

DSMM 国家标准应用情况与未来发展

(征求意见稿)

2024 年 8 月

前 言

全球数据安全治理的背景和现状是复杂而严峻的。随着数字经济的发展，数据已成为国家竞争力的战略资源，但同时也暴露在日益增长的安全风险之中。数据安全问题不仅涉及个人隐私、重要数据的保护，更触及国家安全和国际政治经济的多个层面。

数据安全治理在当前面临诸多挑战和问题，比如合规性压力，89.9%的企业认为合规需求是进行数据安全建设的主要原因，这表明监管压力是数据安全治理的主要驱动力之一；技术工具能力不足，超过 50%的企业认为现有数据安全产品/服务无法达到及格标准，突显了现有数据安全技术工具的不足；数据泄露，《2024 年上半年数据泄露风险态势报告》显示 2024 年上半年，数据泄露事件数量达到 16011 起，较 2023 年下半年增长了 59.58%，且黑产交易团伙数量增长近一倍，显示出数据泄露风险的严峻态势。

综上所述，全球数据安全治理正面临多方面的挑战，需要政府、企业、组织和个人的共同努力，通过法律、技术、管理和合作等多方面措施，构建更加安全、高效的数据安全治理体系。

本报告立足我国数据安全产业新发展、新变化、新需求，聚焦数据安全体系建设，梳理了数据安全能力成熟度模型（以下简称 DSMM）国家标准应用的发展历程和实践情况，首次提出以 DSMM 为核心的数据安全治理模式的未来发展方向，并进行了预测，最后希望联合监管部门、第三方机构、数据拥有方、数据方案提供方等数据安全产业上下游生态，持续推动企业、组织机构在数据安全方面

达到更高成熟度水平，构建安全、健康、有序的数据安全产业生态环境。

目 录

一、数据安全治理方法论	1
1.1 DSG 框架及应用概况	1
1.2 DGPC 框架及应用概况	2
1.3 国内 DSG 框架及应用概况	2
1.4 DSMM 框架及应用概况	3
二、DSMM 标准的历程	4
2.1 DSMM 的来源	4
2.2 标准的制定	5
三、DSMM 在我国的发展与实践	5
3.1 国家层面	5
3.1.1 国家法律对于数据安全的宏观要求	5
3.1.2 DSMM 对于数据安全法规的支持	8
3.1.3 DSMM 对其他领域国标的影响	8
3.1.4 各部委对数据安全的落实	11
3.2 地方层面	14
3.3 行业层面	15
3.3.1 各行业的规划要求	16
3.3.2 标准框架对行业安全标准的影响	17
3.3.3 行业的贯标实践	18
3.3.4 对企业数据安全治理的促进	20
3.4 产业实践	22
3.4.1 服务侧	22
3.4.2 需求侧	31
3.5 实践中的挑战与问题	35
四、DSMM 未来发展方向与预测	37
4.1 技术发展对 DSMM 的影响	37
4.2 政策变化对 DSMM 的潜在影响	42

4.3 预测 DSMM 的长期价值与趋势	48
五、结语	49
5.1 对企业与政策制定者的建议	49
5.2 对 DSMM 产业未来发展的展望	50
附录 相关政策汇编	53

一、数据安全治理方法论

1.1 DSG 框架及应用概况

Gartne 在《2017 年数据安全态势》中提及“数据安全治理(Data Security Governance)”，Gartner 对数据安全治理形成一个从上而下的整体框架，包括从治理前提、具体目标到技术支撑的完整体系。该框架对数据治理完整体系进行了阐述，以数据分级分类为核心，提出满足数据安全保护、合规性、敏感数据管理 3 个需求目标，以数据安全人员组织、数据安全使用策略和流程、数据安全技术支持作为主要内容模块，治理的实施步骤包括平衡业务与风险/威胁/合规性的关系、数据优先级设置、制定安全策略、实施安全工具、策略编排和同步等，DSG 框架如下：

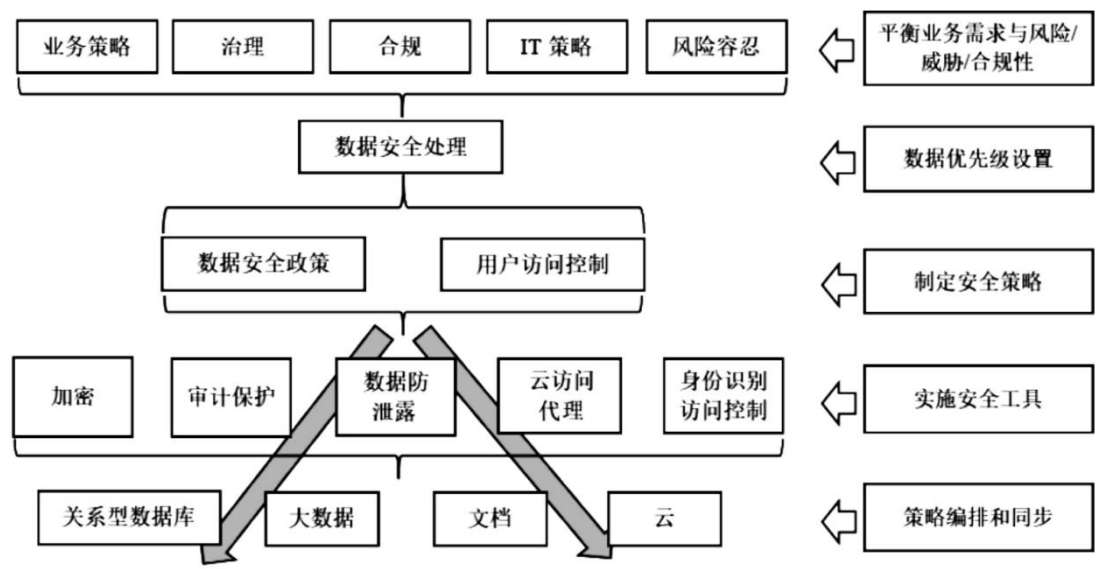


图 1 DSG 框架图

DSG 框架应用于数据安全的治理过程，主要由各工具厂商、咨询机构等依据此框架构建企业级的数据安全过程管理，涵盖企业包括医疗（含卫健委）、金融、政务、能源等。

1.2 DGPC 框架及应用概况

DGPC 框架（Data Governance for Privacy, Confidentiality and Compliance）由微软于 2010 年提出，该框架提供了一种以隐私、机密性和合规为目标的数据安全治理框架，以数据生命周期和核心技术领域为重点关注点，基于威胁建模与风险评估的方法，对组织如何实施数据安全治理进行了概要阐述。DGPC 框架主要是从方法论层面明确数据安全治理的目标，缺少对在数据生命周期各环节落实数据安全治理措施的详细说明。

1.3 国内 DSG 框架及应用概况

MTDSAM 是 2021 年由中国软件评测中心提出的一种 DSG 框架，全称为“Management & Technology” Data Security Evaluation Model，是一种“管理+技术”的数据安全评估模型，模型借鉴了网络安全等级保护测评方法，以数据为中心将测评内容划分为管理与技术两方面。

管理方面以数据分类分级保护要求为基础，首先制定数据管理整体办法及相关文件，然后建立相关制度以规范技术体系，管理域主要是对数据安全顶层设计和制度规范制定相关要求。

技术方面主要对数据安全相关技术落地的指标提出要求，以数据行为安全、数据内容安全和数据环境安全作为指标分类方向，将安全制度与技术有效结合，用于评估组织机构数据安全状态。

MTDSAM 模型将管理方面评估项合称为管理域，将技术方面评估项合称为技术域，两者相加为模型整体评估域，模型框架如下图所示。

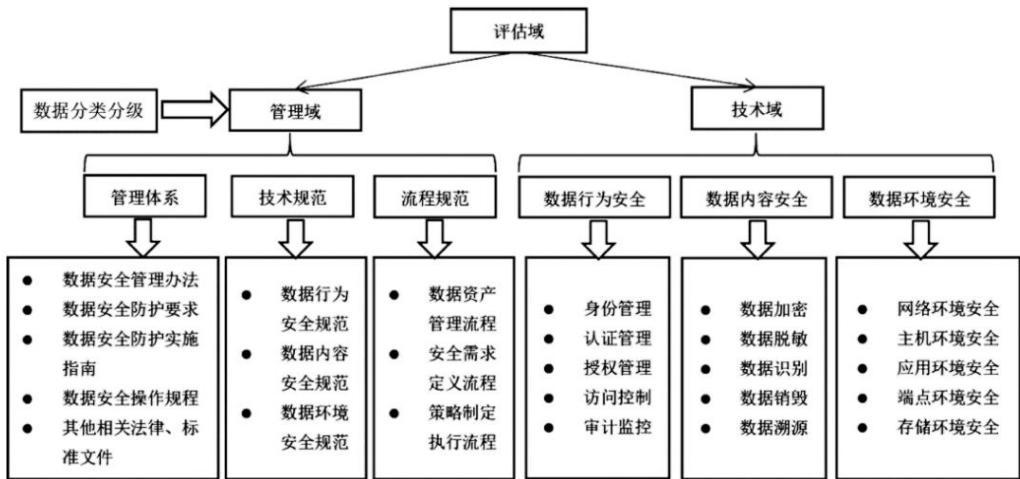


图 2 MTDSAM 模型框架

MTDSAM 模型目前主要在中国软件评测中心进行企业数据安全服务资质评估、安全专项等评估活动，截止至 2024 年 8 月，为超过 50+企业进行了评估，企业范围覆盖物联网、金融、安全等行业。

1.4 DSMM 框架及应用概况

DSMM 是我国首个数据安全领域国家标准，由安全能力、安全过程维度和能力成熟度三个维度构成。安全能力维度明确了组织在数据安全领域应具备的能力，包括组织建设、制度流程、技术工具和人员能力；数据安全能力成熟度等级划分为五级，1 级是非正式执行级，2 级是计划跟踪级，3 级是充分定义级，4 级是量化控制级，5 级是持续优化级；数据安全过程维度包括数据生存周期安全过程和通用安全过程，其中数据生存周期安全过程分数据采集安全、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 6 个阶段。其模型框架如下图所示。

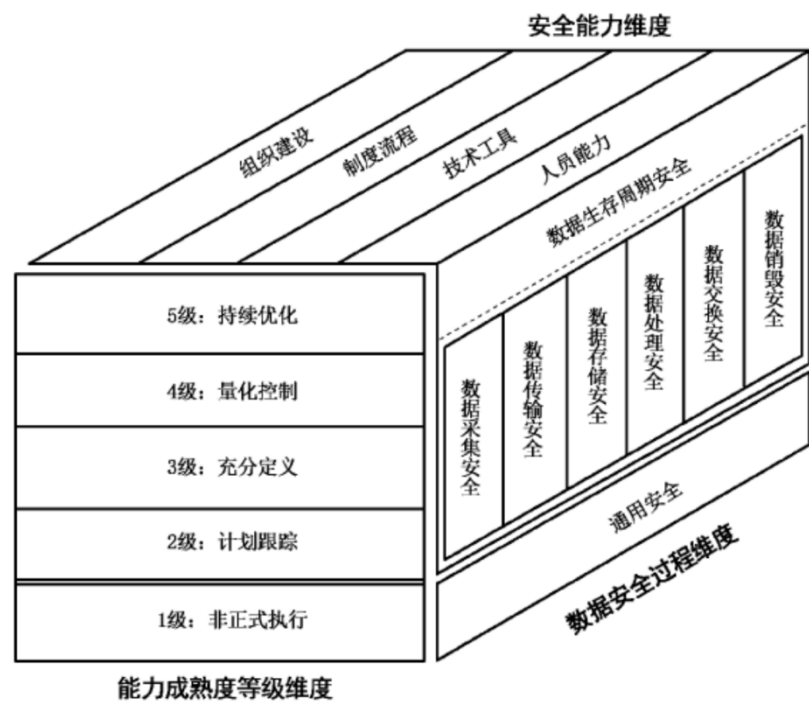


图 3 DSMM 模型框架

基于 DSMM 的数据安全治理方法覆盖范围较广，目前应用于评估、检查等多个方面，同时各企业数据安全落地或第三方机构开发新方法或模型时，大多遵循 DSMM 提出的以数据中心、以数据分类分级为基础、以数据全生命周期流转为线条的安全过程。在产业联盟推广、新模型开发、数据安全体系构建等方面均有所体现。

