君合研究简讯

JUNHE

2019 年 1 月 4 日

电信与互联网法律热点问题

《证券基金经营机构信息技术管理办法》正式发布

2018 年 12 月 19 日，中国证券监督管理委员会（以下简称“**证监会**”）正式发布了《证券基金经营机构信息技术管理办法》（以下简称“**《办法》**”）。证监会于 2017 年 5 月即发布了《办法》的征求意见稿（以下简称“**《征求意见稿》**”）。历经一年半，《办法》在《征求意见稿》的基础上进行了较大幅度的修改。

在《中华人民共和国网络安全法》出台，各行业逐渐加强对信息技术和网络安全监管的大背景下，《办法》对证券基金经营机构在信息技术方面的全面合规体系构建提出了框架性、全面性的要求，明确了监管方向和重点要求。以下我们将对《办法》涉及的各方面进行简要介绍，并分析可能的影响。

一、 《办法》基本适用于证券基金业务活动中的所有相关市场主体

《办法》在第一章明确适用于以下几类主体：

(1) 证券基金经营机构（证券公司和基金管理公司）；

(2) 信息技术服务机构（为证券基金业务活动提供重要信息系统的开发、测试、集成、测评服务以及重要信息系统的运维、日常安全管理服务的机构）；

(3) 证券基金专项业务服务机构；

(4) 从事证券公司客户交易结算资金存管活动的商业银行、从事公开募集基金的基金托管机构、证券基金经营机构在境内依法设立的子公司及其下设机构。

《办法》的适用范围相对广泛，对证券基金业务活动中信息技术相关市场主体基本全部覆盖。

我们注意到，《征求意见稿》在第二条专门将“专项业务服务机构”列举为适用主体之一，并在第五章专章规定了参照适用于专项业务服务机构的条款。《办法》在正文中删除了“专项业务服务机构”的相关规定，而改在第七章附则中规定“证券基金专项业务服务机构参照本办法执行。”而专项业务服务机构的范围有了一定程度的扩大，《办法》明确增加了从事投资顾问、评价、估值等基金服务业务的机构和证券投资咨询机构。该等规定实际仍然将专项业务服务机构纳入到《办法》的规制范围，但实践之中将如何比照执行则存有疑问。

二、 《办法》提出了证券基金经营机构搭建全面信息技术管理合规体系的框架性要求

1、 建立以董事会、管理层、信息技术治理委员会、首席信息官分层负责的治理体系

《办法》明确要求证券基金经营机构董事会审议本公司的信息技术管理目标，对信息技术管理的有效性承担责任。证券基金经营机构经营管理层负责落实信息技术管理目标，对信息技术管理工作承

担责任，组织实施董事会决议。

在公司管理层下，应再设立信息技术治理委员会或指定专门委员会，负责制定信息技术战略并审议有关事项。信息技术治理委员会成员除公司高级管理人员及内部部门负责人外,还可聘请外部专业人员担任信息技术治理委员会委员或顾问。

相比《征求意见稿》,《办法》将信息技术管理的有效性的责任主体上升到证券基金经营机构的董事会层面。并且,《办法》首次提出证券基金经营机构应当指定一名符合《办法》要求的人士担任首席信息官。

2、 建立包括系统安全、数据治理和应急管理方案在内的全方位信息技术合规制度和方案

在信息技术安全方面,《办法》从信息系统安全、数据治理、应急管理三个方面均作了细节性的规定。

在系统安全方面,《办法》要求对于重要信息系统的上线或重大变更，证券基金经营机构应制定专项实施方案，停用的则应开展影响评估，制定系统停用和数据迁移保管方案。持续监测重要信息系统的运行状况，跟踪异常情形并及时处置。相关文档均应采集并保存，确保满足应急处置和审计需要。

数据治理方面，新增了证券基金经营机构将经营及客户数据按照重要性和敏感性进行分类分级、并根据不同类别和级别作出差异化数据管理制度安排的要求。同时,《办法》特别强调证券基金经营机构应当记录数据和客户信息的使用情况，持续监督信息技术服务机构等相关方落实保密协议，一旦发现服务机构违规存储或使用自身经营数据和客户信息的，应责令其改正并销毁已获取的经营数据和客户信息，拒绝配合整改的服务机构应当立即终止合作。《办法》也强调证券基金经营机构不得收集与服务无关的客户信息，不得购买或使用非法获取或来源不明的数据，不得违法截取、留存客户信息，或以任何方式向其他机构、个人提供客户信息。

