过25%，到2025年规模有望接近2000亿元。
- 产业发展方面，全国数据交易机构逐步升级优化，服务模式和服务内容不断创新，各地围绕数据要素市场培育的路径和模式各具特色，数据要素市场交易机构、运营体系、保障机制初具雏形。
- 在流通实践层面，数据资源基础较好的领域及行业基于先期优势，逐步形成细分领域数据要素市场差异化特征。

图表：2018-2025E 中国数据要素行业市场规模（单位：亿元）



图表：2022 年中国数据要素市场规模（单位：亿元）



资料来源：国家工业信息安全发展研究中心，中商产业研究院，中泰证券研究所

资料来源：国家工业信息安全发展研究中心，中泰证券研究所

2.2.1 数据要素利好政策持续释放，助力市场活力加速迸发

■ **国家战略全方位布局数据要素发展。**近年来，我国高度重视数据要素及其市场化配置改革，陆续出台了多项数据要素相关政策文件，数据要素已成为经济高质量发展的重要支撑。目前，我国数据要素政策体系架构已初步形成，“数据二十条”为推动数据要素发展筑牢政策基础，数据要素统筹管理、协调发展的体制机制将进一步完善。

图表：中国数据要素政策

时间	发布机构	主要政策	主要内容
2022.01	国务院	《“十四五”数字经济发展规划》	到2025年，数据要素市场体系初步建立。数据资源体系基本建成，利用数据资源推动研发、生产、流通、服务、消费全价值链协同。数据要素市场化建设成效显著，数据确权、定价、交易有序开展，探索建立与数据要素价值和贡献相适应的收入分配机制，激发市场主体创新活力。
2022.04	国务院	《中共中央国务院关于加快建设全国统一大市场的意见》	加快培育数据要素市场，建立健全数据安全、权利保护、跨境传输管理、交易流通、开放共享、安全认证等基础制度和标准规范，深入开展数据资源调查，推动数据资源开发利用。
2022.09	国务院	《全国一体化政务大数据体系建设指南》	鼓励依法依规开展政务数据授权运营，积极推进数据资源开发利用，培育数据要素市场，营造有效供给、有序开发利用的良好生态推动构建数据基础制度体系。
2022.12	中共中央、国务院	《关于构建数据基础制度更好发挥数据要素作用的意见》（简称“数据二十条”）	本次意见提出“数据二十条”，主要包括以下几方面内容：1)建立保障权益、合规使用的数据产权制度；2)建立合规高效、场内外结合的数据要素流通和交易制度；3)建立体现效率、促进公平的数据要素收益分配制度；4)建立安全可控、弹性包容的数据要素治理制度等。
2023.01	工业和信息化部等十六部门	《关于促进数据安全产业发展的指导意见》	到2025年，数据安全产业基础能力和综合实力明显增强，产业规模迅速扩大。优化创新资源要素配置，促进以数据为关键要素的数字经济健康快速发展，加速数据要素市场培育和价值释放。
2023.02	中共中央、国务院	《数字中国建设整体布局规划》	到2025年，基本形成横向打通、纵向贯通、协调有力的一体化推进格局，数字中国建设取得重要进展。数字基础设施高效联通，数据资源规模和质量加快提升，数据要素价值有效释放。
2023.03	中共中央、国务院	《党和国家机构改革方案》	组建国家数据局。负责协调推进数据基础制度建设，统筹数据资源整合共享和开发利用，统筹推进数字中国、数字经济、数字社会规划和建设等，推进数据要素基础制度建设、推进数字基础设施布局建设等职责划入国家数据局。
2023.08	财政部	《企业数据资源相关会计处理暂行规定》	规范了企业数据资源相关会计处理，同时强化了相关会计信息披露。
2024.01	国家数据局等17部门	《“数据要素×”三年行动计划（2024—2026年）》	到2026年底，数据要素应用广度和深度大幅拓展，在经济发展领域数据要素乘数效应得到显现，打造300个以上示范性、显示度高、带动性广的典型应用场景，涌现出一批成效明显的数字要素应用示范地区，数据交易规模倍增，推动数据要素价值创造的新业态成为经济增长新动力。

