***摘 要：****对证券期货行业而言，不断提升数据安全治理水平，在促进数据利用同时，保障数据安全，对促进数字经济发展具有重要意义。本文聚焦数据安全治理路径，提出从数据安全合规出发，严格落实监管要求，结合机构或企业自身实际，选择合适数据安全治理框架，参考通行的技术标准，不断实践并迭代提升的思路。*

***关键字：****数据安全  数据安全治理 路径*

**一、背景**

**数据是做强做优作大数字经济的重要基础。**2022年第2期《求是》杂志刊发了习近平总书记的重要文章《不断做强做优做大我国数字经济》，指出数字经济正在成为重组全球要素资源、重塑全球经济结构、改变全球竞争格局的关键力量。在2023年2月印发的《数字中国建设整体布局规划》中指出要按照“2522”的整体框架进行布局，夯实数字基础设施和数据资源体系“两大基础”。

**数据安全治理是建设“数字中国”的重要保障之一。**在《数字中国建设整体布局规划》指出，要强化数字中国关键能力，一是构筑自立自强的数字技术创新体系。二是筑牢可信可控的数字安全屏障。在《数据安全法》指出：维护数据安全应建立健全数据安全治理体系，提高数据安全保障能力。

**数据安全治理是一个长期化过程，需要选择适当的、可持续优化的路径。**显而易见，在“数字中国”发展战略指引下，数据成为经济发展的重要驱动要素，也是企事业单位拥抱数字经济的必然选择。在证券期货行业的企事业单位，也必然要从自身实际出发，结合行业、企业特点，建立健全企业数据安全治理体系，提高数据安全保障能力，积极参与数字中国建设，为促进数字经济发展添砖加瓦。

**二、数据安全治理基本要素**

在证券期货行业，做好数据安全治理，有三个基本要素需要在先期进行考量。它们分别是合规、质量和成熟度。

**（一）合规**

**合规是根本性基础。**

合规包含了法律法规层面、监管要求及本单位的制度层面合规。合规是做好数据安全治理基本依据，同时也是底线性要求。不能全面细致分析、理解并严格落实合规要求，在后续的实施环节就可能存在重大缺点和漏洞，甚至可能出现违法、违规的情况。

法律法规层面，涉及数据安全的包括《网络安全法》、《数据安全法》、《个人信息保护法》，《关键信息基础设施保护条例》等。

监管要求层面，证券期货行业需要严格遵循和落实证监会有关基本要求，同时根据不同情形，也需要遵循人民银行发布的有关要求。

企业内部制度，一般是在前两者基础上结合本单位实际制定，不做赘述。

如图1所示，证券期货行业机构在数据安全领域需要遵循的主要合规，其他未在图中列明的要求，建议各机构可自行梳理补充。



图1：与数据安全相关的主要合规要求（部分）

**（二）质量**

**数据质量是基本保障。**

数据质量是数据治理中的重要环节，同时也是数据安全治理基本保障之一。数据质量低下，就可能造成很难理清数据资产、数据模型不统一、数据格式混乱等等问题，同时造成分类分级不准确，保护措施落实不到位等等问题。因此，数据安全治理中要确保数据质量的协同改进和提升。

数质量一般需要较为规范、统一的数据模型，标准化的数据规范，同时需要持续的维护和更新。在证券期货行业，由于行业特定业务属性，还需要考量数据的跨机构访问、使用以及监管方对数据分析、审查等等需要，所以也需要遵循一定特定标准。

提高数据质量，除结合本企业的业务特点外，同时应关注两点，一是**要遵循行业监管要求**，例如《中国证监会数据管理办法（试行）》《中国证监会数据质量管理细则（试行）》，特别是后者中规定的数据质量评价指标，可以视为证券期货行业数据质量贯标的基本依据；二是**要关注证券期货行业相关标准**，例如证券期货业数据模型相关标准、证券期货业投资者权益相关数据的内容和格式相关标准（可在资本市场标准网查询和下载）。