二、DSMM 标准的历程

2.1 DSMM 的来源

DSMM 是一套旨在提升组织数据安全防护水平的标准和方法论。它来源于阿里巴巴集团大量数据安全实践和研究，同时借鉴了能力成熟度模型（CMM）的思想，以数据为中心，围绕数据的整个生命

周期及数据通用安全进行定级评估，从而提高数据安全防护水平。DSMM 的核心内容强调从实践中来，服务于实践去，通过科学的方法论指导组织机构评估和提升自身的数据安全防护能力。

2.2 标准的制定

DSMM 国家标准的制定过程是行业内多方权威机构共同努力的成果。这一过程联合了 40 多家企事业单位共同参与，通过大量实践和研究基础上形成，并在 2019 年 8 月 30 日正式发布，于 2020 年 3 月 1 日正式实施，在此期间，由阿里巴巴推动立项的数据安全相关国际标准《电子业务数据的生命周期管理的安全参考架构》于 2018 年也正式发布了。

DSMM 国家标准旨在围绕数据的全生命周期，包括采集、传输、存储、处理、交换和销毁等环节，从组织建设、制度流程、技术工具、人员能力四个能力维度进行综合考量，并根据 1 至 5 级的成熟度等级进行评估，以全面提升组织的数据安全防护能力。

DSMM 国家标准的制定过程充分体现了多方共同参与、科学评估和实践验证的原则，确保了标准的科学性、实用性和有效性。通过这一过程，DSMM 不仅成为了国家标准，也成为了推动行业数据安全防护水平提升的重要工具。

三、DSMM 在我国的发展与实践

3.1 国家层面

3.1.1 国家法律对于数据安全的宏观要求

国家的网络安全与数据安全紧密相连、相互依存，从数据传输通道的安全、非法访问的防范、数据存储的安全、数据备份与恢复的保障等方面看，网络安全是数据安全的基础和底座。而数据安全又是网络安全的重要组成部分，数据安全的要求促使网络安全更加精细化和全面化，数据安全面临的挑战又推动着网络安全技术不断创新和发展。因此只有将网络安全和数据安全作为一个整体进行考虑，两者协同发展，才能有效地保护数据资产安全，应对日益复杂的安全威胁，为国家的安全和发展提供坚实保障。

从我国发布的《网络安全法》《数据安全法》《个人信息保护法》等法律来看，目前，我国法律对于数据安全的宏观要求，主要体现在构建全面的数据安全法律框架、明确数据安全保护的基本原则、强化数据安全监管与处罚机制等方面。

（1）构建全面的数据安全法律框架

近年来，我国已经形成了以《网络安全法》《数据安全法》《个人信息保护法》等法律为核心，行政法规、部门规章为依托，地方性法规、地方规章为抓手，国家标准为指南的安全法规保障体系。这些法律法规共同构成了我国数据安全保护的宏观法律框架，为数据安全工作提供了坚实的法律基础。

（2）明确数据安全保护的基本原则

一是合法正当、必要诚信原则。要求数据处理活动必须遵守法律法规，不得违反公序良俗，且需确保数据处理的必要性和最小范围，保护个人合法权益。

二是目的明确、最小必要原则。强调数据收集和处理必须有明确的目的，且收集的数据量应限于实现该目的所必需的最小范围。

三是权责一致、安全可控原则。要求数据处理者对其处理的数据承担安全责任，确保数据处于有效保护和合法利用的状态，并具备相应的数据安全能力。

四是全程管理、保障权益原则。强调对数据的收集、存储、使用、加工、传输、提供、公开等全生命周期进行安全管理，保障数据主体的合法权益。

（3）强化数据安全监管与处罚机制

一是建立数据安全监管体系。国家建立健全数据安全监管机制，对数据处理活动进行全程监管，确保数据安全法律法规的有效实施。

二是明确数据安全责任主体。规定数据处理者是数据安全的第一责任人，需建立健全数据安全管理制度和技术防护措施，保障数据安全。

三是加大违法处罚力度。对于违反数据安全法律法规的行为，依法予以严厉处罚，包括警告、罚款、暂停相关业务、吊销相关证照等，构成犯罪的依法追究刑事责任。

（4）推动数据安全技术与产业发展

一是鼓励技术创新。支持数据安全技术的研发和应用，推动数据安全产品和服务的创新发展，提升数据安全防护能力。

二是促进产业融合。推动数据安全技术与云计算、大数据、人工智能等新一代信息技术的深度融合，培育数据安全产业生态体系。

（5）加强国际合作与交流

积极参与国际数据安全规则的制定和交流合作，推动构建公正、合理、互利的国际数据安全治理体系，共同维护全球数据安全。

3.1.2 DSMM 对于数据安全法规的支持

DSMM 作为数据安全领域的标准，其制定和实施与国家的数据安全法规高度契合。例如，《数据安全法》中提到，国家促进数据安全检测评估、认证等服务的发展，支持数据安全检测评估、认证等专业机构依法开展服务活动。DSMM 正是基于这一背景，为组织提供了数据安全能力成熟度评估的框架和方法，有助于组织合规、有效地开展数据安全工作。

同时，DSMM 标准从组织建设、制度流程、技术工具、人员能力四个安全能力维度出发，对数据采集、传输、存储、处理、交换、销毁等全生命周期的安全过程提出了分级要求。这为组织在不同阶段开展数据保护建设提供了分级别的实践指南，有助于组织根据自身实际情况，逐步建立和完善数据安全保障体系，以满足数据安全法规的要求。通过实施 DSMM 评估，组织可以全面梳理自身的数据安全现状，发现数据安全能力短板，从而有针对性地加强数据安全管理和防护。这一过程不仅提升了组织的数据安全意识，还增强了组织在数据安全法规方面的合规能力。

3.1.3 DSMM 对其他领域国标的影响

DSMM 在数据安全方面的治理理念、架构设计、方法路径、实践效果等，对多个领域的十几个数据安全类国家标准产生了积极的影

响，DSMM 已经成为了多行业和领域的数据安全基线，并推动数据安全国家标准体系的完善和发展。

一是理念与原则的传播。DSMM 强调的数据安全治理理念，注重从组织建设、制度流程、技术工具和人员能力四个维度全面提升数据安全能力。这种全面、系统的治理理念被更多行业和领域的国家标准所借鉴，促使其他标准在制定和完善过程中，更加注重从多个方面协同保障安全，而非仅仅关注单一技术或管理要素，推动各领域形成综合、立体的安全保障体系。

二是评估与度量方法的借鉴。DSMM 明确的成熟度等级划分方式和关键过程域与指标的定义提供了一种清晰的评估框架，这种分级模式和评估指标可以为其他领域的国家标准提供参考，以确定自身领域内相关能力的成熟度等级，明确关键的业务流程、管理环节或技术要点作为评估的重点领域，并设定具体、可衡量的指标，使评估结果更具层次感和可操作性，确保评估的科学性和准确性。

三是促进跨领域协同与融合。在数字化时代，各领域之间的边界逐渐模糊，数据的跨领域流动和共享日益频繁。DSMM 的出现有助于推动与其他涉及信息安全、网络安全等领域国家标准的协同发展，减少标准之间的冲突和重叠，形成更具整体性和一致性的标准体系。

四是推动行业整体安全水平提升。DSMM 对于数据安全的高标准要求，可能激励其他领域国家标准在保障安全性方面设定更高的目标和更严格的规范，这种对数据安全的高度重视和积极行动，会

在整个行业内形成良好的示范效应，促使其他领域的组织也更加关注自身的安全问题，从而推动各行业整体安全水平的提升。

随着数据安全重要性的不断提升，近年来，在交通运输领域、电子商务领域、通信领域、生物学领域等多个领域的国家标准制定中，均参考或引用了 DSMM，借助 DSMM 对数据安全的严格要求，推动各行业数据安全管理的规范化和标准化发展。

标准编号	标准名称	引用情况
GB/T 41773-2022	信息安全技术 步态识别数据安全要求	步态识别数据处理者应符合 GB/T 37988 数据安全能力成熟度等级 3 的规定
GB/T 41806-2022	信息安全技术 基因识别数据安全要求	基因识别数据处理者应符合 GB/T 37988 数据安全能力成熟度等级 3 规定的要求
GB/T 41807-2022	信息安全技术 声纹识别数据安全要求	组织机构数据处理者应按照 GB/T 37988 达到数据安全能力成熟度 3 级以上要求
GB/T 41819-2022	信息安全技术 人脸识别数据安全要求	处理者处理人脸识别数据应符合 GB/T 37988 数据安全能力成熟度等级 3 规定的要求
GB/T 42971-2023	第三方电子合同服务平台信息安全技术要求	第三方电子合同服务平台系统数据安全，应符合 GB/T 37988 的要求
GB/T 42012-2022	信息安全技术 即时通信服务数据安全要求	即时通信服务提供者的数据安全能力应至少符合 GB/T 37988 中的 2 级能力要求
GB/T 42013-2022	信息安全技术 快递物流服务数据安全要求	快递物流服务提供者的数据安全能力应至少符合 GB/T 37988 二级能力要求
GB/T 42014-2022	信息安全技术 网上购物服务数据安全要求	网上购物服务提供者的数据安全能力应至少符合 GB/T 37988 中的 2 级能力要求
GB/T 42015-2022	信息安全技术 网络支付服务数据安全	网络支付服务提供者的数据安全能力应至少符合 GB/T 37988 二

	要求	级能力要求
GB/T 42016-2022	信息安全技术 网络音视频服务数据安全要求	网络音视频服务提供者的数据安全能力应至少符合 GB/T37988 二级能力要求
GB/T 42017-2022	信息安全技术 网络预约汽车服务数据安全要求	网络预约汽车服务提供者的数据安全能力应至少符合 GB/T 37988 中的 2 级能力要求
GB/T 43445-2023	《信息安全技术 智能手机预装应用程序基本安全要求》	数据安全能力宜至少符合 GB/T 37988 二级能力要求
GB / T 42888-2023	《信息安全技术 机器学习算法安全评估规范》	组织和个人开展机器学习算法相关的数据处理活动时，应具备基本数据安全能力，应达到 GB/T 37988 中规定的 2 级水平，宜达到 3 级水平
GB/T 37932-2019	《信息安全技术 数据交易服务安全要求》（标准修订并征求意见）	数据交易服务机构应按照 GB/T 37988-2019 的要求审核数据需方的数据安全能力成熟度确保不低于数据供方的数据安全能力成熟度

3.1.4 各部委对数据安全的落实

中央网信办和各部委对于数据安全极为重视，分别从各种的管理侧重出台相关数据安全合规的要求。

（1）中央网信办

发布了《十四五国家信息化规划》对数据安全提出了要求，强调要建立健全数据安全治理体系，研究完善行业数据安全政策，建立数据分类分级保护制度，规范数据采集、传输、存储、处理、共享、销毁全生命周期管理，推动数据使用者落实数据安全保护责任；起草了《网络数据安全条例（征求意见稿）》，明确了数据处理者的责任和义务，要求数据处理者采取备份、加密、访问控