资料来源：政府网站，中泰证券研究所

2.2.2 数据要素领域相关标准有效促进市场标准化体系建设

■ 数据要素流通是数字经济时代重要研究内容，数据要素流通标准化工作是建立统一开放、竞争有序的数据要素市场的本质内在要求。数据要素体系标准化将有效促进数据要素市场体系建设，充分发挥数据要素作用。

- 国家层面，数据要素供给侧数据存储、数据共享开放、数据分类等已经发布了国家标准；
- 地方层面，各省市积极开展数据要素流通标准研制工作，抢抓国家推动数据价值化新机遇、培育数据要素市场。

图表：数据要素领域相关标准

	实施日期	标准号	标准名称	主要内容
国家标准	2024.03	GB/T 35274-2023	信息安全技术 大数据服务安全能力要求	规定了大数据服务提供者的大数据服务安全能力要求，适用于指导大数据服务提供者的大数据服务安全能力建设，也适用于第三方机构对大数据服务提供者的大数据服务安全能力进行评估。
	2024.03	GB/T 42884-2023	信息安全技术 移动互联网应用程序（App）生命周期安全管理指南	立足于移动应用安全管理工作，避免开发引入或管理不当造成如恶意代码攻击、应用程序漏洞、用户隐私数据泄露、数据保护不当等安全威胁，为App提供者在App开发、运营等生命周期的安全管理提供指导，同时为App分发平台管理者和移动智能终端厂商等管理App提供参考。
	2024.03	GB/T 42888-2023	信息安全技术 机器学习算法安全评估规范	明确了相关企业针对算法安全的技术性评估指标，并按照业务流程将安全风险归类为算法、数据和环境三个层面。
	2024.03	GB/Z 42885-2023	信息安全技术 网络安全信息共享指南	确立了网络安全信息共享活动要素和基本原则，描述了共享活动的范围和过程，适用于各类组织或个人间的网络安全信息共享活动，为网络运营者、关键信息基础设施运营者、网络安全服务机构等相关方组织有效的网络安全信息共享提供参考。
地方标准	2023.12	DB33/T 1329-2023	数据资产确认工作指南	本标准提供了数据资产确认的工作框架，数据资产初始确认、变更确认和终止确认的指导和建议，适用于指导组织进行数据资产确认工作。
	2023.05	DB3301/T 0403-2023	数据知识产权交易指南	本文件提供了数据知识产权交易的基本原则、交易标的、交易相关方、交易流程、评价和改进等建议，适用于数据知识产权交易。
	2022.12	DB3310/T 93-2022	公共数据授权运营指南	描述了公共数据授权运营的基本原则、数据范围、运营流程、数据产品类型及计价方式、安全管理等内容，适用于指导公共数据授权主体和运营单位开展公共数据授权运营活动。
	2021.06	DB15/T 2199—2021	数据交易安全技术要求	给出了数据资源交易参考框架，规定了数据资源交易参与方安全要求和数据资源交易过程中数据生命周期安全要求，适用于数据资源交易参与方进行安全自评估，也可供第三方测评机构对数据资源交易参与方进行安全评估时参考。
	2020.6	DB52/T 1468—2019	基于区块链的数据资产交易实施指南	本标准规定了基于区块链的数据资产交易实施的术语、定义和缩略语、基本要求、数据资产交易规范等要求。本标准适用于：为数据资产交易平台的实施提供正确的指引：a) 对数据资产交易方记录；b) 对数据资产交易流程记录，对数据资产交易溯源，构建区块链分布式、多方可信促进数据资产流通。

资料来源：政府网站，数据要素小能手公众号，人民数据公众号，中泰证券研究所

2.3 多省级数据局开年密集揭牌，数据安全产业作为配套工程乘风提速

■ 多省份数据管理机构揭牌，呈大同小异和因地制宜的发展趋势。

- 2023年10月25日，国家数据局正式挂牌成立，负责协调推进数据基础制度建设，统筹数据资源整合共享和开发利用，统筹推进数字中国、数字经济、数字社会规划和建设等。
- **2024年，新一轮机构改革逐步在省级层面落地，省级数据管理机构密集揭牌。**截止2024年1月26日，已有14家省级数据局相继挂牌，全国各省市数据要素化市场加速推动。

