# 证券期货业网络与信息安全保护
# ——谈《证券期货业网络和信息安全管理办法》的落实

作者：杨迅 | 夏雨薇

《证券期货业网络和信息安全管理办法》(**“《安全管理办法》”**)已于 2023 年 5 月 1 日生效，替代 2012 年通过的《证券期货业信息安全保障管理办法》(**“《保障管理办法》”**)，成为规证券期货业的网络和信息安全的主要法律文件。该《安全管理办法》在证券、基金、期货行业全面落实《网络安全法》、《数据安全法》、《个人信息保护法》以及《关键信息基础设施安全保护条例》下对网络、数据和个人信息的保护，对核心机构、经营机构、信息技术系统服务机构提出了更为全面的监管要求。

本文合证券期货业目前的监管态势、相应的法律法规要求，与《安全管理办法》的最新规定，对各经营机构的网络和信息安全重点合规义务进行梳理和总结。

## 正文：重点合规义务分析

### 一. 责任机构与专业人员

《安全管理办法》要求证券期货经营机构(“经营机构”)指定或设立专门的工作牵头部门以及双责任人：机构主要负责人为第一责任人，分管网络和信息安全工作的领导班子成员或高管为直接责任人。换言之，经营机构至少应当指派有信息技术专业能力的部门分管网络和信息安全工作，而其工作主要内容应当是组织、管理并落实《安全管理办法》下的各项合规义务。

证券期货业并非首个要求落实双责任人制度的行业。《工业和信息化领域数据安全管理办法(试行)》要求“*本单位法定代表人或者主要负责人是数据安全第一责任人，领导团队中分管数据安全的成员是直接责任人*”。可见，除了配置专业的责任人员外，机构主负责人必须在整体经营层面重视、了解网络和信息安全管理工作，接受监管的问责。

如您需要了解我们的出版物，
请联系：

Publication@llinkslaw.com

《安全管理办法》进一步要求从事网络和信息安全工作的工作人员具有与其职责相匹配的专业知识和职业技能。也就是说，经营机构在选聘相应网络和信息安全工作人员前应详细了解并审查其从业记录、经验与相应资质。必要时，应当对拟聘人员进行核查，并最好将相应工作记录和证明材料留档备查。

## 二. 数据安全与个人信息保护

在《保障管理办法》的基础上，《安全管理办法》新设专章规范投资者的个人信息保护。该章节在《个人信息保护法》的原则规定上，对经营机构提出了相应的落地要求。

《安全管理办法》一方面强调经营机构应当充分遵守《个人信息保护法》下的一些原则性规定，即保障投资者的撤回同意权、对外提供投资者个人信息时应当获得单独同意，另一方面也充分考虑到了经营机构的客户身份识别、反洗钱筛查、投资者的适当性管理等监管要求，对相应的个人信息处理义务进行明确——当处理个人信息是提供服务所必需的，或履行法定职责或义务所必需的，投资者拒绝提供相应的个人信息，经营机构可以拒绝向投资者提供服务。同时，如果对外提供个人信息是基于履行法定职责或法定义务的，经营机构也不必再次获得投资者的“单独同意”。

此外，《安全管理办法》要求经营机构在不可控区域、测试环境等高风险区域加强个人信息严格保护。例如，在经营机构网络安全防护边界以外处理投资者个人信息的，应采取数据脱敏、数据加密的安全措施。通过非自主运营渠道(短信、邮件)发送投资者敏感个人信息的，也应当对敏感个人信息进行脱敏处理。经营机构也可参考《个人金融信息保护技术规范》附录 A 与《金融数据安全 数据生命周期安全规范》附录 C，落实相应的信息屏蔽和脱敏技术。