制等必要措施保障数据安全。数据处理者还应建立数据安全管理制度和技术保护机制，对个人信息和重要数据进行重点保护，对核心数据实行严格保护。

（2）工业和信息化部

发布了《工业和信息化领域数据安全管理办法》，明确了该领域内数据处理的规范与要求，同时强调数据的分类分级管理，并着重提出了对重要数据和核心数据的保护要求；《“十四五”大数据产业发展规划》规划中强调了数据安全的重要性，提出要完善数据安全保障体系，强化大数据安全顶层设计，落实网络安全和数据安全相关法律法规和政策标准。鼓励行业、地方和企业推进数据分类分级管理、数据安全共享使用，开展数据安全能力成熟度评估、数据安全认证等。加强数据安全保障能力建设，引导建设数据安全态势感知平台，提升对敏感数据泄露、违法跨境数据流动等安全隐患的监测、分析与处置能力。筑牢数据安全保障防线，坚持安全与发展并重。《关于促进数据安全产业发展的指导意见》，旨在推动数据安全关键技术和产品的创新发展，为数据安全提供有力的产业支撑；《工业领域数据安全标准体系建设指南》，提供了一个全面的框架，旨在指导工业领域在数据安全方面的标准化工作，强调加强数据全生命周期安全管理，涉及数据收集、存储、使用、加工、传输、提供、公开等环节。

（3）教育部

联合中央网信办、工信部、公安部、市场监管总局等七部门发布《关于加强教育系统数据安全工作的通知》，要求建立数据安全责任体系和分类分级制度，形成数据资源目录，健全全生命周期数据安全保障制度，建立个人生物识别信息审查制度和数据安全评估制度，常态化开展数据安全监测预警通报，构建数据安全协同治理新格局。

（4）自然资源部

发布了《自然资源领域数据安全管理办法》，明确了自然资源领域数据的定义、分类、安全管理、风险监测预警、应急处置、监督检查以及法律责任等方面的要求。

（5）中国人民银行

起草了《中国人民银行业务领域数据安全管理办法（征求意见稿）》，旨在规范金融机构的数据处理活动，明确数据安全管理的职责和要求。

（6）国家金融监管局

制定了《监管数据安全管理办法(试行)》，明确了监管数据的定义、安全要求以及相关管理措施。

（7）国家卫健委

发布了《十四五全民健康信息化规划》要求建立健全的数据安全管理制度，包括数据的收集、存储、使用、加工、传输、提供和公开等各个环节；《关于进一步完善医疗卫生服务体系的意见》强

调加快健康医疗数据安全体系建设，提高医疗卫生数据安全防护能力。

3.2 地方层面

（1）贵州省贵阳市

贵阳市人民政府关于印发《贵阳市促进软件和信息技术服务业发展的若干措施》，对于通过数据安全能力成熟度模型（DSMM）2级及以上认证，且证书在有效期内的企业，给予一次性30万元资金支持。

贵州省贵安新区贵安新区人民政府关于印发《贵阳贵安促进软件和信息技术服务业发展的若干措施（修订）》，对首次通过数据安全能力成熟度模型（DSMM）2级及以上的企业，给予一次性20万元资金支持。

（2）上海市闵行区

闵行区人民政府关于印发《闵行区关于大力推进新型工业化高质量发展的若干政策意见》，对于完成智能制造能力成熟度模型、数据管理能力成熟度模型、数据安全能力成熟度模型等贯标的企业给予上限50万元的资助。

（3）天津市

天津市印发《天津市关于进一步支持发展智能制造政策措施的通知》，支持大数据评估。对大数据领域合同额占主营业务收入60%以上的企业，给予不超过合同额10%、最高50万元支持。对首次通过国家《数据安全能力成熟度模型》（GB/T 37988—2019，DSMM）、

《数据管理能力成熟度评估模型》（GB/T 36073—2018，DCMM）认证的企业，分别给予最高 50 万元支持。

（4）重庆市合川区

重庆市合川区人民政府印发《合川区加快网络安全产业发展的若干政策》，对通过数据安全能力成熟度模型（DSMM）二级、三级、四级的企业分别给予 10 万元、15 万元、20 万元奖励。

（5）青岛市

青岛片区管委印发《中国（山东）自由贸易试验区青岛片区关于支持先进制造、科技创新高质量发展的试行政策》，对新通过国家“两化融合管理体系”、CMMI、ITSS、DCMM、DSMM 等资质认证的企业，按照最高不超过申报项目平均认证成本的 90% 给予补贴，每家企业最高补贴 50 万元。

青岛西海岸新区印发《青岛西海岸新区关于支持“5G+工业互联网”融合应用的若干政策》的通知，对新通过国家“两化融合管理体系”、CMMI、ITSS、DCMM、DSMM 等资质认证的企业，按照最高不超过申报项目平均认证成本的 90% 给予补贴，每家企业最高补贴 50 万元。

（6）无锡市

无锡市人民政府印发《市政府办公室关于推进数据基础制度建设的实施意见》，提出鼓励企业开展数据安全能力成熟度模型（DSMM）等国家标准的贯标，强化企业数据管理、应用和保护能力。

3.3 行业层面

3.3.1 各行业的规划要求

DSMM 评估适用于多个行业，包括但不限于大数据企业、信息技术产业、互联网企业、金融业、银行业、保险业、证券行业、电子商务平台、数据中心、政务和高校等企事业单位。DSMM 评估的收益包括帮助组织发现数据安全能力的短板，提升数据安全能力，增加企业数据安全的意识。

DSMM 标准在各行业的数据安全规划中起到了重要支持作用，它提供了一套系统化的方法来指导组织机构如何建设和评估自身的数据安全能力。DSMM 评估不仅关注企业业务数据的保护，还全面展示企业数据安全能力的成熟度评估等级，帮助企业识别和解决数据安全方面的问题，给出评估结论和安全提升建议。

序号	行业	规划名称	规划内容
1	工业	《工业和信息化领域数据安全管理办法》	明确了该领域内数据处理的规范与要求，同时强调数据的分类分级管理，并着重提出了对重要数据和核心数据的保护要求。
2		《工业领域数据安全标准体系建设指南》	提供了一个全面的框架，旨在指导工业领域在数据安全方面的标准化工作，强调加强数据全生命周期安全管理，涉及数据收集、存储、使用、加工、传输、提供、公开等环节。
3	教育	《关于加强教育系统数据安全工作的通知》	要求建立数据安全责任体系和分类分级制度，形成数据资源目录，健全全生命周期数据安全保障制度，建立个人生物识别信息审查制度和数据安全评估制度，常态化开展数据安全监测预警通报，构建数据安全协同治理新格局。
4	金融	《中国人民银行业务领域数据安全	旨在规范金融机构的数据处理活动，明确数据安全管理的职责和要求。

		全管理办法（征求意见稿）》	
5		《监管数据安全管理办法（试行）》	明确了监管数据的定义、安全要求以及相关管理措施。
6	卫 生 健康	《十四五全民健康信息化规划》	要求建立健全的数据安全管理制度，包括数据的收集、存储、使用、加工、传输、提供和公开等各个环节。
7		《关于进一步完善医疗卫生服务体系的意见》	强调加快健康医疗数据安全体系建设，提高医疗卫生数据安全防护能力。

3.3.2 标准框架对行业安全标准的影响

（1）政务行业

2019 年，贵州市场监管局牵头立项了贵州省“一云一网一平台”标准体系等 25 项地方标准，其中关于政务数据安全的《DB52T 1540.6-2021 政务数据 第 6 部分：安全技术规范》于 2021 年 8 月 18 日正式发布，关于政务数据安全技术框架，DSMM 重要的参考和输入，成为了政务行业的标准的重要安全基线。

（2）交通运输

2022 年启动了“交通运输数据安全合规性评估指南”的研究和编制，期望建立适用行业内安全需求和管理现状的评估指标体现，改指南的框架合理的借鉴了 DSMM 3 级的要求并结合了行业特征。

网络预约汽车服务提供过程中，主要关注网络环境中的数据收集、存储、使用、加工、传输、提供和公开等数据处理活动的安全性要求。GB/T 42017-2022《信息安全技术 网络预约汽车服务数据安全要求》，提出网络预约汽车服务提供者的数据安全能力应至少符合 GB/T 37988 中的 2 级能力要求。

（3）电子商务

网上购物服务提供过程中，主要关注网络产品和服务在安全性方面的要求，以确保网络产品和服务的设计、开发、部署和维护过程中能够保护用户的数据安全和隐私。GB/T 42014-2022《信息安全技术 网上购物服务数据安全要求》，提出网上购物服务提供者的数据安全能力应至少符合 GB/T 37988 中的 2 级能力要求。

（4）即时通信

即时通信服务提供过程中，主要关注网络环境下的数据收集、存储、使用、加工、传输、提供和公开等数据处理活动，尤其是个人隐私保护。GB/T 42012-2022《信息安全技术 即时通信服务数据安全要求》，提出即时通信服务提供者的数据安全能力应至少符合 GB/T 37988 中的 2 级能力要求。

（5）快递物流

快递物流服务提供过程中，主要关注网络环境下的数据收集、存储、使用、加工、传输、提供和公开等数据处理活动，尤其是个人隐私保护。GB/T 42013-2022《信息安全技术 快递物流服务数据安全要求》，提出快递物流服务提供者的数据安全能力应至少符合 GB/T 37988 中的 2 级能力要求。

3.3.3 行业的贯标实践

DSMM 政策在不同行业实施时，会根据行业的特定需求、数据特性、业务流程和监管要求进行调整和定制。

(1) 金融行业。金融行业对数据安全要求极高，因此 DSMM 的实施通常会非常严格。同时还会考虑金融监管机构的要求，如中国人民银行和银保监会的规定，对 DSMM 的相关评估内容进行增强。

(2) 电信行业。电信运营商处理大量用户数据，因此 DSMM 的实施重点在于保护用户隐私和通信安全。实施中会侧重于网络安全和用户数据的加密存储及传输。

(3) 医疗行业。医疗数据涉及个人隐私和敏感信息，DSMM 政策会着重于患者信息的保密和安全。医疗机构会遵循《中华人民共和国数据安全法》和《个人信息保护法》等法律法规。

(4) 教育行业。教育行业在实施 DSMM 时，会特别关注学生和教职工个人信息的保护。政策实施会与教育信息化和网络安全管理相结合。

(5) 工业和制造业。工业领域在实施 DSMM 时，会关注工业控制系统和智能制造的数据安全。政策会支持企业采用先进的数据保护技术，如区块链和物联网安全解决方案。

(6) 互联网企业。互联网企业在处理用户数据时，DSMM 的实施会非常关键，以确保数据的合规使用和存储。企业需要遵循国家互联网信息办公室等监管机构的相关规定。

(7) 政府机构。政府部门在实施 DSMM 时，会侧重于保护国家机密和公民个人信息。政策实施会与电子政务和智慧城市建设紧密结合。

（8）电子商务。电子商务平台需要处理大量交易数据，DSMM政策的实施会强调数据的加密和用户隐私保护。企业会依据国家市场监管总局等机构的要求来加强数据安全。

（9）交通运输。交通行业在实施 DSMM 时，会关注乘客信息和物流数据的安全。政策会支持使用安全技术来保护车辆通信和导航系统的数据。

（10）能源行业。能源行业在实施 DSMM 时，会特别关注关键基础设施的数据保护，如电网和石油天然气系统。政策会强调数据安全技术的应用和跨部门的数据安全管理。

不同行业的 DSMM 实施情况会根据行业特点和监管环境有所不同，但共同的目标是提高数据安全能力，确保数据的安全和合规使用。随着数据安全法规的不断完善和技术创新，DSMM 的实施将更加深入和广泛。

3.3.4 对企业数据安全治理的促进

DSMM 对企业数据安全治理的影响，主要体现在以下几个方面：

（1）提供标准化评估框架

DSMM 为企业提供了一个系统化的数据安全能力评估框架，从组织建设、制度流程、技术工具、人员能力四个维度综合考量企业的数据安全能力。这种框架有助于企业全面审视自身在数据安全方面的优势和不足，为数据安全治理提供明确的方向和目标。

（2）推动数据安全管理体系建设

DSMM 强调以数据为中心，围绕数据全生命周期进行安全管理和能力建设。这促使企业在构建数据安全管理体系时，注重从数据采集、传输、存储、处理、交换到销毁的全过程管理，确保数据在各个阶段都得到充分保护。同时，DSMM 还关注组织架构、制度流程、技术工具和人员能力等方面的建设，为企业提供了全面的管理体系建设指导。