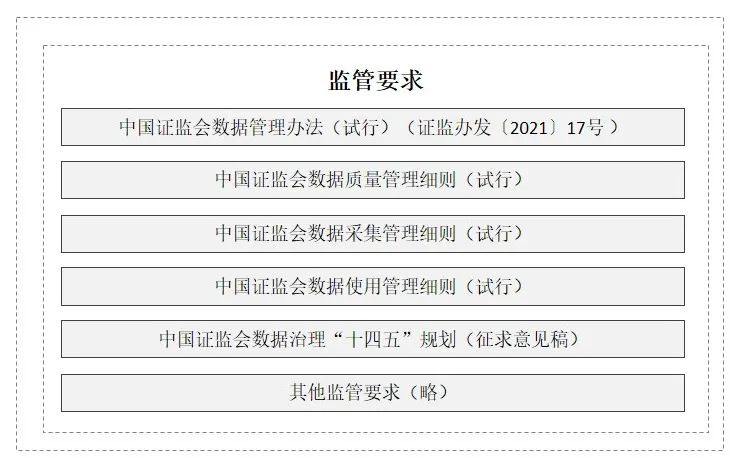


图2：与数据质量相关的主要监管要求

除上述之外，较高的数据质量，可以为通过使用工具实现数据治理铺平道路，也可以为进一步提升数据质量管理水平。从而为实现工具化、平台化的数据安全治理工作铺平道路。

**（三）成熟度**

**数据安全治理的成熟度是一个逐步提高的过程。**

成熟度这个概念本身就说明了一种逐步迭代，不断改进和提升的过程。数据安全治理基本目标就是通过一系列的治理活动，不断提升数据安全能力成熟度。大家熟知的数据安全能力成熟度模型（Data Security Capability Maturity Mode，简称DSMM）于2019年8月30日正式发布《信息安全技术 数据安全能力成熟度模型》（GB/T 37988-2019），为衡量一个组织的数据安全能力成熟度水平提供了可评判的基本依据。企业或组织通过这个衡量“标尺”，可以清晰的识别自身数据安全能力短板，从而有目的、有针对性的实施数据安全管理，补足短板，持续改进和提升数据安全能力。

**三、数据安全治理思路**

数据安全治理不是一蹴而就的，也不可能通过一次改进或治理活动就能够彻底解决所有问题，需要抓住重要的、迫切的关键性问题，反复迭代，持续改进。图3是本文主要讨论的一个数据安全治理路径，供参考。

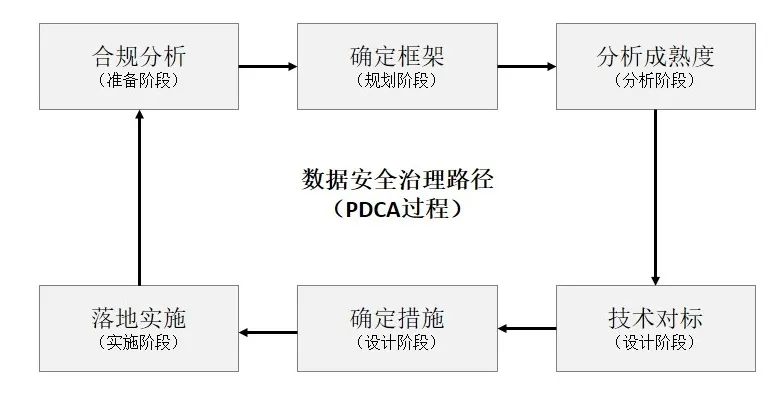


图3：数据安全治理路径

**（一）准备阶段——从确保合规出发**

证券期货行业作为国家金融领域重要行业，一定要切实把握合规的重要性，将合规作为基本出发点。从确保合规出发提升数据治理能力，需要做好几项必要的工作：

**1.深入理解并严格遵守法律法规要求**

最基本《网络安全法》《数据安全法》、《个人信息保护法》要深入理解并遵守。结合本单位特点，如果是关键信息基础设施单位，还要遵守《关键信息基础设施保护条例》及相关要求。涉及可能存在国家核心数据、重要数据的，还应考虑遵守《网络安全审查办法》；涉及数据出境的，还应遵守《数据出境安全评估办法》等规章。证券期货行业机构还应遵循《证券期货业网络和信息安全管理办法》等要求。这些都是要结合企业自身特点进行汇总、整理，深入分析、理解并严格遵守和落实的。

**2.将法律法规和监管要求科学融入自身数据安全管理相关制度**

数据安全的落实离不开具体落实，而法律法规、监管要求通常要考虑通用性、普遍性，行业机构或企业就要结合自身特点，在法律法规、监管要求基础上进一步细化和完善，并科学融入到企业自身制度中。例如关键信息基础设施运营者，就应制定适合自身特点的有关关键信息基础设施相关的数据安全保护制度、规范、方案。而如证券公司、期货公司、基金公司的投资者客户众多，也需要结合自身特点，制定可覆盖投资者个人信息保护的相关制度，从而为切实保障投资者个人信息安全奠定基础。

**（二）规划阶段——选择合适数据安全治理框架**

在对数据安全合规充分认识的基础上。实施数据安全治理，应该选择一个适当数据安全治理框架。目前国内外有多种版本的数据安全治理框架，建议证券期货行业机构或企业结合自身实际和国情出发选择自身的治理框架。常见的数据安全治理框架主要有：

**Gartner数据安全治理框架。**Gartner最早提出数据安全治理理念，并认为数据安全治理不仅仅是一套用工具组合的产品级解决方案，而是从决策层到技术层，从管理制度到工具支撑，自上而下贯穿整个组织架构的完整链条。**Gartner数据安全治理框架更加强调过程性**，包含了五个过程：平衡业务需求与风险，识别、确定优先级和管理数据集生命周期，定义数据安全策略，实施安全产品，制定所有产品的政策。