应急管理方面,《办法》要求制定应急预案，每年至少演练一次并保存演练报告，持续完善应急预案，应充分考虑重要信息系统故障、外包技术服务机构无法提供服务、重大人员变动、自然灾害等可能影响重要信息系统平稳运行的事件。备份系统应当与生产系统具备同等的处理能力。

《办法》删除了《征求意见稿》对经营机构重要信息系统在境内独立部署并将经营活动中收集和产生的重要数据和客户信息存放在境内的要求。但根据《网络安全法》等法律的要求，证券基金经营机构作为金融机构，其重要信息系统产生、收集的重要数据、个人信息，仍有可能被要求遵守本地化存储、出境前安全评估的法律要求。

3、 加强内部、外部审计保证持续性合规

《办法》第三、四章对于指导证券基金经营机构组织信息技术合规工作、管控风险和保障信息技术安全方面，提出了非常细致的审计要求，包括对内部审查的要求、定期信息技术管理工作专项审计（频率不低于每年一次）、委托专业机构开展信息技术管理工作全面审计（频率不低于每三年一次）、及时跟踪和整改问题、保存审计报告不少于二十年等。

4、 加强对于信息委托服务的监管

《办法》规定，证券基金经营机构委托信息技术服务机构提供服务的，应当对服务机构及其信息系统进行内部审查，并向证监会报送审查意见，选择前应制定更换服务方的流程和预案，确保特定情况下可及时更换。双方应签署服务协议、保密协议，对于协议内容《办法》也做了原则性的规定。

证券基金经营机构依法应当承担的责任不因委托外包而免除或减轻，其应当清晰、准确、完整的掌握重要信息系统的技术架构、业务逻辑和操作

流程等内容，确保重要信息系统运行始终处于自身控制范围。除法律法规及证监会另有规定外，不得将重要信息系统的运维、日常安全管理交由信息技术服务机构独立实施。

《征求意见稿》关于经营机构、专项业务服务机构应选择住所地在境内的信息技术服务机构的要求，《办法》也予以删除，而是对信息技术服务机构新增了无违法记录、股东及实际控制人无违法记录、安全稳定的技术服务能力、高效应急响应能力、熟悉证券基金业务等要求。

三、《办法》搭建了信息技术管理的新监管要求

1、 监管和指导机构

《办法》规定，中证信息技术服务有限责任公司在证监会指导下制定相关配套业务规则，协助开展信息技术相关备案、监测、检测和检查等工作。信息技术服务机构应自愿接受其业务指导、遵守相关业务规则。

2、 监督管理事项

除上述提及的委托信息服务机构的报送审查意见外，《办法》要求证券基金经营机构新建或更换重要信息系统所在机房、证券基金交易相关信息系统时，向证监会报送材料，并且向证监会报送年度信息技术管理专项报告；《办法》也要求信息技术服务机构定期向证监会报送材料，发生重大变化或存在明显缺陷、可能造成重大影响时，立即向证监会及其派出机构报告。

另，《办法》明确要求信息技术服务机构向证监会备案，并且只有符合相应要求的信息技术服务机构有资格向证券基金经营机构提供服务。

四、我们的观察

《办法》体现了在网络安全逐渐成为金融行业风险防范重要方面的趋势下，证监会对于证券基金经营机构的信息技术管理的监管思路，并旨在通过合规体系搭建要求、定期报告、事件报告、信息技术服务机构备案等多种方式结合，对信息技术活动进行全方位的监管。另外，《办法》也在细节上增加了对于数据管理、系统内部分区、最小授权管理原则等信息系统安全的要求，明确要求证券基金经营机构不得使用、购买来源不明的客户信息，均体现出网络安全和信息保护等方面通常的合规思路。

《办法》在具体适用范围、实践执行力度、以及如何与《网络安全法》相关规定衔接上（包括跨境传输的相关规定以及等级保护的相关规定），仍将有待在实践之中观察。

董　潇　合伙人　　电话：86 10 8519 1718　邮箱地址：dongx@junhe.com
袁　琼　律　师　　电话：86 10 8553 7663　邮箱地址：yuanq@junhe.com

JUNHE BULLETIN

JUNHE

January 4, 2019

Telecom and Internet Law

CSRC Issues Administrative Measures on Information Technology for Securities and Funds Business Operators

On December 19, 2018, the China Securities Regulatory Commission (CSRC) formally issued its *Administrative Measures on Information Technology of Securities and Fund Business Operators* ("Measures"), which include numerous amendments to its May 2017 consultation paper ("Consultation Paper").