（3）提升数据安全防护能力

通过 DSMM 的评估和指导，企业可以识别出数据安全方面的潜在风险和薄弱环节，并采取相应的措施进行改进和提升。例如，企业可以根据 DSMM 的要求加强数据安全技术的研发和应用，提升数据分类分级、加密脱敏、访问控制等安全防护能力；同时，加强数据安全人才的培养和引进，提升人员的安全意识和专业能力。这些措施有助于企业构建更加完善的数据安全防护体系，提升数据安全防护水平。

（4）促进合规性和持续改进

DSMM 与相关法律法规和标准紧密衔接，确保企业在数据安全治理过程中符合合规性要求。通过 DSMM 的评估和改进机制，企业可以不断发现自身在数据安全方面的不足和问题，并采取持续改进的措施进行提升。这种持续改进的机制有助于企业不断提升数据安全能力水平，确保数据安全和隐私保护工作的持续有效进行。

（5）增强市场竞争力和信誉度

随着数据安全和隐私保护意识的不断提升，越来越多的客户和合作伙伴开始关注企业的数据安全能力水平。通过 DSMM 的评估认证，企业可以向外界展示自身在数据安全方面的优势和实力，增强市场竞争力和信誉度。这有助于企业吸引更多的客户和合作伙伴，拓展市场份额和业务领域。

3.4 产业实践

3.4.1 服务侧

在 DSMM 产业实践的服务侧，为企业实施 DSMM 提供了全方位、多层次的支持，推动了 DSMM 在产业中的广泛应用和落地。

（1）评估与咨询服务

众多专业的咨询机构应运而生，拥有经过培训和认证的测评师团队，能够依据 DSMM 标准为企业提供准确、客观的评估服务以及定制化的咨询服务，能根据评估结果为企业制定针对性的数据安全改进方案。同时，提供涵盖组织架构优化、制度流程建设、技术工具选型和人员培训等方面的综合解决方案，帮助企业逐步提升数据安全能力成熟度等级。然而，不同的咨询机构在服务内容和侧重点上有所差异。例如：

① 咨询机构

提供全面的咨询服务。传统的咨询机构凭借其丰富的行业经验和专业知识，能够为企业提供全方位的 DSMM 咨询服务。包括帮助企业理解 DSMM 标准的要求和内涵，从组织建设、制度流程、技术

工具、人员能力等多个维度进行全面的评估和差距分析，找出企业当前数据安全管理体系与标准之间的差距。

制定定制化的解决方案。根据差距分析的结果，咨询机构可以为企业制定定制化的 DSMM 实施规划和路线图。明确各阶段的目标、任务和优先级，结合企业的业务特点、规模和发展战略，提供符合企业实际情况的具体建议和改进措施，以帮助企业逐步提升数据安全能力成熟度水平。

协助企业进行变革管理。在实施 DSMM 的过程中，往往需要对企业现有的组织架构、业务流程等进行调整和优化。咨询机构可以协助企业进行变革管理，帮助企业管理层和员工理解变革的必要性，协调各部门之间的工作，促进新的数据安全管理体系的顺利推行，减少变革过程中可能遇到的阻力和问题。

提供培训和知识转移。为了确保企业能够持续有效地实施 DSMM，咨询机构通常会提供相关的培训服务。培训内容包括 DSMM 标准解读、实施方法、最佳实践分享等，旨在提升企业人员对数据安全的认识和理解，培养企业内部的数据安全专业人才，同时将咨询过程中积累的知识和经验转移给企业，使其具备独立开展数据安全管理工作能力。

② 律师事务所

法律合规指导。律师事务所在 DSMM 产业实践中主要提供法律合规方面的专业服务。帮助企业解读和遵循相关的数据安全法律法规和标准，确保企业的数据安全管理措施符合法律要求。例如，在

数据采集、存储、处理、传输和销毁等各个环节，律师事务所可以依据法律规定，指导企业建立相应的合规流程和制度，避免因违法违规行而面临法律风险。

隐私保护咨询。随着数据隐私保护的重要性日益凸显，律师事务所可以为企业提供隐私保护策略的制定和咨询服务。协助企业处理用户隐私数据，明确用户数据的收集、使用和披露规则，制定隐私政策，保障用户的合法权益。在涉及跨境数据传输等复杂场景时，律师事务所能够根据不同国家和地区的隐私法规要求，为企业提供合规的解决方案。

合同与协议审查。对于企业与外部合作伙伴、供应商、客户等之间涉及数据安全的合同和协议，律师事务所可以进行专业审查，确保合同中明确了各方在数据安全方面的权利和义务，包括数据的归属、使用范围、安全责任划分等条款，以减少因合同不清晰而引发的纠纷和安全隐患。

合规审计与风险评估。律师事务所可以参与企业的数据安全合规审计工作，对企业的数据安全管理体系进行审查和评估，发现潜在的法律合规风险点。并根据审计结果，为企业提供整改建议和风险应对策略，帮助企业建立健全的数据安全合规风险管理机制。

③ 安全厂商

技术解决方案提供。安全厂商的核心优势在于其技术实力，能够为企业提供各种数据安全技术解决方案以支撑依据 DSMM 的要求开展数据安全能力建设。这包括数据加密技术，确保数据在存储和

传输过程中的保密性；访问控制技术，如身份认证、权限管理等，防止未经授权的访问；数据备份与恢复技术，保障数据的可用性和可恢复性；安全审计技术，对数据操作行为进行监测和记录，以便及时发现安全事件等。

安全产品研发与供应。安全厂商会不断研发和推出各类数据安全产品，如防火墙、入侵检测系统、数据防泄漏系统、安全管理平台等。这些产品可以帮助企业构建多层次的安全防护体系，抵御外部攻击和内部威胁。企业可以根据自身的需求和预算，选择适合的安全产品来提升数据安全防护能力。

安全服务支持。除了提供产品，安全厂商还会提供相关的安全服务。例如，安全咨询服务，帮助企业进行安全规划和架构设计；安全评估服务，对企业的数据安全状况进行检测和评估；安全运维服务，负责安全产品的安装、配置、维护和升级等工作，确保安全产品的有效运行和性能优化；应急响应服务，在发生安全事件时，能够迅速响应，采取措施进行处置，降低损失和影响。

与其他机构合作。安全厂商通常会与咨询机构、律师事务所等其他相关机构进行合作。与咨询机构合作，可以为企业提供更全面的 DSMM 解决方案，将技术与管理相结合；与律师事务所合作，可以更好地理解和满足法律合规要求，共同为企业打造符合标准和法规的数据安全管理体系。

（2）培训与教育服务

依托 DSMM 中对数据安全人员的管理能力、技术能力、合规能力、运营能力的要求,培训机构形成了完善的 DSMM 系列培训课程,通过培训,提高企业人员对数据安全的认识和技能水平,为 DSMM 的实施奠定人才基础。

DSMM 培训在培训内容、培训目标与受众等方面与国内现行的其他数据安全培训存在一定的差异性,例如由中国网络安全审查技术与认证中心开展的 CCRC-DSO(数据安全官)培训、中国信息安全测评中心开展的 CISP-DSG(注册数据安全治理专业人员)培训等。

① 培训内容

CCRC-DSO(数据安全官)涉及数据安全定位与态势、企业数据安全管理体系构建及实施、相关法律法规实务、数据安全技术实践与落地、个人信息保护及安全标准解读、境外主要国家及地区数据安全制度、安全基座上数据价值实现路径和方式等多方面内容。课程立足三大法律,拓展国际视野,构建三位一体框架,以数据为中心,兼顾安全与业务,配套落地工具,以培养懂数据、懂技术、懂合规的综合人才为目标,注重输入与输出相结合。

CISP-DSG(注册数据安全治理专业人员)知识体系结构包括信息安全知识(如信息安全保障、评估、网络安全监管、支撑技术等)、数据安全基础体系(结构化、非结构化、大数据应用及数据生命周期等技术知识)、数据安全技术体系(数据安全风险、各类数据安全技术、数据安全运维等知识和实践)、数据安全管理体系(数据

制度、标准、策略、规范、规划等技术知识和实践）。培训内容实用性强，涵盖国内相关政策文件、标准规范及全球最新实践。

DSMM（数据安全能力成熟度模型）培训重点围绕数据安全能力成熟度模型展开，包括数据安全的战略规划、组织架构、制度流程、技术工具、人员能力等多个维度。通过培训，学员能够深入理解 DSMM 模型的各个级别要求、评估方法以及如何基于该模型建立和完善企业的数据安全管理体系，提升企业整体的数据安全能力和成熟度水平。例如，培训内容会涉及如何进行数据分类分级、如何制定数据安全策略、如何保障数据全生命周期的安全等具体实践内容，同时也会强调数据安全与企业业务的融合以及如何通过数据安全能力的提升来创造价值。

② 培训目标与受众

CCRC-DSO 旨在培养能够应对数据安全挑战、构建数据安全治理框架、提升企业数据安全建设成熟度、实现数据安全合规运营、推动数据依法有序利用并培养数据安全高端人才的专业人员。适合政务、金融、教育、汽车、地产、电信、医疗、信息科技、互联网等单位及正在进行数字化转型的传统企业的管理决策人员、数据安全相关部门人员、数据安全相关单位管理层及商务技术人员、从事数据安全的律师及法务、合规、风险相关人员、审计师、咨询顾问等专业人士以及其他对数据安全领域有兴趣的人员。

CISP-DSG 主要目标是培养具备数据安全治理过程管理、数据安全技术体系设计、数据安全管理体系设计基本知识和能力的数

安全治理专业人才。面向从事个人信息保护、数据安全、网络安全、合规风控、信息审计、应急管理、安全监管等业务的专业人员，包括企业信息安全负责人、数据安全部门工作人员、大数据部门工作人员、信息安全管理人員、技术支持人員、运维人員、数据管理人員、风险管理人員、安全管理人員、安全监管人員、安全审计人員、数据信息使用者等。

DSMM 培训目标是帮助企业 and 组织提升数据安全管理和技術能力，达到相应的成熟度级别，以满足法律法规和业务发展的需求。受众广泛，且针对企业不同层级的人员设定有不同的课程体系，包括企业的数据安全管理人员、技术人员、合规人员，以及希望提升自身数据安全能力的各类组织和机构的相关人员。无论是大型企业还是中小型企业，只要涉及数据处理和管理，都可以从 DSMM 培训中受益，了解如何建立健全的数据安全管理体系，提高数据安全保障水平，降低数据安全风险。

总体而言，CCRC-DSO 侧重于培养综合的数据安全管理人才，强调企业层面的数据安全治理框架构建和运营；CISP-DSG 专注于数据安全治理专业能力的培养，针对数据安全领域的专项治理；DSMM 培训则以国家标准为依据，全面提升企业的数据安全能力成熟度。

(3) 技术产品与工具服务

科技公司研发并推出一系列支持 DSMM 实施的技术产品和工具，如数据安全管理平台、风险评估工具、加密软件等。这些产品和工

具能够帮助企业更高效地进行数据安全管理和风险防控。以下是一些常见的产品/工具种类分析。

产品/工具种类	功能	优势	应用场景
数据分类分级	帮助企业根据数据的重要性、敏感性等因素，对数据进行分类和分级，确定不同数据的保护级别和访问权限。例如，将数据分为机密、秘密、内部公开、外部公开等不同级别。	能够使企业清晰地了解数据资产的价值和重要性分布，为后续的数据安全策略制定和资源分配提供依据，提高数据管理的效率和针对性。	广泛应用于各类拥有大量数据的企业，如金融机构、互联网企业、大型制造业等，在数据治理的初始阶段发挥重要作用。
数据加密	通过加密算法对数据进行加密处理，使未经授权的人员无法获取数据的真实内容。包括对静态数据（如存储在数据库、文件系统中的数据）和动态数据（如在网络中传输的数据）的加密。	提供了高强度的数据保护，即使数据被非法获取，也能保证其保密性，防止敏感信息泄露。	适用于对数据保密性要求极高的场景，如涉及商业秘密、个人隐私数据的处理和传输，像金融交易数据、医疗病历数据的加密保护。
身份认证与访问控制	用于验证用户的身份，确保只有合法授权的用户能够访问相应的数据和系统资源。包括多种认证方式，如密码、指纹、令牌、生物识别等，并根据用户的身份和权限设置访问控制策略。	有效防止未经授权的访问，降低数据被滥用、篡改的风险，增强系统和数据的安全性。	各类信息系统、网络应用等都需要身份认证与访问控制工具，保障用户数据和系统的安全，如企业内部办公系统、电子商务平台等。
数据脱敏	对数据中的敏感信息进行脱敏处理，在不影响数据可用性的前提下，隐藏或替换敏	便于在开发、测试、数据分析等场景中使用真实数据的同时，保护敏感信息，避免	在软件开发、数据共享、数据分析等环节中经常使用，例如银行

