中国证券期货业信息安全工作规划

证券期货业信息化工作领导小组办公室

2014 年 11 月

期货业信息安全工作规划

目　录

前　言

证券期货业是一个高度依赖信息技术的行业，证券期货业信息系统的建设与安全运行，不仅关系到证券期货市场的稳定和健康发展，还关系到国家金融安全和社会稳定，对于保护投资者的合法权益也具有十分重要的意义。

近年来，随着移动互联、云计算、大数据等新兴技术的蓬勃兴起，层出不穷的创新业务，在商业模式应用、技术风险控制等方面对金融业造成了巨大的冲击，对金融监管部门的监管模式也形成了挑战。证券期货业在当前的互联网金融浪潮中，信息系统建设与安全运行的压力越来越大，所面临的信息安全形势日趋复杂。

在这种形势下，为确保证券期货业信息系统的安全可靠运行，加强信息技术对业务创新的支持，更好地保障证券期货业市场未来发展，中国证监会根据人民银行《金融业网络安全规划（2015-2020 ）》的总体要求，紧密结合《资本市

场信息化建设总体规划（2014-2020 ）》，组织制定《中国证券期货业信息安全工作规划》。

本规划阐述了如何构建新形势下的信息技术监管体系，做好信息安全基础建设和保障，有效应对新技术与新业务应用带来的新挑战，以更好地应对复杂多变的信息安全形势，全面、系统地解决行业信息安全工作中的突出问题，明确了今后一个时期的工作任务。规划期为 2015 年至 2020 年。

第一章 总体战略

第一节 指导思想和规划目标

（一）指导思想。贯彻落实党中央“加强金融基础设施建设，保障金融市场安全高效运行和整体稳定”的要求，紧密围绕“确保资本市场平稳安全运行、有序健康发展”这个核心，密切结合行业信息化工作，推进落实《资本市场信息化建设总体规划(2014-2020）》和《金融业网络安全规划（2015-2020 ）》，加强证券期货业信息安全基础设施建设，稳步提升证券期货业信息安全保障水平，为监管转型、业务发展提供有力支撑，切实保护投资者权益。

（二）规划目标。建立责任明确、保障有力的证券期货业信息安全治理体系，健全信息技术治理机制，提升信息安全地位，突出顶层设计能力；加强行业信息安全公共基础设施建设，促进资源整合和安全服务共享，提升信息安全风险管理水平；大幅提高信息系统风险防范能力和重大网络攻击抵御能力；健全行业信息安全监管体系，提升监管效能，形

成适应资本市场发展的监管机制；提升信息技术安全可控水平，增强应急响应能力，保障行业信息系统的安全稳定运行。

第二节 基本原则

信息安全工作坚持“稳定可靠、促进发展、安全可控、协作共赢”的原则。

（一）稳定可靠。以确保信息系统稳定运行为前提，加强行业公共基础设施、信息安全与应急管理体系建设，提高测试开发与运行维护管理能力，促进资本市场健康有序、高效和可持续发展。

（二）促进发展。结合新形势下业务和技术发展趋势，从战略高度把握信息安全发展方向，增强信息安全工作的前瞻性与执行力，促进信息安全工作持续改进，有效防范信息安全风险。

（三）安全可控。建立安全可控的信息技术长效机制，在安全可控的前提下，鼓励自主创新和行业协作，逐步提升信息安全保障水平。

（四）协作共赢。坚持行业协作互助原则，促进资源整合与共享，探索建立信息安全服务和信息技术产品行业联盟，实现合作共赢，增进共同利益。

第二章 规划任务

图：规划任务总体框架

第三节 健全信息技术治理机制，深入开展信息技术治理工作

积极推动行业机构加强信息技术治理工作，完善信息技术治理架构，健全信息技术决策与责任担当机制，在信息技术战略规划、支持业务创新、需求管理、价值管理、风险管

理等方面进行科学决策。引导行业机构逐步建立和完善信息技术治理跨部门协调机制，促进信息技术与业务融合。加强信息技术风险控制，制定和完善信息技术内控制度与流程。优化信息技术基础架构、数据架构、应用架构、安全架构，提高信息技术系统的可用性、灵活性和可扩展性，以满足业务高速发展的需要。