最后，《安全管理办法》明确禁止强制用户进行生物信息识别验证。除非确有必要或法律要求的，经营机构不得将生物识别信息(人脸、步态、指纹、虹膜、声纹等)作为唯一的客户身份认证方式，而应当提供其他可选方式。不得强迫个人进行生物识别认证的要求，在长期以来的监管实践中，也有诸多处罚案例。因而，建议经常使用人脸识别验证技术对用户进行核验的金融类 App 在履行相应的人脸核验流程时向用户提供其他核验渠道。

## 三. 安全事件应急处置

《安全管理办法》在《证券基金经营机构信息技术管理办法》(“**《技术管理办法》**”)《证券期货业网络安全事件报告与调查处理办法》(“**《安全事件报告与调查处理办法》**”)的基础上对证券期货业的应急处置义务进行了归纳，规定应急处置主要分为以下几个环节：日常监测与漏洞排查、事前应急预案和应急演练、事中应急处置和报告以及事后调查。

### 1. 日常监测与漏洞排查

《安全管理办法》要求经营机构建立监测预警机制，持续监测信息系统和基础设施的运行状况。核心机构、经营机构和信息技术系统服务机构需及时加固、整改可能存在安全缺陷、安全漏洞的网络和信息安全产品或者服务。

### 2. 事前应急预案和应急演练

《安全管理办法》要求经营机构再制定应急预案后，定期开展应急演练并形成报告存档备查。《技术管理办法》还要求经营机构每年至少开展一次应急演练，并且两年内需要覆盖全部的重要信息系统。针对应急演练的情况和业务系统的变更情况，对应急预案进行持续性更新。

根据 2021 年更新的《技术管理办法》对应急管理的要求，经营机构应当在应急预案中明确：应急管理建设目标、备份信息系统建设和恢复机制、备份数据恢复机制、业务恢复或替代措施、应急联系方式、与客户沟通方式、向监管部门及有关单位的报告路径、应急预案披露与更新机制等内容。

应急预案应当充分考虑的应急事件包含如下:

- 网络安全事件;
- 自然灾害和公共卫生事件;
- 本机构网络和信息安全相关重大的人事变动(例如分管的高管、重要的网络和信息安全团队发生的变动)；以及
- 主要信息技术系统服务机构退出。

### 3. 事中应急处置和报告

一旦发生安全事件，经营机构应当根据《安全事件报告与调查处理办法》的要求，对发生的网络和信息安全事件进行分类并按要求向证监会以及相应的其他有关机关(例如公安机关)上报。如果相应的网络和信息安全事件构成数据安全事件[1]、个人信息安全事件[2]的，还需要根据《数据安全法》《个人信息保护法》的要求，向网信办等相关监管部门报告安全事件。

《安全管理办法》在重申报告义务以外，也从个人信息保护的角度新增安全事件的通知义务。如果网络和信息安全事件对投资者造成影响时，经营机构需要通过有效渠道(官方网站、客户交

[1] 《数据安全法》第 29 条 开展数据处理活动应当加强风险监测，发现数据安全缺陷、漏洞等风险时，应当立即采取补救措施；发生数据安全事件时，应当立即采取处置措施，按照规定及时告知用户并向有关主管部门报告。

[2] 《个人信息保护法》第 57 条 发生或者可能发生个人信息泄露、篡改、丢失的，个人信息处理者应当立即采取补救措施，并通知履行个人信息保护职责的部门和个人。通知应当包括下列事项：
(一)发生或者可能发生个人信息泄露、篡改、丢失的信息种类、原因和可能造成的危害；
(二)个人信息处理者采取的补救措施和个人可以采取的减轻危害的措施；
(三)个人信息处理者的联系方式。
个人信息处理者采取措施能够有效避免信息泄露、篡改、丢失造成危害的，个人信息处理者可以不通知个人；履行个人信息保护职责的部门认为可能造成危害的，有权要求个人信息处理者通知个人。