	感数据内容，如将姓名、身份证号等替换为虚拟值。	因数据使用不当导致的隐私泄露问题。	在将数据提供给外部机构进行数据分析时，可先使用数据脱敏工具处理。
数据安全审计	对数据的访问、操作、传输等行为进行记录和监控，生成审计日志，以便对数据安全事件进行追溯和分析。	能够及时发现异常的数据操作行为和安全事件，为事后调查和责任追究提供证据，同时也有助于发现数据安全管理工作中的漏洞和风险点。	适用于对数据安全合规性要求较高的企业和组织，如政府部门、金融机构等，用于监督和保障数据安全策略的有效执行。
数据备份与恢复	定期对数据进行备份，并在数据丢失或损坏时能够快速进行恢复，保证数据的可用性和完整性。	在遇到硬件故障、人为误操作、自然灾害等导致数据丢失的情况下，能够迅速恢复数据，减少数据损失和业务中断的时间。	是各类企业和组织保障数据安全的重要手段，尤其是对于关键业务系统和重要数据，如企业的核心业务数据库、文件服务器等的备份。
数据防泄漏	通过监测和控制数据的传输、存储等环节，防止数据未经授权地流出企业或组织，如防止通过电子邮件、移动存储设备、网络上传等方式泄漏数据。	能够实时监控数据的流向，及时发现和阻止数据泄漏行为，保护企业的核心数据资产。	在企业内部网络环境中应用广泛，特别是对于拥有大量敏感数据且与外部有频繁数据交互的企业，如科研机构、高新技术企业等。

（4）认证与审计服务

认证机构依据 DSMM 标准为企业提供认证服务，证明企业的数据安全能力达到一定的成熟度等级。同时，审计服务机构也可协助企业进行内部审计，确保数据安全措施的有效执行和持续改进。

2021 年，数据安全认证（贵州）有限公司获得国家认证认可监督管理委员会批复，成为全国首家数据安全服务认证机构。这标志着贵州省在推动大数据战略行动向纵深发展，以数据安全为引领的大数据产业迈上了高质量发展的新台阶。2021-2024 年，北京、上海、广东、江苏、浙江、四川等地的认证机构陆续备案了 DSMM 认证规则。截至 7 月 31 日，全国备案 DSMM 认证规则的认证机构共 39 家。随着数据安全重要性的不断提升以及相关标准的逐步推广，未来可能会有更多的认证机构获得 DSMM 认证资质，且覆盖区域也有望进一步扩大。

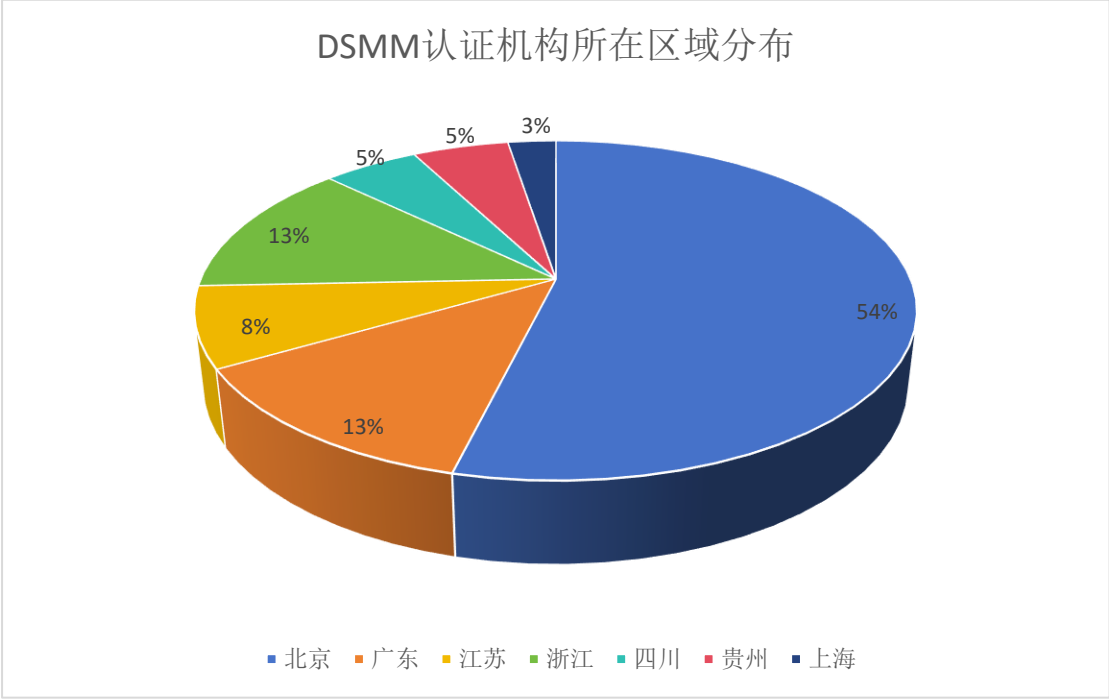


图 4 全国 DSMM 认证机构所在区域分布情况

3.4.2 需求侧

数据安全的需求侧是驱动数据产业发展的决定性因素。随着数字经济的发展，数据成为众多行业企业的重要生产要素，其安全直接关系到企业的业务安全以及数据未来的衍生价值安全。而随着数

据价值的提升，数据窃取、数据供应链泄露、数据滥用等数据安全风险激增，源于合规、业务发展、风险管理、行业竞争与协同以及用户隐私保护等方面的考量，监管、行业、企业及个人对数据安全的关注程度广泛提升，特别是在政务、金融、运营商等重点行业的数据安全技术和服务的需求旺盛，推动了 DSMM 在产业中的广泛应用和实践。

（1）监管层面

在安全三大法规要求的指引下，监管聚焦关系到国家安全、社会稳定的重点行业和业态，明确了对于重要数据的目录管理和报送机制、对于出海企业的网络安全审查机制、对于关基的安全保护机制、关于云安全的审查机制、关于数据出境合规路径等，数据安全能力成熟度可为企业满足以上监管要求并持续合规提供有效的提升路径，监管要求成为需求侧的重要组成部分。

（2）行业层面

一是满足行业内数据共享。行业内的数据共享可以促进创新，有助于提高行业整体效率，推动行业标准的形成和完善，提升整个行业的数据管理水平。DSMM 为行业提供了一套数据安全管理的标准和方法，通过实施 DSMM，企业可以建立起完善的数据安全体系，保护共享数据不被泄露、篡改或滥用。其次，在数据共享过程中，信任是关键。DSMM 可以帮助企业建立信任机制，通过第三方评估和认证，证明企业的数据安全能力达到一定水平，增强合作伙伴的信任，明确数据共享的责任和义务，避免因数据安全问题引发的纠纷。

二是满足行业间数据流通。不同行业之间的数据交互和共享日益频繁，需要统一的数据安全标准来保障数据的流通安全，DSMM 为行业间的协同合作提供了共同的语言和框架。

（3）企业层面

一是合规需求驱动。随着数据安全相关法规的日益严格，企业为了满足合规要求，落实数据安全监管要求方面的焦点问题，包含实现重要数据和核心数据等的识别与保护，个人信息主体权益保护、数据分类分级的落地、数据出境合规的实践等，避免法律风险，需要依据 DSMM 来评估和提升数据安全能力。

二是数据价值驱动。在数字化转型过程中，企业的业务对数据的依赖程度不断加深，保障数据安全成为业务稳定发展的关键。通过实施 DSMM，能够增强客户和合作伙伴对企业的信任，拓展业务机会。

三是风险管理驱动。企业可以依据 DSMM 的数据安全要求，对数据的采集、传输、存储、处理、交换、销毁全生命周期进行评估，识别和防范数据安全风险，降低数据泄露、篡改等事件对企业造成的损失。

（4）个人层面

个人隐私保护需求。用户对个人数据的隐私保护意识不断增强，要求企业提供可靠的数据安全保障。企业依据 DSMM 加强数据安全管理，能够满足用户对个人隐私保护的期望。

随着数据安全重要性的日益凸显，DSMM 认证受到了越来越多行业和企业关注，认证企业的数量呈上升趋势，且认证覆盖的区域也在不断扩大。据不完全统计，截至 2024 年 7 月 31 日，全国范围内通过 DSMM 认证，并获得认证机构颁发认证证书的共计 363 家组织，涵盖政务、通信、金融、能源、烟草、交通运输等领域。