图表：国家数据局正式揭牌后动作汇总

序号	时间线	事件
1	2023.10.25	国家数据局正式挂牌
2	2023.10.31	重庆市委召开数字重庆建设推进会，国家数据局局长出席会议
3	2023.11.07	国家数据局局长一行赴杭州高新区(滨江)调研“中国数谷”建设工作，听取数据要素产业实践经验与应用探索等成果汇报
4	2023.11.10	国家数据局局长出席北京数据基础制度先行区启动会议并作重要讲话，首次公开谈数据要素制度建设
5	2023.11.23	第二届全球数字贸易博览会数据要素治理与市场化论坛，国家数据局局长首次提出数据基础设施建设
6	2023.11.25	国家数据局局长在上海举行的2023全球数商大会开幕式上致辞，首次透露将研究实施“数据要素X”行动
7	2023.12.08	国家数据局局长在第二届数字政府建设峰会开幕式上致辞，首次公开发声“公共数据、数字政府”
8	2023.12.25	国家数据局和国家发展改革委发布《数字经济促进共同富裕实施方案》
9	2023.12.31	国家数据局等17部门联合印发《“数据要素X”三年行动计划(2024—2026年)》
10	2024.01.07	第二十五届北大光华新年论坛在北京举行，国家数据局局长出席论坛并发表主题演讲，对《“数据要素X”三年行动计划(2024-2026年)》进行解读

图表：2024年省级数据局挂牌成立情况盘点

序号	公布时间	省市	机构名称
1	1月5日	江苏	江苏省数据局
2	1月11日	四川	四川省数据局
3	1月11日	内蒙古	内蒙古自治区政务服务与数据管理局
4	1月14日	上海	上海市数据局
5	1月15日	青海	青海省数据局
6	1月15日	云南	云南省数据局
7	1月15日	河北	河北省数据和政务服务局
8	1月16日	湖南	湖南省数据局
9	1月18日	广东	广东省政务服务和数据管理局
10	1月19日	天津	天津市数据局
11	1月21日	福建	福建省数据局
12	1月25日	湖北	湖北省数据局
13	1月25日	河南	河南省数据局
14	1月26日	浙江	浙江省数据局

资料来源：中移智库公众号，政府网站，中泰证券研究所

资料来源：工程壹家公众号，政府网站，中泰证券研究所

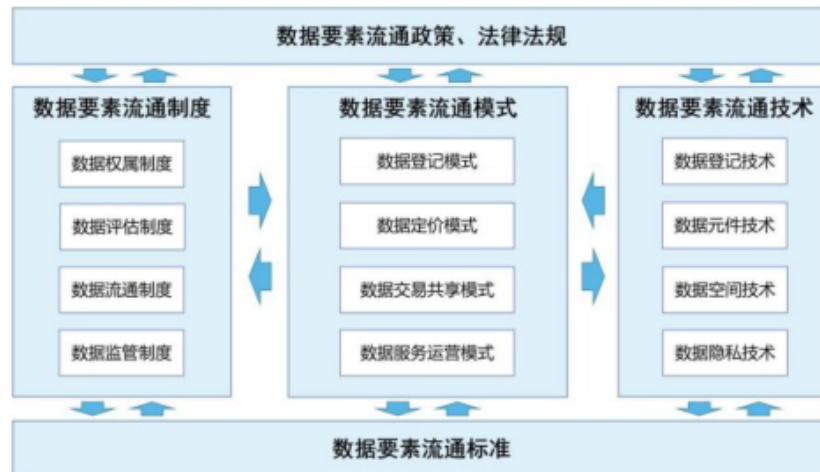
2.4 “数据要素×安全流通”，加强数据安全保障，推动数据资产入表、数据资本化

- “数据要素×”三年行动计划，保障支撑章节提出优化数据流通环境、加强数据安全保障，加大中央预算内投资“数据要素×”试点工程，引导社会资本投向数据产业，推动数据资产入表、数据金融创新等活动。
- **数据安全保障侧**，行动计划提出：一、建立数据安全治理体系，落实数据分类分级保护、网络安全等级保护、关基信息保护以及个人信息保护。二、发展精细化、专业化数据安全产品，开发面向中小企业的数据安全工具包，轻量化、定制化个人数据安全防护产品。三、鼓励有实力的企业提供基于云端的数据安全服务。
- **数据流通环境侧**，行动计划提出：一、强化交易所合规管理和服务质量，标准化、高效率推动数据共享流通。二、深海隐私计算、可信数据空间、区块链技术应用，建设重点行业和领域数据流通平台，促进数据合规高效流通使用。三、因地制宜建设各类数据园区，培育数商、第三方专业服务机构等流通服务主体。