The Measures have been issued against the backdrop of increasing regulation and supervision of information technology and cybersecurity following the promulgation of the Cybersecurity Law. They provide detailed requirements to guide securities and fund business operators in the construction of a comprehensive compliance system for their information technology, and clarify the underlying regulatory principles.

Below, we provide a brief overview of key aspects of the Measures and an analysis of the implications.

I. The Measures apply to key participants involved in the securities and fund sector

Chapter 1 of the Measures stipulates that the Measures apply to the following subjects:

(1) Securities and fund business operators, i.e., securities companies and securities fund management companies;

(2) Information technology service providers, i.e., institutions that provide development, testing, integration, assessment, operation, maintenance or day-to-day security management services for any of the important information technology systems for securities and fund business operators;

(3) Institutions providing special services to securities and fund businesses ("special servicing institutions");

(4) Commercial banks engaged in the deposit and custody of securities businesses' customer transaction settlement funds; fund custodians for publicly-raised funds; subsidiaries duly incorporated onshore by securities and fund management business operators; and any institutions established by such subsidiaries.

The scope of application of the Measures is relatively broad, and covers almost all information technology-related market participants involved in the securities and fund sector.

We note that Article 2 of the Consultation Paper specifically lists "special servicing institutions" as

being among the applicable subjects, and that Chapter 5 thereof details the provisions specifically applicable to these special servicing institutions. Unlike the Consultation Paper, the final version of the Measures removes the special provisions applicable to special servicing institutions from the main body and stipulates in the ancillary Chapter 7 that special servicing institutions for securities investment funds shall be governed by reference to the Measures. The definition of special servicing institutions has also been expanded to include fund servicing institutions engaging in investment advisory, rating and evaluation, and securities investment advisory institutions. While it appears that the final version of the Measures still includes special servicing institutions, it remains to be seen how such institutions will be governed in practice with reference to the Measures.

II. The Measures lay out the basic requirements for building comprehensive informational technology compliance systems for securities and fund business operators

1. Establish a tiered governance structure, comprising the board of directors, senior management team, information technology management committee, and chief information officer

The Measures explicitly require the board of directors of a securities and fund business operator to review and be responsible for the company's information technology management objectives, and for the senior management team to be responsible for the management and implementation of the board's information technology decisions.

An information technology management committee or designated special committee shall be established under the company's senior management team, with responsibility for formulating information technology strategies and reviewing the relevant matters. In addition to company's senior management officers and departmental heads, the information technology management committee may also engage external professionals to serve on or as consultants to the committee.

The Measures raise the responsibility for the effectiveness of the information technology compliance system beyond that of the Consultation Paper, to board level. In addition, for the first time, the Measures stipulate that securities and fund business operators shall designate a person that meets the requirements of the Measures as the chief information officer.

2. Establish comprehensive information technology compliance policies and schemes covering system security, data governance and emergency management

The Measures provide detailed provisions for three aspects of information technology security, namely, information system security, data governance and emergency management.

System Security. The Measures require securities and fund business operators to formulate special implementation plans for the launch of or material alteration to any important information technology system, or, if such system is not currently in use, to conduct an assessment of its impact, and to formulate a system outage and data migration and safekeeping plan. Securities and fund business operators shall continuously monitor the operation of all important information technology systems, identify any abnormal occurrences, and deal with them in a timely manner. All relevant documents shall be collected and stored so as to ensure that emergency response and auditing requirements are able to be met.

Data governance. The Measures impose new requirements on securities and fund business operators to classify any data obtained during business operations or from clients according to the data's significance and sensitivity, and to take appropriate data management arrangements accordingly. The Measures specifically emphasize that securities and fund business operators shall keep records of the usage of any data and client information, and continuously monitor their information technology service provider or other related parties to ensure they are performing their undertakings in relation to non-disclosure. If it is found that any information technology service provider has stored or used such data or information in violation of laws and regulations, the relevant securities and fund business operators shall order the information technology service provider to make the necessary corrections, and to destroy such data and information, and shall terminate the business relationship if such service provider refuses to cooperate and make corrections. The Measures also emphasize that securities and fund business operators shall not collect any irrelevant client information, shall not purchase or use data which are obtained illegally or from an unknown source, shall not intercept or store client information in violation of the law, and shall under no circumstances provide client information to any other institutions or individuals.

Emergency management. It is a requirement that emergency plans be formulated. There must be at least one test emergency exercise per year and the reports of such exercise shall be kept on record. The emergency plans shall be subject to ongoing review and improvement, and shall take into full consideration any event which might influence the stable operation of important information technology systems, such as the breakdown of such systems, an outsourced technology service provider's failure to provide services, significant staff alterations or natural disasters. Backup systems shall have the same processing capacity as the original system.