易终端、电话或者邮件)进行风险提示、告知必要措施。该要求是对《个人信息保护法》第 57 条的通知义务在证券期货业落地的细化，旨在保障投资者个人信息相关的知情权。

**4. 事后调查**

在应急处置结束且系统恢复正常运行后，经营机构还需要根据《报告和调查处理办法》[3]的时限要求向证监会及其派出机构提供事件总结报告。

## 四. CIIO 监管

在《关键信息基础设施保护条例》的基础上，《安全管理办法》也进一步细化了对 CIIO 的要求。

| | 新增义务 |
|---|---|
| **管理责任人要求** | - 将关键信息基础设施安全保护情况纳入网络安全第一责任人、直接责任人和相关人员的责任考核机制;<br>- 为每个关键信息基础设施指定一名网络和信息安全管理责任人，并明确岗位职责和分工。 |
| **安全检测和风险评估要求** | - 将新建承建关键业务的重要网络设施、信息系统的，纳入安全检测和风险评估的项目中;<br>- 每年至少进行一次整体的安全检测和风险评估;<br>- 包括 CII 运行情况、面临的主要威胁、风险管理情况、应急处置情况。 |
| **专项评审要求** | - CII 运行变更或者下线移除，可能产生较大影响的，应开展专项评审；未通过评审的，原则上不得实施运行变更或下限移除。 |
| **CII 性能要求** | 对关键信息基础设施的安全运行进行持续监测，定期开展压力测试，确保系统性能容量在历史峰值的三倍以上，交易时段相关网络带宽应当在近一年使用峰值的两倍以上。 |
| **灾备要求** | 建设同城和异地灾难备份中心，实现数据同步保存。 |
| **报送网络和信息安全管理年报** | - 网络和信息安全管理年报中应当囊括网络和信息安全检测和风险评估情况;<br>- 在报送网络和信息安全管理年报时，CII 安全保护年度计划必须单独报送。 |
| **其他要求** | 与《关键信息基础设施安全保护条例》要求相同，包括但不限于建立专门安全管理机构并任命相关岗位；对关键岗位人员进行背调；采购网络产品或服务时，根据法律要求申报网络安全审查等。 |

[3] 核心机构和经营机构应当在网络安全事件应急处置结束、系统恢复正常运行后 7 个工作日内，组织内部调查，准确查清事件经过、原因和损失，查明事件性质，认定并追究事件责任，提出整改措施，并进行事件总结报告。事件总结报告内容应当包括：
(一)事件基本情况，包括事件发生时间、地点、经过、影响范围、影响程度、损失情况等；
(二)应急处置情况，包括事件报告的情况、采取的措施及效果；
(三)事件调查情况，包括事件原因、事件级别、责任认定和结论；
(四)事件处理情况，包括事件暴露出的问题及采取的整改措施，责任追究情况。
暂时无法确定事件原因、责任和结论的，应当提交事件的初步分析报告，同时尽快查找原因，认定并追究事件责任，采取整改措施，并在事件应急处置结束、系统恢复正常运行后 30 个工作日内提交事件补充报告。

## 五. 供应商管理

《安全管理办法》进一步提出了对供应商的要求，特别是细化了信息技术系统服务机构的服务与产品有关的义务。在原有的供应商管理的要求上，经营机构应当与供应商签订合同，约定双方的网络和信息安全的权利与义务。如供应商提供的服务或产品引发网络安全事件的，有义务配合监管机关进行原因查明和责任认定。

此外，《安全管理办法》进一步要求，在信息技术系统服务机构的备案要求下，经营机构应当督促相关的信息技术系统服务机构依法履行备案。也就是说，除了根据《技术管理办法》对信息技术系统服务机构进行内部审查外，经营机构还需要对信息技术系统服务机构的备案情况进行核查并履行督促义务。