图表：数据安全保护对象总体视图



图表：数据要素流通总体框架

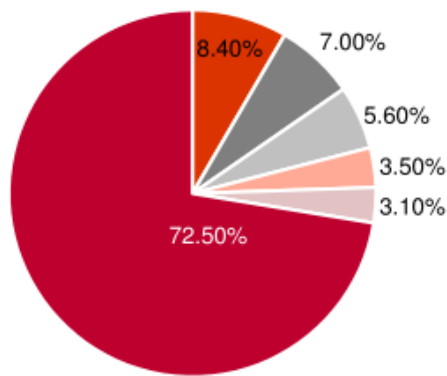


2.5.1 数据安全市场规模持续扩大，竞争格局多元化

- 数据的流动性、多样性和可复制性使数据安全风险不断放大，数据安全需求爆发，未来将推动市场规模进一步扩大。
- 十六部门联合促进数据安全产业发展，1500亿市场呼之欲出。2023年1月，工信部等十六部门联合发布《关于促进数据安全产业发展的指导意见》，目标到2025年，数据安全产业规模超过1500亿元，年复合增长率超过30%。
- 根据IDC数据，2022年中国数据安全软件市场规模为8.6亿美元，同比增长23%。预计到2027年，中国数据安全软件市场规模将达到22.2亿美元，年复合增长率 20.7%。
- 数据安全市场的竞争将日益激烈，新兴安全厂商与传统IT巨头积极布局。企业间竞争主要体现在技术实力、产品线丰富度、服务质量等方面。同时，新技术、新业态的涌现也为市场带来新的竞争力量。

图表：2023H1中国数据安全软件市场份额

■ 奇安信 ■ 阿里巴巴 ■ 启明星辰集团 ■ 安恒信息 ■ 天融信 ■ 其他



资料来源：IDC，中泰证券研究所

2.5.2 各领域数据安全需求持续升级

- 数据安全行业的下游客户主要为政府、电信运营商、金融、能源、军工等领域的用户。下游行业用户的数据安全保障需求则对本行业的发展具有较大的促进作用。突发性的、造成较大范围损害的网络威胁事件往往会对下游行业的数据安全保障需求产生催化作用，促使其加大数据安全投入。
- 政府行业——建设数字政府应先构筑数据安全“堤坝”。政务业务需要汇集和融合的数据体量庞大，在安全方面不仅要保障数据完整性、保密性和可用性，更需要确保数据在联合使用过程中的隐私性，各省市数据安全建设脚步加快。
- 电信行业——数据安全建设全面展开。数据安全管控平台类项目建设已全面展开；数据安全评估进入正常轨道，多数运营商公司每年都会购买数据安全评估服务；数据泄漏在数据时代的背景下显得尤为突出，采购增速较高。
- 医疗卫生行业——对数据安全的关注度空间提升，越来越多的医疗单位会实施系统性数据安全保护方案。

