证券期货业信息安全标准规划
（2023-2025）

全国金融标准化技术委员会证券分技术委员会

参与人员名单

规划起草单位：

中国证监会科技监管局、国泰君安证券股份有限公司、上海证券交易所、深圳证券交易所、大连商品交易所、中证信息技术服务有限责任公司、杭州安恒信息技术股份有限公司、上海市信息安全测评认证中心、兴业证券股份有限公司、长江证券股份有限公司、海通证券股份有限公司、华泰期货有限公司、天融信科技集团股份有限公司、奇安信科技集团股份有限公司、杭州默安科技有限公司、北京梆梆安全科技有限公司、南京大学、北京邮电大学

规划起草人员：

姚前、蒋东兴、俞枫、周云晖、陈炜、路一、周亚超、李宏达、倪惠康、陈凯晖、袁明坤、周桉、徐明、裘岱、黄清华、肖昱、王玥、潘进、王征宇、胡卫宁、李雪莹、吴云坤、沈锡镛、董振兴、仲盛、高志鹏

目 录

1　总体目标

为适应证券期货业业务创新与发展，降低行业整体信息安全风险与成本，有效规范行业信息安全标准的制定与应用工作，进一步提高和完善行业信息安全标准化水平，保障行业数字化转型发展，以《证券期货业科技发展“十四五”规划》《金融标准化“十四五”发展规划》为指导，根据《网络安全法》《数据安全法》《个人信息保护法》《关键信息基础安全保护条例》等法律法规要求，特制定《证券期货业信息安全标准规划（2023-2025）》（以下简称“本规划”）。

基于《证券期货业系统安全标准规划（2020-2022）》《证券期货业数据安全标准规划（2020-2022）》制定的思路和方法，结合我国网络安全政策法规和证券期货行业发展现状及标准化工作需求，本规划进一步完善了证券期货业信息安全标准体系，为行业机构信息安全管理提供指引，指导行业机构建立健全系统性信息安全架构与制度，加强数据全生命周期安全管理和技术防护，对证券期货行业信息系统的建设运维、检测评估、数据安全、行业监督管理、行业关键信息基础设施保护等提供基础性支持。本规划提出了 2023 至 2025 年证券期货业信息安全标准的整体规划，作为证券期货业信息安全标准化工作的重要依据。

根据证券期货行业的业务发展及标准化需求，组织制定信息安全领域优先级较高的国家标准或行业标准项目，持续跟踪国内外及行业信息安全工作动态，根据工作任务紧迫性和相互依赖性等因素及时调整工作计划，以满足行业高速、安全且高效兼容的信息安全标准化建设需求。

2　总体要求

本规划遵从网络安全相关法律法规和标准规范要求，适用于指导证券期货业信息安全领域的标准制定、修订与应用工作。

在行业信息安全标准制定过程中，各标准相关立项、牵头、参与单位应充分理解本规划，参照本规划制定的工作方案、标准体系以及目前行业标准化实际情况，有计划地推进标准的研制工作。

在行业信息安全标准应用过程中，证券期货行业相关机构应结合目前行业标准化现状及标准实际应用情况，选择合适的标准工作路线，按照本规划提出的标准应用建议，全面系统地推进标准应用工作。

3　基本原则

3.1 建立统一的风险管理思想

从风险管理、风险评估的视角检验相关信息安全标准体系是工作组的指导方针之一，标准体系本身以及标准本身均应体现风险评估的思想，引入安全控制模型，为行业提供更全面、更有效的风险信息。

3.2 优先关注行业高风险点

在信息安全标准体系的制定过程中，不仅需要从风险评估角度出发，还需结合证券期货行业的信息安全特点，充分发掘本行业与其他行业风险的差异，并加以分析，总结行业应用较集中的高风险点，以此作为信息安全标准体系设计方案的理论依据和着手点。

3.3 关注行业应用及新技术

把握证券期货业的相关特性，优先保证行业内应用系统的信息安全。新兴技术的引入往往带来新的风险点，应着重考虑目前已采用或即将大规模采用的新技术对证券期货行业所带来的影响，优先制定信息安全统一规范。

3.4 问题导向与整体布局并重

坚持问题导向，紧紧围绕证券期货行业信息安全的政策要求、重点工作、技术应用的急需事项，加快关键技术、产业亟需标准的研究和制定工作。积极借鉴和应用先进的理念、方法和技术，整体推进证券期货行业信息安全标准与其他信息安全标准、其他信息化标准、其他数据安全标准之间的协调统一。前瞻性考虑标准的实用性、应用成本和应用范围等因素，分步实施，持续优化，推动行业发展与信息安全均衡发展。

3.5 创新发展与注重实效相结合

坚持用创新发展的眼光来规划和开展信息安全标准化工作，让标准保持鲜活的生命力。以标准在证券期货业的应用效果作为研制标准的出发点和落脚点，切实提高标准质量，提升标准实施应用效果。