**微软数据安全治理框架DGPC。**微软的治理框架更加侧重强调隐私、保密和合规，以更好实现数据安全风险控制。主要围绕“人员、流程、技术”三个核心能力领域的具体控制要求，同时强调与现有安全框架体系或标准协调合作。

**中国软件评测中心网安中心数据安全治理框架（本文以下简称“软测框架”）。**改框架更强调以“让数据使用更安全”为目的，通过组织构建、规范制度、技术支撑等要素共同完成数据安全建设的方法论。框架的核心内容主要由治理层、管理层、执行层和监督层四个层面组成。

应该说这些框架有自身的特点和重要价值，没有绝对的优劣可言，笔者更倾向于选择融合各家长处的方式，例如以软测框架为蓝本，把握治理过程理念，围绕“人、流程、技术”展开。除此之外，国内外还有一些安全机构或企业发布了数据安全治理框架，也可以作为参考框架标准。

**（三）分析阶段——评判成熟度水平，识别短板**

数据治理涉及的方面很多，如何确定自身的短板和关键点，作为一段时期的切入点更加合适，建议将《信息安全技术 数据安全能力成熟度模型》（GB/T 37988-2019）作为基本的自评估（或外部评估）标准。

DSMM的架构由四个安全能力维度、七个安全过程维度、五个安全能力等级构成。四个安全能力维度:组织建设、制度流程、技术工具、人员能力；七个安全过程维度：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、通用安全，共计30个过程域。五个安全能力等级：从低到高依次1至5级。

如前所述，已选取的了数据安全治理框架，在执行DSMM自评估时，需要注意的是，不但要根据DSMM架构分析自身长处和不足，同时要与框架中的内容对应起来，这样就可以评判当前数据安全治理的关键要点在哪些方面。例如，可以将DSMM架构中的组织建设、制度流程与软测框架中的治理层、管理层内容对应起来。同时要注意，软测框架将技术和人员隐含在其中，需要审慎地将DSMM中技术工具、人员能力与软测框架中的有关内容对应。

此外，在DSMM评估基础上，一方面可以知道机构或企业自身数据安全能力水平；另一方面，可以明确数据安全治理框架有哪些薄弱环节，以便在下一步治理工作中进行改进。

为什么不选择在所有的工作开展前首先进行DSMM评估？笔者认为在缺乏明确的出发点和基本建设目标的情况下，直接进行DSMM评估不利于判断哪些环节更需要改进，同时也容易造成改进目标不明确，后续的工作可能变成“胡子眉毛一把抓”。

**（四）设计阶段——结合相关标准完善制度和措施**

在上述评估基础上，需要有针对性地对已确定的治理框架的薄弱环节进行提升和改进。基本的建议有以下几点：

（1）制度层面要确保以合规为基础，结合自身实际制定。

（2）管理层面要把握的高效、协同，流程设计要综合考虑组织、人、技术协调，并尽可能简化。

（3）执行层面，要尽可能参考成熟的、有清晰指导意义的标准，例如在涉及数据生命周期的多个环节安全，可以参考主要标准包括:

* 涉及数据安全保护的，包括：《金融数据安全 数据生命周期安全规范》（JR/T 0223-2021）;《证券期货业数据安全管理与保护指引》（JR/T 0250—2022）;
* 涉及数据分类分级的，可以参考《金融数据安全 数据安全分级指南》（JRT 0197-2020）、《证券期货业数据分类分级指引》（JR/T 0158-2018）。

（4）保护措施选择层面，建议考虑技术与管理充分融合，避免技术手段看似先进，管理手段却落后的情形。建议尽可能多地考虑安全保护的逻辑性问题，避免看似有效的技术措施，在业务层面却丢失数据敏感性的保护。除严格落实强制规定外，还需要在技术措施的选择上兼顾数据使用便利性问题。这是就要结合特定场景来专门考虑的。

（五）实施阶段——在落实环节持续改进并定期回顾，迭代提升成熟度

如前所述，在确定了框架、找到了薄弱环节、明确了制度和措施基础上，就需要严格的落实并持续改进了。

数据安全能力是在不断落实治理的过程中，持续改进的。这个过程中，一是要注重边实施、边改进，持续提升管理与安全技术措施；二是要注重使用必要的数据安全管理工具，不断利用自动化技术、AI工具等提升管理、监控水平和数据安全审计能力；三是要注重阶段性的回顾，关注成熟度提升的进展，寻找薄弱环节，确定下一个迭代的改进计划，这也是最重要的一点。

**四、结束语**

数据安全治理的根本目标是在保障安全的前提下，促进数据利用。由于数据自身存在的分散性、流动性、多变性等特点，为数据安全治理带来了很高的挑战，也不可能有通用的、普适性的方法或路径能够解决数据安全治理中的所有问题。

本文仅提供了一种数据安全治理路径思路，在具体实践中，建议机构或企业结合自身实际，选择合适的治理路径，通过不断持续改进，必然会逐步提升数据安全能力，不断促进机构或企业的数字化转型。