图表：数据安全产业链示意图



图表：广东联通数据安全体系框架





3

AIGC驱动数据安全防线构筑

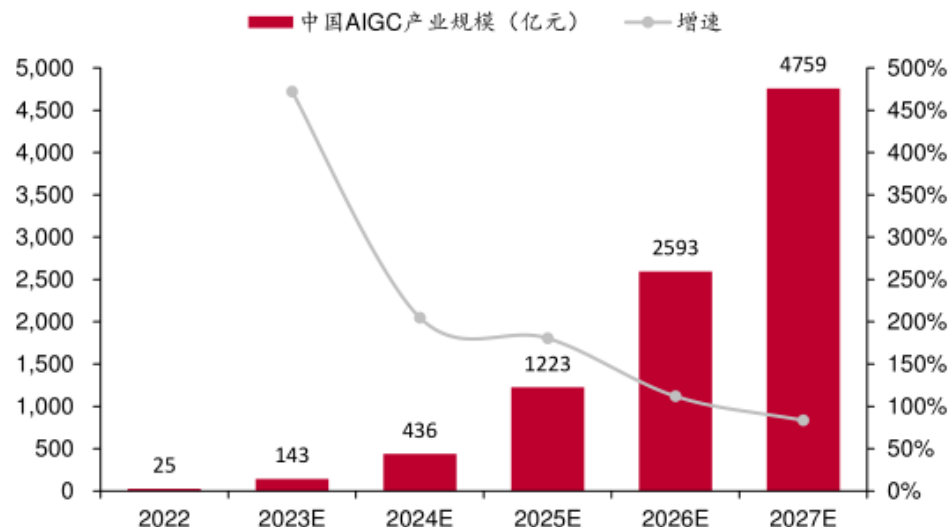
3.1 AIGC：引领下一代技术风口与产业趋势，产业规模展望庞大

- 2023年，以ChatGPT等为代表的AIGC技术应用火遍全球，由大模型驱动的AIGC时代正式开启。
- 在政策推动与技术应用落地等多方位因素驱动下，我国AIGC行业正迎来新的风口。当前，新一轮科技变革正向着纵深演进，AIGC及AI大模型为各行业各领域带来了创新机遇。
- 2024年是AI产业年，越来越多的创新应用场景和产品形态将不断涌现。
- **AIGC未来产业规模展望庞大**。预计2027年，中国AIGC产业规模将达到4759亿元，逐步建立完善模型即服务产业生态，2030年中国AIGC产业规模有望突破万亿元，达到11441亿元。

图表：2024年AIGC应用层十大趋势



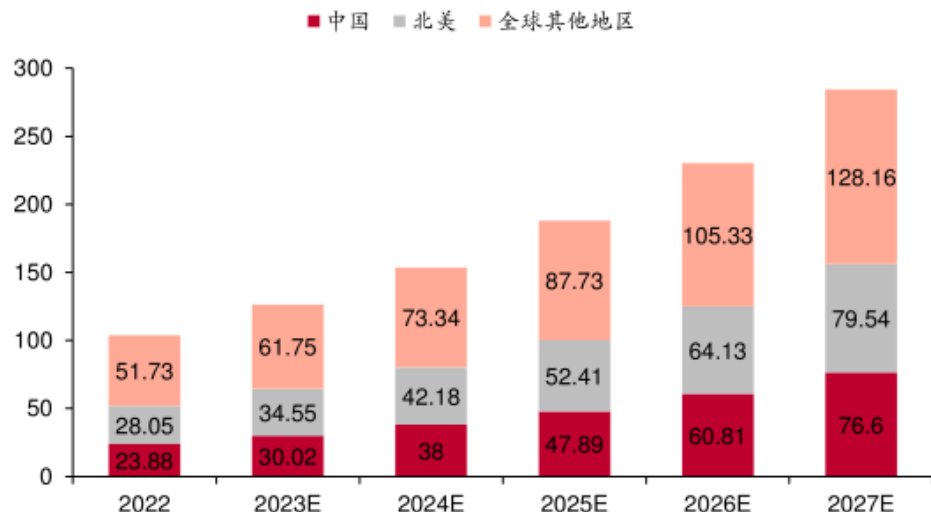
图表：2022-2027E中国AIGC产业规模



3.2 AIGC对数据的使用量前所未有，驱动数据要素市场需求爆发

- **全球数据总量和算力规模高速增长。**据IDC数据显示，2022年全球数据圈数据量规模达到103.66ZB，中国数据量规模将从2022的23.88ZB增长至2027年的76.6ZB，CAGR达到26.3%，增速有望位列全球第一。
- **大模型技术取得的突破离不开高质量数据的发展。**数据已成为未来人工智能竞争的关键要素，人工智能正在从“以模型为中心”加速向“以数据为中心”转变。
- **人工智能发展驱动数据要素市场需求爆发。**伴随着大模型时代的到来，大模型训练使用的数据集规模持续增长，更加需要大规模、高质量、多样化的数据集提升模型效果和泛化能力。如2018年GPT-1数据集约4.6GB，2020年GPT-3数据集达到了753GB，而2021年Gopher数据集已达10550GB，2023年GPT-4的数据量更是GPT-3的数十倍以上。