（一）提升行业机构管理层对信息技术价值的认识。在行业高管培训工作中，增加信息技术治理相关内容，促进行业机构管理层充分认识信息技术在业务发展与创新中的重要作用。

（二）建立首席信息官制度。推动行业机构设立首席信息官，促进行业机构建立和完善信息技术决策机制与职责担当机制。

（三）开展信息技术审计工作。贯彻落实《证券期货业信息系统审计规范》，大力推进行业信息技术审计工作，加强信息技术审计队伍建设，增强信息技术审计的专业性和独立性。

（四）推行技术架构革新。引导行业机构研究设计符合自身特点的信息技术新架构，逐步建立行业共享的基础架构库，为提升行业自主开发能力奠定基础。

（五）优化资金投入与人员结构。行业机构应优化信息技术投入结构，增加软件研发和信息安全建设的资金投入占比；优化信息技术队伍结构，提高业务分析、架构设计、软件研发和信息安全的人员比例，建立健全专业人才培养与引进机制。

第四节 完善信息安全管理体系，增强信息系统建设与运行安全

引导行业机构完善信息安全管理体系，推动行业机构在信息系统建设和运行等环节深入加强安全管理，规范软件开发过程管理，确保信息安全管理体系的全覆盖。推动行业机构加强信息系统运维团队建设，提升运维精细化管理水平。督促行业机构持续提升业务连续性水平，深入落实管理责任制，加强组织保障，优化业务连续性管理制度及决策机制，持续提升业务保障能力。

安全管理标准与规范，编写安全开发测试指南，提供软件开发最佳实践；建立行业共享的安全架构库和安全模块库，为提升行业整体开发安全水平奠定基础。

（七）建立行业软件开发与安全测试基础设施。积极落实《资本市场信息化建设总体规划（2014-2020 ）》，推进建立行业集中研发测试中心与信息安全实验室，鼓励行业机构依据相关标准开展测试评估工作；鼓励交易所等核心机构发挥技术优势，协助行业提高信息安全整体水平。

（八）加强人才培养与团队建设。引导行业机构加强信息技术研发、信息系统运维、信息安全专家团队建设，建立行之有效的人才培养与激励机制，形成“吸引人才、培养人才、留住人才”的良好氛围。

（九）推进信息系统运维精细化管理。引导行业机构结合本单位信息系统运维实际情况，优化完善运维制度及流程，加强自动化运维工具的应用与完善，持续提高运维精细化管理水平；组织建立行业运维操作规范与知识经验库，促

与应用。

引导行业机构正确认识业务连续性的重要性，促进行业机构不断完善业务连续性计划；通过持续演练，确保业务连续性计划的有效性；逐步建立行业信息系统应急知识库，规范信息系统应急手段与措施，稳步提升行业应急标准化水平；协调推动行业机构加强与通信、电力、银行等相关单位的沟通与配合，签订应急处理及服务协议。

（十一）推进托管设施及数据备份中心建设。积极落实《资本市场信息化建设总体规划（2014-2020 ）》，推进行业公共托管设施、行业数据备份中心建设，降低行业机构运行成本；推动制定《证券期货业数据集中备份管理办法》及相关标准，规范工作流程，确保重大灾难等极端情况下市场重要数据安全可用。

提高安全风险防控能力，加强重点领域信息安全管理

重点关注领域的风险控制能力，提升行业整体信息安全防护水平。推动行业机构信息安全意识教育和安全技能培训，提高信息安全管理的专业化程度与安全防范意识。加强以数据安全为核心的防护体系建设，提升行业机构对重大网络攻击的响应和处置能力。制定行业信息技术供应商管理规范，建立行业供应商跟踪评价机制，提高行业对供应商的安全管控水平。

加强行业信息安全培训，督促行业机构明确岗位安全职责，开展安全意识教育，提高从业人员的安全防范意识。

（十三）增强敏感数据保护能力。研究建立行业数据安全管理规范，制定行业敏感数据分类分级参考标准；推动行业机构深入开展数据安全保护工作，明确数据保护责任主

极推进国产密码算法在行业的应用。

深入开展科研攻关、专业队伍建设、跨部门横向合作等工作，研究重大网络攻击的防御方案，积极推动行业信息安全实验室的建设；引导行业机构改变传统网络边界防护的防御思路，整合各类安全技术手段，建立多层次逐级防护体系，加强辅助系统及关联系统等薄弱环节的安全防护与监测，增强重大网络攻击事件的发现、分析、决策和处置能力。

（十五）建立供应商管理和评价体系。制定行业信息技术供应商管理规范，提高重点领域外包服务的安全管控能力；制定行业供应商评价和披露制度，建立供应商产品质量评估与风险预警通报机制，及时发现并防范风险；积极协调供应商开放信息系统接口，并加快制定相关标准，打破技术壁垒，构建良性竞争环境。