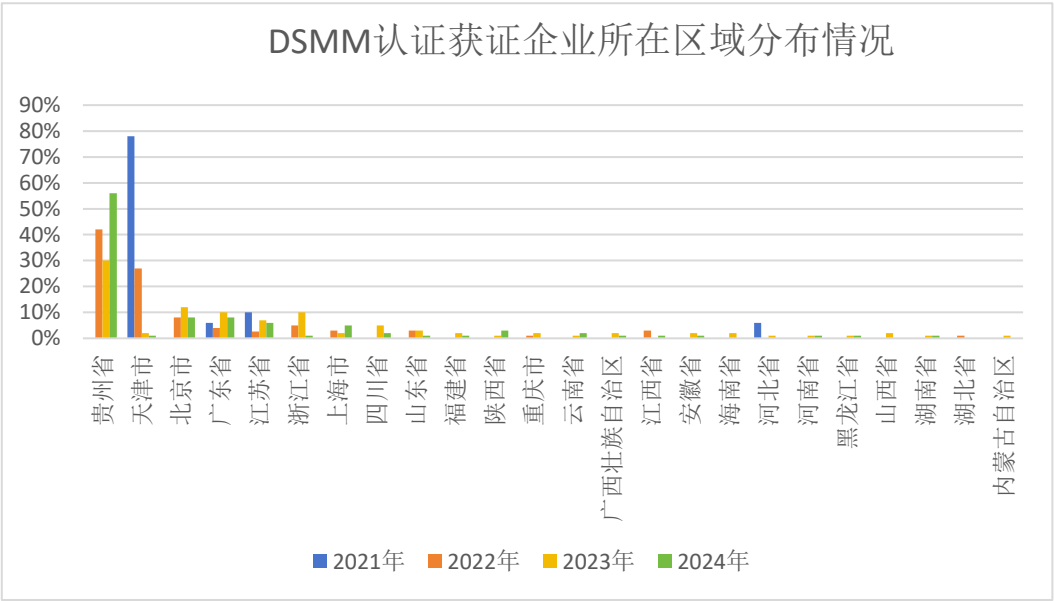


图 5 2021-2024 年度 DSMM 认证获证企业所在区域分布情况

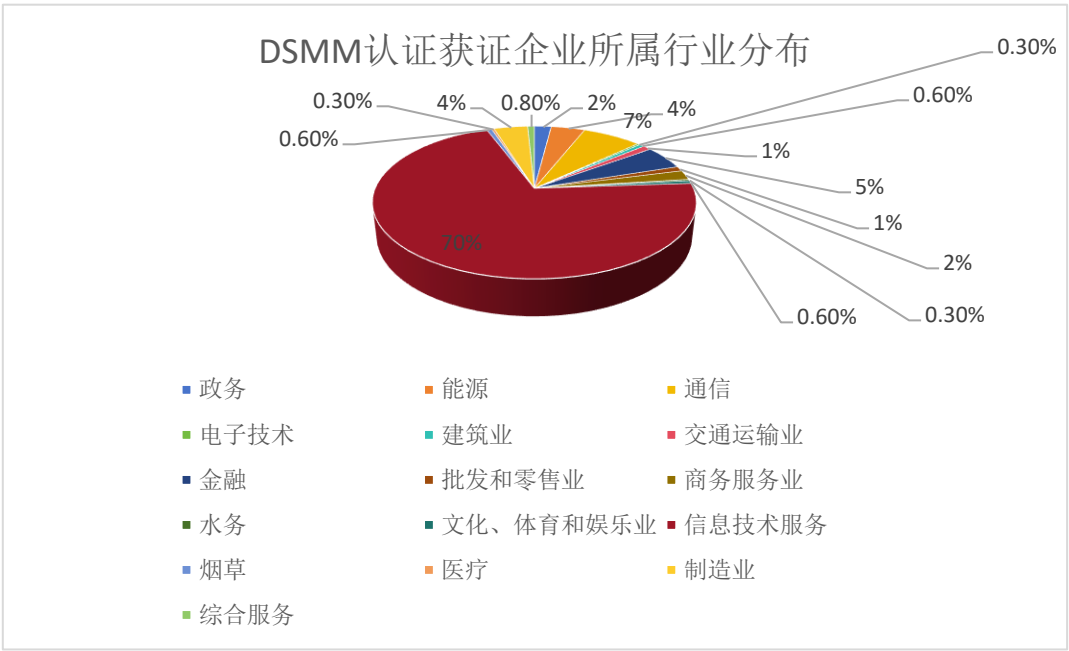


图 6 2021-2024 年度 DSMM 认证获证企业所属行业分布情况

3.5 实践中的挑战与问题

（1）市场推广问题

让数据安全治理从成本中心逐步转向价值中心。企业以往聚焦内部数据安全治理体系的构建，如今强调激活数据要素、发挥数据价值和构建开放服务。在数字化转型中，DSMM 不仅可以强化基础管理，在安全得到充分保障的情况下，还可以助力与业务深度融合，成为价值创造的核心工具。

然而，在市场推广中仍然面临企业对 DSMM 的认知度和接受度低、推广渠道有限、成本效益难以直观体现等问题。许多企业对 DSMM 了解有限，不清楚其价值和实施的必要性，导致市场推广难度大。部分企业认为数据安全工作已经在开展，没必要再依据新模型进行调整，对 DSMM 的独特优势和长远意义认识不足。DSMM 相关宣传和推广主要集中在专业领域的会议、论坛等，面向广大企业的普及性推广渠道不足，导致很多企业接触不到 DSMM 的信息。并且企业在考虑引入 DSMM 时，往往难以直接看到实施后带来的明确经济效益，更多的是潜在风险的降低和合规性的提升，这使得企业在决策时存在顾虑，影响市场推广速度。

（2）贯标实践问题

各企业在开展贯标工作时，存在标准理解与实际情况脱节、实施难度较大、缺乏行业针对性指导、评估认证较为复杂等问题。DSMM 的文字描述存在较多专业术语，与企业的实际业务和管理情况较难对应，企业在理解和应用标准时存在困难，无法将标准要求具体落

实到自身组织中。且要达到 DSMM 的要求，企业需要在组织建设、制度流程、技术工具和人员能力等多个方面进行全面提升和改进，这对于一些基础薄弱的企业来说挑战巨大，实施过程中可能会遇到各种阻力和问题。

DSMM 虽然有配套的实施指南，但由于行业众多，指南难以覆盖到所有行业的特殊情况，部分行业在依据标准进行贯标时缺乏更具针对性的指导，导致实施效果不理想。DSMM 的评估和认证过程相对也较复杂，涉及多个维度和大量指标，需要企业投入大量时间和精力准备相关材料，且不同评估机构的标准和流程可能存在差异，增加了企业的贯标成本和不确定性。

（3）产业生态问题

一个健康有序的产业生态能够为 DSMM 的推广和应用提供有利的环境，助力 DSMM 标准的有效实施，直接影响数据安全产业的健康成长。然而，在实践过程中仍然面临产业协同不足、专业人才短缺、技术创新滞后等问题。

DSMM 涉及到咨询、评估、认证、培训、技术服务等多种服务业态，但目前这些环节之间的协同合作不够紧密，存在各自为战的情况，尚未形成高效的产业协同效应。DSMM 的实施也需要既熟悉数据安全又了解企业业务和管理的复合型人才，但目前这类专业人才较为匮乏，人才培养体系尚不健全，难以满足产业快速发展的需求。并且随着信息技术的快速发展，新的数据安全威胁不断出现，但

DSMM 相关的技术创新和解决方案研发相对滞后，不能及时满足市场对新型数据安全防护的需求，影响产业生态的完善和发展。

四、DSMM 未来发展方向与预测

4.1 技术发展对 DSMM 的影响

随着安全大模型、云计算、基础安全前沿技术等的发展，为 DSMM 带来了新的机遇和挑战，但同时也伴随着一定的消极影响和安全风险。未来应积极关注这些技术的发展趋势，将其与 DSMM 相结合，不断提升数据安全能力，以适应数字化时代的发展需求。

（1）安全大模型的应用

一是风险评估更精准。安全大模型可以分析大量的安全数据和事件，为 DSMM 中的风险评估提供更准确的依据。通过对历史数据的学习，大模型能够预测潜在的数据安全风险，帮助企业提前采取防范措施。

二是安全策略优化。利用安全大模型的智能分析能力，可以为 DSMM 中的安全策略制定提供更科学的建议。大模型可以根据企业的具体情况和行业趋势，生成个性化的安全策略，提高数据安全管理的效率和效果。

三是自动化安全管理。安全大模型可以实现部分安全管理任务的自动化，如异常检测、威胁预警等。这有助于减轻企业在 DSMM 实施过程中的人力负担，提高安全管理的及时性和准确性。

安全大模型技术为 DSMM 带来新的机遇和能力提升的同时，也伴随着一系列风险和挑战。例如：

数据隐私与安全问题：安全大模型在处理数据时，可能涉及大量敏感数据，若这些数据被泄露或滥用，将对数据隐私和安全造成严重威胁。例如，训练数据中包含的个人信息、企业机密等数据，如果遭到窃取或不当使用，会引发隐私泄露风险。同时，大模型产生的数据量庞大且复杂，DSMM 需要适应这种大规模数据的全生命周期管理需求，确保安全大模型产生的数据在每个阶段都有明确的安全策略和控制措施。

模型误判与不确定性：安全大模型具有强大的分析能力，但仍可能存在误判或不确定性。在某些复杂情况下，可能会给出不准确的安全评估结果或建议，导致错误的决策。这可能影响 DSMM 评估的可靠性，使企业对自身数据安全状况产生误判。

技术依赖与风险集中：过度依赖安全大模型技术，可能导致企业在数据安全方面过于依赖单一技术解决方案，忽视其他传统安全措施的重要性。一旦安全大模型出现故障、被攻击或存在技术缺陷，可能会使企业的数据安全防线全面崩溃，造成严重后果。

因此在应用安全大模型技术时，企业需要充分认识到安全大模型技术带来的消极影响，并采取相应的措施来应对风险，如加强数据隐私保护、进行模型验证和评估、培养专业人才等，以确保数据安全管理的有效性和可靠性。

（2）云计算的发展

一是云安全策略与 DSMM 融合。企业在采用云计算时，需要将云安全策略与 DSMM 相结合。这包括选择可靠的云服务提供商、签

订明确的安全协议、实施数据加密和访问控制等措施。同时，企业还需要对云服务提供商的安全管理进行监督和评估，确保其符合 DSMM 的要求。

二是云原生安全与 DSMM 协同发展。云原生安全技术，如容器安全、微服务安全等，与 DSMM 可以协同发展。这些技术可以为云环境中的数据安全提供更全面的保障，同时也有助于推动 DSMM 在云环境中的应用和完善。

云计算的发展为 DSMM 带来积极影响的同时，也伴随着一定的安全风险，例如：

依赖第三方云服务提供商：企业使用云计算服务意味着对第三方云服务提供商的依赖增加。如果云服务提供商出现服务中断、故障或终止服务等情况，可能会对企业的业务运营和数据安全造成严重影响。

新技术应用带来的未知风险：云计算的发展不断推动新技术的应用，如人工智能、大数据、物联网等，新技术在带来便利和创新的同时，可能存在未知的漏洞或安全隐患，从而引入新的安全风险和挑战。

（3）信息技术应用创新的发展

一是自主可控与数据安全。信创强调信息技术的自主可控，这对于保障数据安全具有重要意义。在 DSMM 实施过程中，优先选择自主可控的信息技术产品和服务，可以降低数据被外部攻击和控制的风险。

二是信创生态与 DSMM 协同。信创产业的发展将推动形成更加完善的信息技术生态体系。在这个生态体系中，企业可以更好地实施 DSMM，实现数据安全管理与信息技术创新的协同发展。例如，信创产品的安全认证和评估可以为 DSMM 提供参考依据，促进数据安全水平提升。

三是信创政策推动 DSMM 落地。政府对信创的支持政策也将促进 DSMM 的落地实施。政府可以通过制定相关政策和标准，引导企业加强数据安全，推动信创产业与数据安全的深度融合。

信息技术应用创新的发展为 DSMM 带来积极影响的同时，也伴随着一定的安全风险，例如：

技术成熟度和稳定性风险：信创技术处于发展阶段，部分技术可能相对不够成熟和稳定。在 DSMM 实施过程中，如果采用不成熟的信创技术，可能会出现技术故障、漏洞等问题，影响数据的有效性和可靠性。

兼容性和互操作性问题：信创技术可能与现有非信创技术或不同厂商的信创技术之间存在兼容性和互操作性问题。在企业的复杂 IT 环境中，如果数据安全技术之间不能良好兼容和协同工作，可能会导致安全防护出现漏洞或盲区。对于 DSMM 而言，可能会影响安全能力维度中技术工具的协同作用，降低整体的数据安全防护水平。

（4）基础安全前沿技术的发展

一是操作系统层面的技术发展。现代操作系统在安全机制方面不断进步，如更严格的访问控制、身份认证技术、数据加密功能、

更精细的安全策略定义和执行、日益强大的安全监测和审计功能等，使得在 DSMM 框架下，企业能够利用操作系统提供的这些先进安全特性，更有效地保护数据的机密性、完整性和可用性，提升数据安全防护水平。

二是加密技术的发展。不断发展的加密技术，如量子加密、同态加密等，为 DSMM 中的数据加密提供了更强大的手段。这些先进的加密技术可以更好地保护数据的机密性和完整性，防止数据被窃取和篡改。

三是零信任安全架构。零信任安全架构强调对用户和设备的身份验证和授权，不默认信任任何内部或外部的实体。这与 DSMM 中的访问控制理念相契合，可以为企业提供更严格的数据安全保护。

四是隐私计算技术。如多方安全计算、联邦学习等，可以在不泄露原始数据的情况下进行数据计算和分析。这为 DSMM 中的数据共享和利用提供了新的解决方案，既满足了数据安全要求，又实现了数据的价值挖掘。

然而，先进的基础安全前沿技术往往具有较高的复杂性，这对企业的技术团队提出了更高的要求。企业需要具备足够的专业知识和技能来部署、配置和维护这些技术，否则可能导致技术应用不当，影响数据安全。同时，新技术的潜在漏洞和不确定性也会对企业的数据安全构成潜在威胁，在 DSMM 中，可能会影响企业达到较高的安全成熟度等级，因为即使企业在其他方面做得很好，但如果所采