图表：全球数据量规模（单位：ZB）



图表：人工智能发展对数据要素供给提出更高要求



资料来源：IDC Global DataSphere 2023，中泰证券研究所

资料来源：中国信息通信研究院，中泰证券研究所

3.3 生成式大模型面临的数据安全合规风险

- 大模型的训练及其应用的落地需要大量的数据作为支撑，由此带来的个人隐私泄露和数据篡改等数据安全风险已成为法律所必须因应的重要议题。针对不同阶段涉及的数据处理行为，大模型的动态数据安全风险存在差异。
- 训练数据的采集阶段：大模型的搭建依托于海量的训练数据，由于训练数据的来源属性具有多元性，所可能引发的数据安全风险也是多重而非单一的。如难以保障模型开发者对每个训练信息主体都完全符合知情同意的具体要求。
- 在模型的训练与调整阶段，如无法保障模型内存储数据免遭黑客攻击或内部工作人员非法披露导致数据泄露风险。
- 大模型在全球范围内收集和使用用户的个人数据面临极大的合规风险。如国内的ChatGPT用户出于数据分析或信息统计等目的，将其收集的一定规模的个人数据的传输至OpenAI的境外数据处理中心，就很可能构成事实上的数据出境行为，如果未经审批许可将导致极大的合规隐患。

图表：AIGC风险图谱



图表：AIGC生命周期各阶段的数据处理活动及其风险因素

生命周期	模型训练阶段	应用运行阶段	模型优化阶段
主要活动	立项设计，数据采集 数据清洗，数据标注 模型训练，模型验证	2C：开发者直接向使用者提供服务 2B/2B-2C：由服务提供者集成开发者技术以向使用者提供服务	利用应用运行阶段采集的数据开展模型优化
数据合规核心风险要素	隐私性与合法性 数据质量 可靠性与稳健性	隐私性与合法性 透明性与可解释性 准确性与公平性 应用风险 信息内容监管 信息安全	隐私性与合法性

- **数据合规：**企业、组织或个人在数据生产全环节和数据管理各版块的行为符合法律法规、行政规章、标准规范、行业准则、内部制度、合同协议、操守规范等要求。
- 大模型的训练和运行需要海量数据的支撑，庞大的数据基础极有可能引发数据安全风险，故采取切实可行的措施是保护数据流通和隐私安全的关键所在，同时也需深度挖掘这些数据的潜在价值。
- 数据脱敏、身份认证与访问控制、数据加密等技术常用于直接或间接地保护隐私信息不被泄漏。如数据脱敏通常用于公共数据开放等数据流通环节，数据脱敏技术可以以直接的方式隐去敏感信息，具有效率高、计算成本低的优势。