息技术安全可控能力建设。加快行业集中研发测试中心等基础设施建设，鼓励科技自主创新，推动设立专项科研基金。加强信息技术人才队伍建设，强化信息技术外包管理，提高重点领域、关键环节的安全控制能力，增加信息技术产品可知、可信与可控度，保障资本市场安全稳定运行。

以国家网络安全审查相关政策为依据，出台与行业信息安全需求相适应的配套政策，制定行业信息安全审查标准，借助行业集中研发测试中心与信息安全实验室的力量，加强行业专用信息技术、产品和服务的安全审查和检测。

（十七）组建行业开源联盟，鼓励科技自主创新。积极整合行业机构开发团队资源，引导组建行业开源联盟，推动设立专项科研基金，建立科技创新奖励机制，对行业信息化及信息安全重点难点问题进行深入研究，加大对符合行业信息技术发展方向、能够形成自主知识产权的科技攻关项目的

重点关注开源信息技术产品的测试、评估和研究，积极鼓励利用开源技术开展自主创新，逐步探索形成以开源技术产品为主流的行业安全可控整体解决方案；构建行业信息技术创新示范交流平台，建立相应知识、经验库，促进科技创新成果共享。

鼓励行业机构培养与引进高端信息技术人才，加强系统架构顶层设计，提高核心系统自主研发、自主运维能力，持续完善信息技术外包管理，稳步实现网络基础设施、关键应用软件、安全防护系统等重点领域的安全可控。

（十九）推进国产化信息技术产品应用。鼓励交易所等核心机构先行推广国产化信息技术产品应用；推动行业机构采取“先外围后核心、先分支后总部”的策略，稳步扩大国产化信息技术产品的应用范围，提高国产化信息技术产品的应用比例，降低对国外信息技术产品的依赖。

第七节 研究新技术新应用安全风险，积极应对新形势新挑战

云计算、大数据、移动终端等新技术所带来的行业信息技术应用更新和技术场景变化，对信息安全提出了新的挑战。程序化交易、国际化、互联网金融等业务模式创新，要求信息安全适应业务发展的需求，以保障资本市场的健康稳定和可持续发展。

引导行业机构深入研究新技术和新业务模式，建立有针对性的安全保障机制，在合理利用新技术提高业务能力和管理能力的同时，结合新技术的特点制定相应的风险防范措施，以防范新技术应用衍生风险，保持信息系统的安全服务等级和风险应对水平。

（二十）加强移动终端应用安全管理。制定行业移动终端应用软件开发、测试、应用等技术标准和安全管理标准；通过行业信息安全基础服务机构与第三方监测机构的合作，及时发现假冒、篡改的移动终端应用，逐步探索建立移动终

端应用安全性监测、预警体系，以有效防范移动终端应用软件被恶意篡改。

（二十一）加强云技术、云服务应用指导。建立行业云技术安全应用评价体系，出台行业云技术应用安全规范；加强对公有云服务应用的安全管理，防范来自云服务提供商的安全风险；鼓励行业内有实力的机构建立社区云，为中小机构提供云服务。

（二十二）加强大数据平台安全防护。引导行业机构加强大数据平台的安全防护，积极研究制定并落实防护措施，加大数据跨地域、跨行业流动管理，强化数据安全访问控制，提高数据保护能力。

（二十三）制定程序化交易技术标准，控制程序化交易风险。制定行业程序化交易技术标准和安全管理策略，引导行业机构加强程序化交易管理，有效防范程序化交易风险。

（二十四）研究市场国际化信息安全风险，提高风险应对能力。积极开展市场国际化风险的专题研究，推动国际化

相关安全技术研究，保障市场国际化业务往来中的数据安全，制订风险应对方案，全面提高安全风险应对能力。

（二十五）加强互联网金融技术监管，防范互联网金融安全风险。研究互联网金融技术监管模式，构建新形势下的监管体系，明确各方职责。督促行业机构完善面向互联网开放系统的安全防护措施，提升安全技术保障能力。

第八节 完善信息安全监管体系，建立适应市场化需求的监管机制

在新的历史时期，要保持清醒的认识和判断，不断更新观念，实现监管模式从单一性、强制性、封闭性向多样性、协商性、开放性的转变；转变监管理念，充分利用市场化的手段，对市场经营机构实行市场化管理，做到事前引导，事后监管；大力推进落实《资本市场信息化建设总体规划（2014-2020 ）》，加强行业网络与安全建设；深入贯彻落实《中国证监会行业信息化与信息安全工作制度》，加强行业监管队伍的建设，形成监管合力，建立系统性、规范性、前瞻性的监管体系，实现深入化、精细化监管；加强横向合作，