The Measures remove the requirement that the important information technology systems must be deployed within the territory of China, and that important data and client information collected and produced during the business operation shall be stored within the territory of China, as was originally proposed in the Consultation Paper. However, according to the Cybersecurity Law and other relevant laws, securities and fund business operators, being financial institutions, may be still required to store important data and client information collected and produced by any important information systems within the territory of China, and to conduct security assessments before transferring such information and data overseas.

3. Enhancing internal and external auditing to ensure continuous compliance

Chapters 3 and 4 of the Measures provide the detailed auditing requirements to guide securities and fund business operators in their information technology compliance, risk control and information security protection. These include requirements for internal auditing, periodic special auditing on information technology management (not less than once per year), entrusting professional institutions to conduct comprehensive auditing on information technology management (not less than once every three years), tracking and rectifying any problems in a timely manner, and safekeeping auditing reports for no less than twenty years.

4. Improving supervision of entrusted information services

The Measures stipulate that if a securities and fund business operator engages an external

information technology service provider to provide services, it shall conduct internal inspections on such servicing provider and its information system, and submit the relevant inspection reports to the CSRC. Before determining which external provider to engage, such securities and fund business operator shall formulate procedures and plans to quickly replace such external servicing provider should certain circumstances arise. A securities and fund business operator and a servicing provider should enter into both a service agreement and a non-disclosure agreement, with the Measures providing general, in principle requirements on the content of such agreements.

The obligations that securities and fund business operators assume in accordance with any laws will not be exempted or mitigated due to any entrustment or outsourcing. Securities and fund business operators are expected to clearly, precisely and completely understand the technological structures, business logic and operational procedures of their key information systems, and to ensure that the operation of these systems is always under their control. An information technology service provider shall not be entrusted to independently manage the operation, maintenance and day-to-day security of key information systems, unless the laws and regulations stipulate this or CSRC approval has been granted.

The Consultation Paper required that securities and fund business operators and special servicing institutions should use only those information technology service providers domiciled within the territory of China. The final version removes this requirement, but imposes new conditions on information technology service providers, such as requiring that a service provider, its shareholders and de facto controllers have no recorded violations of laws or regulations, that it has safe, stable technology servicing capacity, an effective emergency response capability, and familiarity with securities and funds businesses.

III. The Measures set out new regulatory requirements for information technology management

1. Regulatory and guiding institutions

The Measures stipulate that, under the guidance of the CSRC, the China Securities Information Technology Services Limited Company shall be responsible for formulating the relevant implementation rules to assist in the filing, monitoring, detection and inspection for information technology. Information technology service providers shall voluntarily accept the operational guidance of the same and comply with all relevant implementation rules.

2. Supervision and administration

As well as the above mentioned requirements, when engaging information technology service providers, the Measures require that relevant materials shall be submitted to the CSRC when a securities and fund business operator establishes or replaces the information system being used in trading of securities or funds, or changes the computer room where an important information system is located. Special information technology reports shall be submitted to the CSRC every year. The Measures also require that information technology service providers shall submit materials to the CSRC or its local agencies at regular intervals, and immediately inform the CSRC in the event of any significant change, any obvious defects or any other circumstances that might have a significant impact.

In addition, the Measures explicitly require that all information technology service providers shall be filed with the CSRC, and only those which meet the relevant requirements will be permitted to

provide services to the securities and fund business operators.

IV. Our Observations

Within an environment in which cybersecurity is becoming an increasingly important aspect of risk prevention in financial industries, the Measures provide insights into the CSRC's thinking on information technology within securities and fund operation institutions.

They aim to provide comprehensive supervision and regulation of all major dimensions of information technology activities through various means, including requirements relating to the set-up of compliance systems, periodic reports, reports for special events and filing of information technology service providers.

In addition, the Measures also provide detailed requirements for the security of information system, such as data management, system separation, and minimum authorization principles. They explicitly require that securities and fund business operators shall not use or purchase client information from unknown sources. In these respects, the Measures are consistent with the other approaches to compliance in the areas of cybersecurity and information protection.

It remains to be seen how the Measures will be applied in practice, the scope of their application, the intensity of their enforcement and how they will interact with the Cybersecurity Law, and in particular the latter's provisions regarding cross-border data transfer and multi-level protection system.

Marissa Dong	Partner	Tel: 86 10 8519 1718	E-mail:dongx@junhe.com
Lena Yuan	Associate	Tel: 86 10 8553 7663	E-mail:yuanq@junhe.com

.