图表：数据安全技术体系框架图



资料来源：《数据安全治理白皮书 5.0》，中泰证券研究所

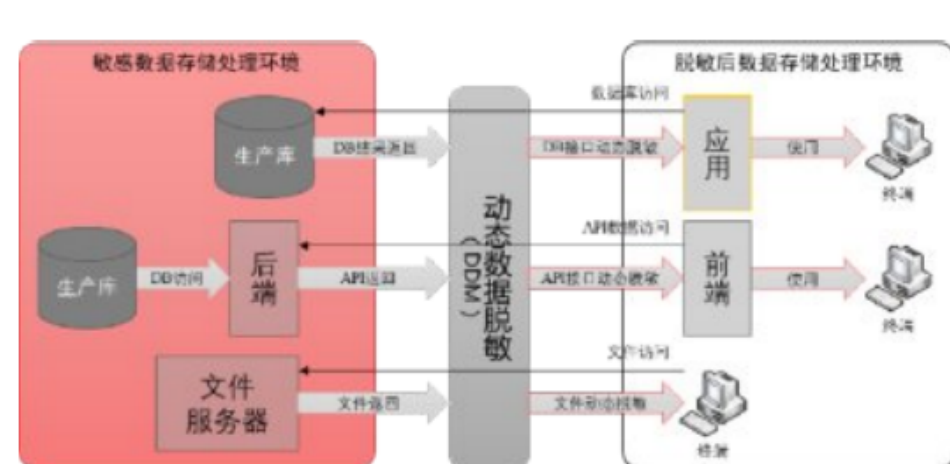
3.4.1 数据有效脱敏——切实满足数据使用需求和合规监管要求

- 数字化转型和数据安全合规的双重背景下，数据脱敏作为数据安全保障措施之一，普遍应用在数据使用的过程中。
- 数据脱敏是一种保护敏感信息的技术手段，指对敏感数据通过变形、转换等手段降低数据的敏感程度，从而在数据全生命周期各阶段实现保护敏感数据的目的，从使用场景上分为数据静态脱敏和数据动态脱敏。
- 数据静态脱敏一般用在非生产环境，将敏感数据从生产环境抽取并脱敏后用于培训、分析、测试、开发等非生产环境。
- 数据动态脱敏一般用在生产环境中，将敏感数据实时进行脱敏后用于应用访问等生产环境。
- 在使用 LLM 大模型服务时，数据脱敏对于保护个人隐私和企业信息安全具有重要意义。如果未对敏感数据进行脱敏处理，LLM 大模型可能在无意识中泄露用户的敏感信息，如模型可能会记住并泄露曾在训练集中出现过的敏感数据。

图表：数据静态脱敏框架示意图



图表：业务系统前台场景下动态数据脱敏

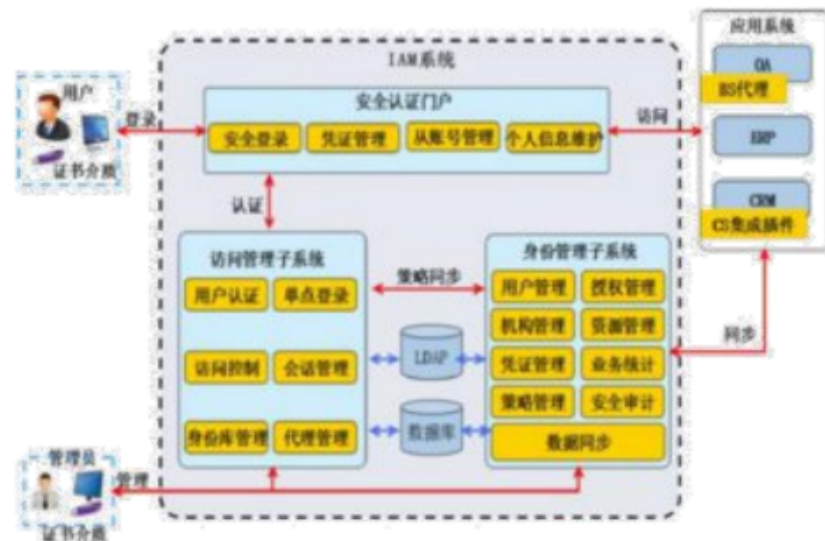
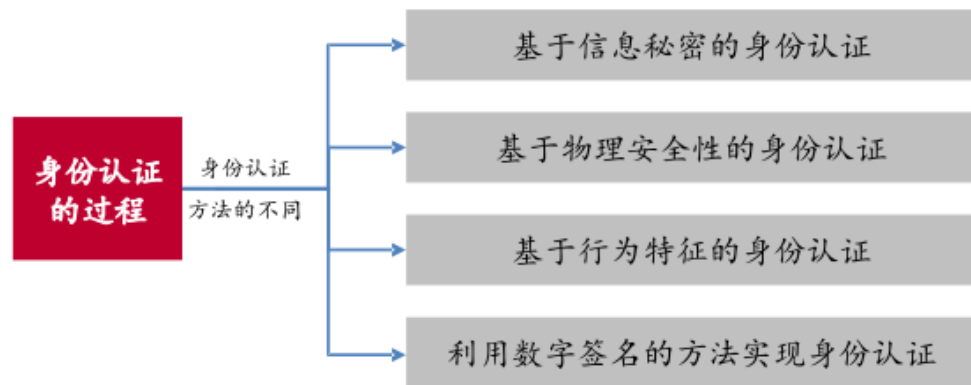