用的前沿技术存在重大安全漏洞，也会降低整体的数据安全保障水平。

4.2 政策变化对 DSMM 的潜在影响

（1）网络安全法

网络安全法强调了网络运营者对网络安全的保护责任，包括保障数据的安全性。这促使企业更加重视数据安全，对 DSMM 产生了以下影响：

一是需求方面：企业为满足法律合规要求，对全面评估自身数据安全能力、发现潜在风险并进行整改的需求增加，从而推动对 DSMM 评估和认证的需求。

二是促进方面：促使企业加强在数据采集、传输、存储、处理等各个环节的安全措施建设，提升数据安全管理和技术水平，进而推动 DSMM 相关实践的开展和完善。

三是影响方面：让企业意识到数据安全在整体网络安全中的重要性，引导企业依据 DSMM 标准建立健全数据安全治理体系，提升数据安全保障能力。

（2）数据安全法

数据安全法是我国数据安全领域的基础性法律，其对 DSMM 的影响如下：

一是需求方面：明确了数据分类分级保护制度，这使得企业需要依据 DSMM 进行数据分类分级，以确定不同类别和等级数据的安全保护义务，从而产生对 DSMM 更细化和精准实施的需求。例如，

金融、工业等行业根据该法制定相应的数据分类分级规范，推动了 DSMM 在各行业的具体应用。

二是促进方面：规定了国家促进数据安全检测评估等服务的发展，支持相关专业机构开展活动，为 DSMM 评估认证提供了法律支持和发展契机，促进了 DSMM 评估认证机构的发展以及企业对 DSMM 的重视和应用。

三是影响方面：强调了建立健全数据安全治理体系，以数据为中心，从组织建设、制度流程、技术工具和人员能力等方面提升数据安全保障能力，这与 DSMM 的理念和维度相契合，推动企业按照 DSMM 要求构建全面的数据安全治理体系，提升整体数据安全水平。

（3）个人信息保护法

个人信息保护法聚焦于个人信息的保护，对 DSMM 的影响体现在：

一是需求方面：企业为确保个人信息处理活动的合规性，需要依据 DSMM 对涉及个人信息的数据安全能力进行评估和提升，尤其是在个人信息的收集、存储、使用、共享等环节，对 DSMM 中相关能力项的需求更为突出。

二是促进方面：促使企业在 DSMM 的框架下，进一步完善个人信息保护相关的制度流程和技术措施，加强人员培训和能力提升，以满足法律对个人信息保护的严格要求，推动 DSMM 在个人信息保护领域的深入应用和发展。

三是影响方面：强化了企业对个人信息安全的重视程度，使得企业在 DSMM 的实施过程中，更加注重个人信息相关的数据安全管理和技术防护，提升个人信息数据的安全性和隐私保护水平。

（4）数据二十条

《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》（“数据二十条”）中传达的整体精神和数据安全的相关要求，对 DSMM 未来发展的影响体现在：

一是需求方面：“数据二十条”强调的数据产权、流通交易、收益分配、协同治理等方面的制度建设，关注的数据从产生到使用的全过程等，使得各组织在数据处理的各个环节，需要更明确地界定数据安全风险，强化数据全生命周期各阶段的安全管控。各组织可以依据 DSMM 进一步细化组织建设方面的要求，明确不同角色在数据安全中的具体职责，以满足各组织清晰划分数据安全需求的需求，以及通过 DSMM 为数据全生命周期的安全管控提供更具针对性和全面性的安全保障措施指导。

二是促进方面：“数据二十条”强调了数据安全的重要性，这将促使更多的组织重视数据安全能力的提升。作为衡量组织数据安全能力水平的评估标准，DSMM 可能会得到更广泛的认可和应用。更多的行业、企业和组织为了满足数据安全要求、提升自身竞争力，会积极采用 DSMM 进行自我评估和能力建设，从而扩大 DSMM 的应用范围。同时，“数据二十条”的出台有利于激发数据安全产业的发展。

展活力。随着对 DSMM 需求的增加，围绕 DSMM 将形成更完善的产业生态。

三是影响方面：随着 DSMM 的广泛应用和不断发展，各行业组织依据 DSMM 标准加强数据安全能力建设，将促使行业整体的数据安全水平得到提升。这有助于减少数据泄露、滥用等安全事件的发生，增强公众对数据安全的信心，为数据要素的市场化配置和数字经济的健康发展创造良好的安全环境，进而推动整个行业朝着更安全、更规范的方向发展。同时，在“数据二十条”背景下，DSMM 的发展会促使企业和科研机构加大在数据安全技术方面的研发投入。为了满足 DSMM 更高的安全要求和适应复杂的数据应用场景，会推动数据加密、隐私保护、访问控制、安全审计等技术的创新发展，从而带动整个数据安全技术领域的进步。

（5）网络安全审查

网络安全审查办法将数据安全风险增加为国家网络安全风险评估的因素，将掌握超过 100 万用户个人信息的网络平台运营者国外上市列为网络安全审查的重要场景。其对 DSMM 的影响如下：

一是需求方面：企业尤其是涉及大量用户数据和境外上市的企业，为应对网络安全审查，需要通过 DSMM 评估来证明自身数据安全能力，提升数据安全水平，以满足审查要求，从而产生对 DSMM 评估的迫切需求。

二是促进方面：推动企业加大在数据安全方面的投入，包括完善数据安全管理制度、提升技术防护能力、加强人员安全意识培训等，进而促进 DSMM 在企业中的全面实施和持续改进。

三是影响方面：使企业更加关注数据安全风险，尤其是与国家安全相关的数据安全问题，促使企业依据 DSMM 标准构建更加稳健的数据安全防护体系，增强数据安全的整体保障能力，以应对可能的网络安全审查。

（6）境内外上市监管

政策变化对 DSMM 的影响主要表现为：

一是需求方面：拟上市企业，无论是在境内还是境外上市，都需要满足相应的监管要求，包括数据安全方面的要求。这使得企业为了顺利上市，需要借助 DSMM 来评估和提升自身的数据安全能力，以符合上市监管机构对数据安全的审核标准，从而增加了对 DSMM 的需求。

二是促进方面：促使企业按照 DSMM 的标准和要求，规范数据处理活动，加强数据安全治理，提升数据安全治理水平，以满足境内外上市监管对数据安全的严格要求，推动 DSMM 在企业上市过程中的应用和实践。

三是影响方面：强化了企业对数据安全在上市过程中重要性的认识，引导企业将 DSMM 融入企业整体治理架构，从数据全生命周期的角度保障数据安全，提升企业在上市过程中的竞争力和可持续发展能力。

（7）数据出境监管

《数据出境安全评估办法》《个人信息出境标准合同办法》《促进和规范数据跨境流动规定》的出台，对 DSMM 的影响如下：

一是需求方面：企业在进行数据出境活动时，需要依据 DSMM 评估自身和境外接收方的数据安全保护能力，确保出境数据的安全，这增加了企业对 DSMM 中数据安全能力评估和提升的需求，尤其是在数据传输、存储、处理等涉及出境环节的能力要求方面。

二是促进方面：推动企业加强数据出境相关的数据安全管理和技术防护能力建设，完善数据出境安全管理制度和流程，按照 DSMM 标准建立有效的数据安全保障体系，以满足数据出境监管的要求，促进了 DSMM 在数据出境场景下的应用和发展。

三是影响方面：强调了企业在数据出境过程中对数据安全的责任和义务，促使企业依据 DSMM 标准对数据出境活动进行全面的安全评估和风险管控，保障数据在跨境流动过程中的安全性和合规性，提升企业的数据安全治理水平和国际竞争力。

（8）“东数西算”战略工程

“东数西算”工程的推进对 DSMM 的发展带来的影响体现如下：

一是需求方面：数据安全保障需求：“东数西算”促使大量数据在东西部之间跨区域流动和存储，数据的安全性面临更多风险与挑战。这就迫切需要依据 DSMM 来构建全面、系统的数据安全保障体系，以满足“东数西算”工程中对数据安全的高要求。

二是促进方面：“东数西算”工程涉及众多企业、机构和数据中心，为了确保数据在跨区域传输和存储过程中的安全可靠，这些参与方需要遵循统一的数据安全标准和规范。这将促使更多企业和机构深入了解和应用 DSMM，以提升自身的数据安全能力和水平，从而推动 DSMM 在更大范围、更深层次的应用。

三是影响方面：“东数西算”工程的实施使得数据安全成为关注焦点，基于 DSMM 的要求，企业和机构会不断加强自身的数据安全建设，这将促使整个行业的数据安全意识和能力得到普遍提升，进而提高我国数据安全的整体水平，为数字经济的健康发展奠定坚实基础。

4.3 预测 DSMM 的长期价值与趋势

DSMM 的长期价值和发展趋势在数据安全领域具有重要意义。

一是合规性与风险防控。随着《数据安全法》《个人信息保护法》等法律法规的实施，DSMM 认证帮助企业满足合规要求，减少数据安全事件发生的概率，保护企业数据资产安全。

二是技术与产品创新。DSMM 鼓励技术创新，支持数据安全企业紧密围绕产业数字化需求，创新研发新兴融合领域专用数据安全产品，增强数据安全内生能力。

三是人才培养与引进。DSMM 认证的实施将促进数据安全相关学科专业建设和人才培养，同时鼓励企业引进海外优质人才与创新团队，扩充数据安全人才力量。

四是产业生态构建。DSMM 将助力构建繁荣的产业生态，包括推动产业集聚发展、打造融通发展企业体系、强化基础设施建设等，形成创新链、产业链优势互补的合作共赢关系。

五是国际合作与交流。DSMM 的国际化特点将有助于中国企业与国际标准接轨，促进数据安全领域的全球合作，加强与“一带一路”沿线国家数据安全产业合作，推动产品、服务、技术、品牌“走出去”，参与国际标准制定。

综上所述，DSMM 的长期价值在于帮助企业构建完善的数据安全管理体系，提升数据安全防护能力，同时，DSMM 的发展趋势将朝着技术创新、服务模式多元化、人才培养国际化以及产业生态协同化的方向发展。

五、结语

5.1 对企业与政策制定者的建议

（1）对企业的建议

一是提升数据安全战略，加强顶层驱动力。当前数据安全治理缺少来自企业高层的重视和引领，是一个较为普遍的共性问题，导致数据安全治理难以面向整个企业全面有效的开展。

二是严格落实数安法要求，完善数据安全治理体系。目前企业在数据安全治理方面已取得了初步成绩，但面向数据安全行业监管，如何建立完善、可靠的数据安全治理体系，如何在数字经济时代、新技术发展阶段提升数据安全防护能力，仍需要企业持续不断地优化改进。

（2）对政策制定者的建议

一是提升重点领域 DSMM 应用水平。充分发挥标准对产业发展的支撑引领作用，通过高质高效推进 DSMM 标准贯标工作，压实法定代表人或主要负责人数据安全第一责任，以 DSMM 的小“点”带动数据安全治理的大“面”，通过深入应用 DSMM，促进重点领域整体数据安全保护水平提升。

二是积极发展检测、评估、认证服务。《数据安全法》第十八条指出，国家促进数据安全检测评估、认证等服务的发展，并支持数据安全检测评估、认证等专业机构依法开展服务活动。通过法律规范和认证机制，一是持续推动了数据安全产业的健康发展，二是持续提升企业或组织的数据安全防护能力，三是护航数字经济高质量发展。

5.2 对 DSMM 产业未来发展的展望

数据要素市场化进程加快，数据流通交易需求加强，数据安全的重要性愈发突出，数据生态日益复杂的同时，人工智能等新技术发展带来的数据安全风险愈加严峻。DSMM 产业的未来也将围绕这些方向和难点继续发挥更大价值。

（1）紧扣数据要素市场化进程，让标准发挥基线作用。

在国家数据局的政策指导下，数据资源整合共享与开发利用的进程加快了，数据在组织内外的流通将逐渐成为普遍现象，数据安全问题随之而来。一方面，流通环节涉及的责任主体增多，如何有效划分各方数据安全风险，成为数据高效流通的基本保障；另一方