## 六. 报送、报告、备案、备查等监管义务

《安全管理办法》规定了一系列报送、报告、备案、备查等监管义务，摘要如下:

| | 义务主体 | 监管机关 | 内容 |
|---|---|---|---|
| **报告、报送义务** | | | |
| **1.** | 核心机构和经营机构 | 中国证监会及其派出机构 | 报送等保工作的开展情况。 |
| **2.** | 核心机构和经营机构 | 中国证监会及其派出机构 | 重要系统新建上线、运行变更、下线移除，经评估认为可能对证券期货市场安全平稳运行产生较大影响，应当提前报告。 |
| **3.** | 核心机构和经营机构 | 中国证监会及其派出机构 | 报告本机构和本机构运营平台上的信息发布违法情况。 |
| **4.** | 核心机构、经营机构和信息技术服务机构 | 中国证监会及其派出机构 | 网络安全产品或者服务存在安全缺陷、安全漏洞等风险隐患，且可能对证券期货业网络安全产生较大影响的。 |
| **5.** | 核心机构 | 中国证监会 | 网络安全应急演练后的 15 个工作日内报告应急演练情况。 |
| **6.** | 核心机构和经营机构 | 向中国证监会及其派出机构 | 发生网络安全事件时根据要求上报。 |
| **7.** | 核心机构和经营机构 | 中国证监会及其派出机构 | 对网络安全事件进行调查处理并报告调查结果。 |
| **8.** | 核心机构和经营机构 | 中国证监会及其派出机构 | 每年 4 月 30 日前，完成上一年度的网络和信息工作的专项评估报告，编制网络和信息安全管理年报并报送。 |
| **9.** | CIIO | 中国证监会及其派出机构 | CII 停止运营或者发生较大变化，可能影响认定结果的。 |

| | | | |
|---|---|---|---|
| **10.** | CIIO | 网络安全审查办公室 | 采购网络产品和服务可能影响国家安全的，应当申报网络安全审查。 |
| **11.** | CIIO | 中国证监会及其派出机构 | 每年 4 月 30 日前，完成上一年度的网络和信息工作的专项评估报告，编制网络和信息安全管理年报并报送，单独报送关键信息基础设施安全保护年度计划。 |
| **备案义务** | | | |
| **12.** | 信息技术服务机构 | 中国证监会备案 | 供应商为核心机构和经营机构提供重要信息系统相关产品或者服务的，应当依法作为信息技术系统服务机构备案。 |
| **备查义务** | | | |
| **13.** | 核心机构和经营机构 | / | 每年开展重要信息系统压力测试后对报告留档备查，并保存五年以上。 |
| **14.** | 核心机构和经营机构 | / | 对网络安全应急演练报告留档备查。 |
| **通知义务** | | | |
| **15.** | 核心机构和经营机构 | 受影响的投资者 | 发生网络安全事件对投资者造成影响的，应告知替代方式、应急措施，提示受影响的个人防范、应对可能的风险。 |
| **16.** | 核心机构和经营机构 | 全体投资者 | 终止借助网络向投资者提供服务的，应当提前选取公告、定向通知等方式告知投资者相关业务影响情况、替代方式及应对措施。 |

## 七. 法律后果

《安全管理办法》对于违反网络和信息安全义务的处罚措施，与证监会在其他法律文件中的规定基本一致。经营机构和信息技术系统服务机构如违反《安全管理办法》，可能面临"*责令改正*、*监管谈话*、*出具警示函*、*责令公开说明*、*责令定期报告*、*责令增加内部合规检查次数*"等的监管措施。

此外，一旦证监会发现经营机构内部整理混乱、内控失效或不符合持续性经营规则的，监管机构有权责令经营机构暂停借助网络开展部分或全部业务。进一步地，如相关机构存在违反《网络安全法》《关键信息基础设施安全保护条例》《个人信息保护法》等法律法规的行为时，证监会及其派出机构亦有权根据相应的法律法规进行处罚。