3.4.2 身份认证——防护网络资产的第一道关口

- **身份认证**：计算机网络系统的用户在进入系统或访问不同保护级别的系统资源时，系统确认该用户的身份是否真实、合法和唯一的过程。
- **常用网络身份认证方式**：静态密码方式、动态口令认证、USB Key认证、生物识别技术、CA认证系统。
- **统一身份认证系统（IAM）**：统一身份认证系统是一套全面地建立和维护数字身份，并提供有效地、安全地进行IT资源访问的业务流程和管理手段，从而实现组织信息资产统一的身份认证、授权、访问控制和身份数据集中管理与审计。
- **IAM建设意义**：帮助组织进行应用系统的统一管理，提高数据资产的可管理性，为实施进一步安全保护措施提供支撑。

图表：身份认证的过程根据身份认证方法的不同分类：

图表：统一身份认证系统技术体系框架



3.4.3 访问控制——网络安全防范和资源保护的关键策略之一

- **访问控制：**通过某种途径显式地准许或限制访问能力及范围的一种方法，其建立在身份认证的基础之上。
- 通过限制对关键资源的访问，防止非法用户的侵入或因为合法用户的不慎操作而造成的破坏，从而保证网络资源受控地、合法地使用，是针对越权使用资源的防御措施。
- **主要目的：**限制访问主体对客体的访问，从而保障数据资源在合法范围内得以有效使用和管理。
- **两个任务：**识别和确认访问系统的用户、决定该用户可以对某一系统资源进行何种类型的访问。
- **三个要素：**主体、客体和控制策略。

图表：访问控制过程



图表：业务访问控制流程



4

投资建议与风险提示

投资建议

- 随着数字经济持续推动数据价值释放、海量数据处理需求激增和AIGC跨越式发展，长期而言数据安全产业的发展空间仍然十分广阔。当前时点，我们持续看好数据安全产业投资机遇，建议投资人持续关注，具体包括但不限于以下标的：
- **数据安全：**启明星辰、亚信安全、安恒信息、三未信安、深信服、奇安信、天融信、迪普科技、安博通、麒麟信安、中孚信息、绿盟科技、永信至诚。

风险提示

- AI进展不及预期带来下游需求不及预期的风险。
- 市场竞争加剧的风险。
- 研究报告中使用的公开资料可能存在信息滞后或更新不及时的风险。
- 政策落地不及预期的风险。

重要声明

- 中泰证券股份有限公司（以下简称“本公司”）具有中国证券监督管理委员会许可的证券投资咨询业务资格。
。本公司不会因接收人收到本报告而视其为客户。
- 本报告基于本公司及其研究人员认为可信的公开资料或实地调研资料，反映了作者的研究观点，力求独立、客观和公正，结论不受任何第三方的授意或影响。本公司力求但不保证这些信息的准确性和完整性，且本报告中的资料、意见、预测均反映报告初次公开发布时的判断，可能会随时调整。本公司对本报告所含信息可在不发出通知的情形下做出修改，投资者应当自行关注相应的更新或修改。本报告所载的资料、工具、意见、信息及推测只提供给客户作参考之用，不构成任何投资、法律、会计或税务的最终操作建议，本公司不就报告中的内容对最终操作建议做出任何担保。本报告中所指的投资及服务可能不适合个别客户，不构成客户私人咨询建议。
- 市场有风险，投资需谨慎。在任何情况下，本公司不对任何人因使用本报告中的任何内容所引致的任何损失负任何责任。
- 投资者应注意，在法律允许的情况下，本公司及其本公司的关联机构可能会持有报告中涉及的公司所发行的证券并进行交易，并可能为这些公司正在提供或争取提供投资银行、财务顾问和金融产品等各种金融服务。本公司及其本公司的关联机构或个人可能在本报告公开发布之前已经使用或了解其中的信息。
- 本报告版权归“中泰证券股份有限公司”所有。事先未经本公司书面授权，任何机构和个人，不得对本报告进行任何形式的翻版、发布、复制、转载、刊登、篡改，且不得对本报告进行有悖原意的删节或修改。