面，多频次、广范围的数据流转将带来更大的风险暴露面，如何保障流通环节的安全合规是现实问题。因此随着数据要素市场化的发展，数据安全风险在流通场景下会不断放大，数据安全工作难度加大，DSMM 国家标准的数据安全基线将在更大范围发挥作用。

（2）关注人工智能的发展与演进，用标准护航未来安全。

数据安全面临新技术发展与应用的挑战，人工智能技术可以通过对海量数据的收集分析与实时学习建立大模型文件，以驱动数据分类分级、数据安全风险监测等数据安全治理工作向智能化、高效化、精准化方向演进。同时，数据作为人工智能技术的主要输入之一，在训练、调优等过程面临数据窃取、数据泄露、数据篡改等安全风险，训练生成的模型文件也有可能遭到安全攻击，因此，大模型数据安全风险管理已经成为重要新议题，未来安全需要包含 DSMM 在内的一系列标准护航。

（3）研究日益复杂的数据生态，用标准支撑数据安全运营。

面对数据应用场景下愈加复杂多样的数据生态，数据安全的常态化能力与持续运营成为各机构保障安全、提升效率，降低风险的关键手段。另外，数据安全运营能力的构建能够打破各组织既有数据安全产品之间的壁垒，实现策略的有效整合，提升数据安全工作成效。

（4）继续标准的国际化之路，成为“一带一路”安全保障。

依托 DSMM 标准的国际化特点，通过加强与“一带一路”沿线国家等的数据安全产业合作，推动 DSMM 国内国外双循环，促进与

国际标准衔接和认证结果互认，保障中国产品、服务、技术、品牌“走出去”。

附录 相关政策汇编

序号	地区/部门	相关政策内容	出自文件	链接
1	贵阳市	DSMM2 级及以上认证给予一次性 30 万元资金支持。	《筑府办发(2020)5 号市人民政府办公厅关于印发贵阳市促进软件和信息技术服务业发展的若干措施(试行)的通知》	https://www.guiyang.gov.cn/zwgk/zfxxgks/fdzdgknr/lzyj/gfxwj/szfghxwj/qfbf/202004/t20200424_56676269.html
2	贵阳贵安	对首次通过数据安全能力成熟度模型(DSMM)2 级及以上的企业,给予一次性 20 万元资金支持。	《贵阳贵安促进软件和信息技术服务业发展的若干措施(修订)》	https://www.guiyang.gov.cn/zwgk/zfxxgks/fdzdgknr/lzyj/gfxwj/6szfgfxwj/qfbh/202306/t20230609_80136051.html
3	天津市	对首次通过国家《数据安全能力成熟度模型》标准二级和三级评估认证的企业,给予 40 万元奖励,对首次通过标准四级和五级评估认证的企业,给予 50 万元奖励。	《市委网信办:“2+4”政策引领大数据产业更好发展》	https://www.tj.gov.cn/sy/xwfbh/202009/t20200917_3717265.html
4	上海市闵行区	鼓励企业实施智能制造诊断并根据国家标准完成评估和贯标,对于完成智能制造能力成熟度模型、数据管理能力成熟度模型、数据安全能力成熟度模型等贯标的	《闵行区关于大力推进新型工业化高质量发展的若干政策意见的操作细则(征求意见稿)》	https://zwgk.shmh.gov.cn/mh-xxgk-cms/website/mh_xxgk/qzfgfxwj_wjca/content/c3

		企业给予上限 50 万元的资助。		f240a2-bd09-428f-bc05-62446debc440.htm
5	青岛市	对新通过 DSMM 等资质认证的企业，按照最高不超过申报项目平均认证成本的 90%给予补贴，每家企业最高补贴 50 万元。	《中国（山东）自由贸易试验区青岛片区关于支持先进制造、科技创新高质量发展的试行政策》	http://www.qingdao.gov.cn/zwgk/xxgk/bsgq/gkml/gwfg/202303/t20230302_7030880.shtml
			《关于支持“5G+工业互联网”融合应用的若干政策》	https://www.xihaian.gov.cn/zwgk/bmgk/xxhj/gkml/gwjdbmgw/202310/t20231026_7560137.shtml
6	无锡市	推行企业首席数据官制度，鼓励企业开展数据管理能力成熟度评估模型（DCMM）、数据安全能力成熟度模型（DSMM）等国家标准的贯标，强化企业数据管理、应用和保护能力。鼓励企业申请数据安全认证、个人信息保护认证等，支持企业参与公共数据安全治理。	《市政府办公室关于推进数据基础制度建设的实施意见》	http://www.wuxi.gov.cn/doc/2023/11/29/4123721.shtml
7	中央网信办、市场监管总局、工业和信息化部	推进数据密码保护、数据分类分级、数据脱敏脱密、数据跨境传输等数据安全相关标准研制。推动数据要素流通	《信息化标准建设行动计划（2024 — 2027 年）》	https://www.cac.gov.cn/2024-05/29/c_17185736261184

		标准研制。		37. htm
8	国家发展改革委、国家数据局、财政部、自然资源部	加快推进城市数据安全体系建设，依法依规加强数据收集、存储、使用、加工、传输、提供、公开等全过程安全监管，落实数据分类分级保护制度，压实数据安全主体责任。加强个人隐私保护。推进建设有韧性的城市数据可信流通体系，健全数据要素流通领域数据安全实时监测预警、数据安全事件通报和应急处理机制。	《关于深化智慧城市发展推进城市全域数字化转型的指导意见》	https://www.gov.cn/zhengce/zhengceku/202405/content_6952353.htm
9	国务院办公厅	围绕健全国家网络安全法治体系,2024年拟制定《网络数据安全条例》。此次列入国务院2024年度立法工作计划，预计条例发布在即。	《国务院2024年度立法工作计划》	https://www.gov.cn/zhengce/content/202405/content_6950093.htm
10	国家发展改革委办公厅、国家数据局综合司	全面筑牢数字安全屏障，增强网络安全防护能力，健全数据安全治理体系，切实有效防范各类风险。	《数字经济2024年工作要点》	https://news.pconline.com.cn/1738/17389348.html
11	国家互联网信息办公室	保障数据安全，保护个人信息权益，促进数据依法有序自由流动。	《促进和规范数据跨境流动规定》	https://www.cac.gov.cn/2024-03/22/c_1712776611775634.htm
12	国家数据局综合司、中央网信办秘书局、工业和信息化部	调研各单位数据资源生产存储、流通交易、开发利用、安全等情况,要求按照公安部的要求组织填报《数据安全情况调	《关于开展全国数据资源调查的通知》	https://www.cac.gov.cn/2024-02/22/c_17102705601982

	息化部办公厅、公安部办公厅	查表》，旨在贯彻落实《数字中国建设整体布局规划》工作部署，摸清数据资源底数，加快数据资源开发利用，更好发挥数据要素价值。		50.htm
13	国家数据局、中央网信办、科技部、工业和信息化部、交通运输部等	加强数据安全保障。落实数据安全法规制度，完善数据分类分级保护制度，落实网络安全等级保护、关键信息基础设施安全保护等制度，加强个人信息保护，提升数据安全保障水平。丰富数据安全产品，发展面向重点行业、重点领域的精细化、专业型数据安全产品，开发适合中小企业的解决方案和工具包，支持发展定制化、轻便化的个人数据安全防护产品。培育数据安全服务，鼓励数据安全企业开展基于云端的安全服务，有效提升数据安全水平。	《“数据要素×”三年行动计划（2024—2026年）》	https://www.cs.com.cn/xwzx/hg/202401/t20240105_6383567.html
14	中央网络安全和信息化委员会办公室、中央机构编制委员会办公室、工信部、公安部	建设互联网政务应用应当落实网络安全等级保护制度和国家密码应用管理要求，对互联网政务应用网络和数据安全每年至少进行一次安全检测评估，应当按照国家、行业领域有关数据安全和个人信息保护的要求，对互联网政务应用数据进行分类分级管理，对重要数据、个人信	《互联网政务应用安全管理规定》	https://www.cac.gov.cn/2024-05/22/c_1718054910848581.htm

		息、商业秘密进行重点保护。		
15	国家金融监督管理总局	《办法》共九章八十一条。包括总则、数据安全治理、数据分类分级、数据安全治理、数据安全保护、个人信息保护、数据安全风险评估与处置、监督管理及附则。《办法》主要特点：落实数据安全责任制、明确数据安全归口管理部门、将数据安全风险评估纳入全面风险管理体系、强化数据安全评估、建立数据安全保护基线。	《关于促进企业集团财务公司规范健康发展提升监管质效的指导意见》	https://www.gov.cn/zhengce/zhengceku/202405/content_6948824.htm
16	工信部	要完善数据安全管理体系，具体举措是动态更新工业领域重要数据目录，督促指导企业加强重要数据保护，年度目标成果为编制工业领域重要数据目录。	《工业互联网专项工作组2024年工作计划》	https://wap.miit.gov.cn/jgsj/xgj/wjfb/art/2024/art_8ac5e4c97fd04f309fc5b4cf3d0e3d32.html
17	自然资源部	增强网络安全保障能力，强化数据安全保护能力，健全密码应用保障体系、加强新技术新业态安全保护（云安全、算法安全、模型安全等）。	《自然资源数字化治理能力提升总体方案》	https://www.gov.cn/zhengce/zhengceku/202402/content_6931049.htm
18	工业和信息化部、国家互联网信息办公室、国家发展和改革委员会	促进数据安全产业发展的指导意见	《十六部门关于促进数据安全产业发展的指导意见》	https://www.gov.cn/zhengce/zhengceku/2023-01/15/content_5737026.htm

	委员会等十六部门			htm
19	国家互联网信息办公室、国家发展和改革委员会、工业和信息化部、公安部、交通运输部	规范汽车数据处理活动,保护个人、组织的合法权益,维护国家安全和公共利益,促进汽车数据合理开发利用	《汽车数据安全 管理若干规定 (试行)》	http://www.cac.gov.cn/2021-08/20/c_1631049984897667.htm
20	安徽省通信管理局	全面提升我省电信和互联网行业网络和数据安全管理水平,推动电信和互联网行业高质量发展。	《关于开展 2024 年电信和互联网行业“江淮护航”网络和数据安全专项行动的通知》	https://www.shangyexinzhishi.com/article/20647477.html
21	浙江省通信管理局	为深入贯彻落实党的二十大精神 and 习近平总书记关于网络安全的系列重要讲话精神,做好庆祝新中国成立 75 周年网络安全保障工作,进一步提升我省电信和互联网行业网络安全和数据安全防护水平,护航电信和互联网行业高质量发展,按照工业和信息化部、省委省政府总体部署,现决定组织开展 2024 年电信和互联网行业网络和数据安全检查工作。	《关于开展 2024 年电信和互联网行业网络和数据安全检查的通知》	https://zjca.miit.gov.cn/zwgk/tzgg/art/2024/art_4e98a5b21d074954bba967a260bea2df.html
22	江西省工业和信息化厅	加快全省工业领域数据安全保障体系建设,全面提升我省工业领域数据安全防护能力,促进	《江西省工业领域数据安全能力提升实施方案 (2024-	http://www.jiangxi.gov.cn/art/2024/6/7/art_5

		数据安全产业发展，结合我省工作实际，制定本实施方案。	2026 年）》	006_4912870.html
23	山西省工业和信息化厅	促进我省工业领域数据安全保护能力水平跃升，进一步夯实我省新型工业化安全基石。	《山西省促进工业领域数据安全能力提升实施方案（2024-2026 年）》	https://www.sohu.com/a/768429144_121738814
24	广东省通信管理局	主要开展以下六方面检查：安全合规管理制度机制、网络安全防护检查、数据安全和个人信息保护检查、市场秩序和用户权益保护工作检查、互联网基础资源合规检查、反诈义务落实情况检查。	《2024 年广东省电信和互联网行业网络数据安全和应用合规行政检查》	https://www.cagd.gov.cn/v/2024/03/4820.html