## 总结

《安全管理办法》的实施，实际上是对目前证券期货业与通用行业的现行的网络和信息安全框架的有机结合与落地实践，《安全管理办法》下的大部分的网络和信息安全保护义务并非首创，而是在既有的网络安全和数据保护规定在证券基金行业体系化、具体化的呈现；这样的呈现，也更有利于经营机构进行自纠自查，保证机构内网络和信息安全管理工作的正常运行，维护市场稳定，保障投资者的权益。

## 附表

## 概述: 重点合规义务指引

| | 重点合规要求 | 重点内容提示 |
|---|---|---|
| 1. | 建设网络和信息管理制度体系 | - 对各项合规要求进行制度化;<br>- 确保内部的决策、管理、执行和监督机制。 |
| 2. | 责任机构与负责人 | - 确定第一责任人和直接责任人;<br>- 指定或设立网络和信息安全工作牵头部门或机构;<br>- 任命有专业知识和技能的专业人员。 |
| 3. | 完善网络和信息安全应急处置 | - 建立监测预警机制;<br>- 建立应急预案, 进行应急演练;<br>- 及时上报安全事件并进行必要通知;<br>- 及时进行事后调查。 |
| 4. | 加强网络和信息安全安全措施 | - 保证信息系统的安全性、与信息化工作同步规划、建设、使用;<br>- 新建上线、运行变更、下线移除重要信息系统时进行充分评估并制定相应的保护方案、制定测试方案;<br>- 妥善保存网络日志;<br>- 建立网络和信息安全防护体系;<br>- 建立本地、同城和异地备份与恢复机制;<br>- 定期进行重要系统压力测试;<br>- 加强自主研发能力;<br>- 尊重并保护知识产权。 |
| 5. | 供应商管理 | - 建立供应商准入与管理体系;<br>- 明确双方的网络和信息安全权利义务;<br>- 建立与供应商相关的应急处置机制;<br>- 督促信息技术系统服务机构履行备案义务。 |
| 6. | 加强数据安全与个人信息保护 | - 根据《个人信息保护法》等要求处理个人信息;<br>- 加强数据/个人信息在风险区域使用的管控;<br>- 限制生物识别信息的过度使用。 |
| 7. | 加强关键信息基础设施(“**CII**”)保护 | - 根据《关键信息基础设施安全保护条例》对 CII 进行保护;<br>- 对相关工作人员进行责任考核、背景审查;<br>- 定期进行网络和信息安全监测和风险评估;<br>- 进行重要设施的变更和下线的专家评审;<br>- 进行专项评估, 编制网络和信息安全管理年报并报送;<br>- 定期开展 CII 压力测试;<br>- 建设同城和异地灾备中心。 |
| 8. | 履行报送、报告、备案等监管义务 | 请见本文下表之汇总。 |
| 9. | 网络信息安全教育与人才培养 | |

如您希望就相关问题进一步交流，请联系：

杨 迅
+86 21 3135 8799
xun.yang@llinkslaw.com

如您希望就其他问题进一步交流或有其他业务咨询需求，请随时与我们联系：**master@llinkslaw.com**


| 上海 | 北京 | 深圳 |
| --- | --- | --- |
| 上海市银城中路 68 号<br>时代金融中心 19 楼<br>T: +86 21 3135 8666<br>F: +86 21 3135 8600 | 北京市朝阳区光华东里 8 号<br>中海广场中楼 30 层<br>T: +86 10 5081 3888<br>F: +86 10 5081 3866 | 深圳市南山区科苑南路 2666 号<br>中国华润大厦 18 楼<br>T: +86 755 3391 7666<br>F: +86 755 3391 7668 |
| 香港 | 伦敦 | |
| 香港中环遮打道 18 号<br>历山大厦 32 楼 3201 室<br>T: +852 2592 1978<br>F: +852 2868 0883 | 1/F, 3 More London Riverside<br>London SE1 2RE<br>T: +44 (0)20 3283 4337<br>D: +44 (0)20 3283 4323 | |


**www.llinkslaw.com**

**Wechat: LlinksLaw**

**本土化资源 国际化视野**