4 规划设计方法

基于风险评估的思想和模型，优先关注行业高风险点，突出行业应用和新技术，按照以下总体方法和步骤进行规划。

4.1 思想模型

参考风险评估的思想和模型，以风险为核心梳理信息安全标准建设需求，主要包括：

1) 依据 GB/T 20984-2022《信息安全技术 信息安全风险评估方法》，有机统一技术风险的识别与业务风险的评估，从而满足对信息系统安全风险评估不同层次的要求，将风险分析从技术风险上升到业务风险的高度。
2) 依据信息安全风险管理体系，信息系统生命周期的任何一个阶段，为了达到其信息安全目标，都需要相应的信息安全风险管理。
3) 从具体标准体系的构建角度，参考并融合典型的、公认的安全控制模型 PPDRR。PPDRR 模型包括策略（Policy）、防护（Protection）、检测（Detection）、响应（Response）和恢复（Recovery）5 个主要部分。防护、检测、响应和恢复构成一个完整的、动态的安全循环，在安全策略的指导下共同实现安全保障。PPDRR 模型是一种动态的、自适应的安全控制模型，在不断变化的安全风险和安全需求中，持续为企业提供安全保障。

4.2 标准现状分析

4.2.1 现行信息安全标准与政策

自上而下，调研行业现状，统计和分析证券期货行业现行的信息安全标准和相关政策，得出证券期货业现行信息安全标准见表1，证券期货业信息安全的相关政策见表2。

表 1 证券期货业现行信息安全标准

序号	标准编号	标准名称	标准范围
1	JR/T 0112-2014	证券期货业信息系统审计规范	规定了证券期货业信息系统审计工作的要求。
2	JR/T 0146-2016（所有部分）	证券期货业信息系统审计指南 第 1 部分：证券交易所 第 2 部分：期货交易所 第 3 部分：中国证券登记结算公司 第 4 部分：其他核心机构 第 5 部分：证券公司 第 6 部分：基金管理公司 第 7 部分：期货公司	为证券期货行业内信息系统的安全审计工作提供指南。
3	JR/T 0158-2018	证券期货业数据分类分级指引	给出了证券期货业数据分类分级方法概述及数据分类分级方法的具体描述，并就数据分类分级中的关键问题处理给出建议。 适用于证券期货行业机构、相关专项业务服务机构、相关信息技术服务机构开展数据分类分级工作时使用。
4	JR/T 0191-2020	证券期货业软件测试指南 软件安全测试	给出了证券期货行业信息系统建设过程中的软件安全测试目标及流程、软件安全测试技术、软件安全测试基本测试方法及移动应用安全测试特定测试方法。 适用于指导证券期货行业市场核心机构、证券期货基金经营机构以及证券期货信息技术服务机构实施证券期货业计算机软件和外部信息系统的安全测试。
5	JR/T 0192-2020	证券期货业移动互联网应用程序安全规范	规定了证券期货业移动互联网应用程序的移动终端安全、身份鉴别、网络通信安全、数据安全、开发安全和安全审计。 适用于证券期货业机构开发和发布移动互联网应用程序。
6	JR/T 0060-2021	证券期货业网络安全等级保护基本要求	规定了证券期货业网络安全等级保护的总体要求，以及第一级到第四级等级保护对象的安全通用要求和安全扩展要求。 适用于证券期货业分等级的非涉密对象的安全建设和监督管理。

序号	标准编号	标准名称	标准范围
7	JR/T 0250-2022	证券期货业数据安全管理与保护指引	描述了证券期货业数据安全管理与保护相关的术语和定义、基本原则、组织架构、制度，以及各级数据关于数据采集、数据展现、数据传输、数据处理、数据存储的数据安全管理与保护的思路和方法。 适用于证券期货业机构开展数据安全管理与保护工作的参考和指引。
8	JR/T 0273-2023	证券期货业信息系统渗透测试指南	为证券期货业提供一套通用的信息系统渗透测试框架，深化渗透测试对于行业信息系统的作用，更加规范、安全、稳定地开展渗透测试工作，提升证券期货行业信息系统的渗透测试能力，保障渗透测试质量，控制渗透测试实施风险，进一步保障行业信息系统的安全性。

表 2 证券期货行业信息安全相关政策

序号	名称	描述	发布单位	执行日期	备注
1	期货公司网上期货信息系统技术指引	保障期货公司网上期货业务系统的安全运行，促进期货业务健康发展，保护投资者的合法权益。	中国期货业协会	2009 年 6 月 23 日	
2	网上基金销售信息系统技术指引	保障网上基金销售信息系统的安全、可靠、高效运行，促进基金销售业务健康有序发展，保护投资者的合法权益。	中国证券投资基金业协会	2012 年 11 月 20 日	
3	证券公司网上证券信息系统技术指引	保障网上证券信息系统的安全、可靠、高效运行，促进证券公司网上开展证券业务的健康有序发展。	中国证券业协会	2015 年 3 月 13 日	
4	证券基金经营机构信息技术管理办法	加强证券基金经营机构信息技术管理，保障证券基金行业信息系统安全、合规运行，保护投资者合法权益	中国证券监督管理委员会	2018 年 12 月 19 日	2018（证监会令【第 152 号令】，2018.12.19），2021 年 1 月 6 日证监会令【第 179 号令】修订
5	证券期货业信息安全事件报告与调查处理办法	规范证券期货业信息安全事件的报告和调查处理，减少信息安全事件的发生。	中国证券监督管理委员会	2021 年 6 月 4 日	证监会公告[2021]12 号

序号	名称	描述	发布单位	执行日期	备注
6	证券期货业网络和信息安全管理办法	有效落实相关法律法规要求，规范证券期货业网络和信息安全管理，防范化解行业网络和信息安全风险，维护资本市场安全平稳高效运行。	中国证券监督管理委员会	2023年2月27日	证监会令第218号

4.2.2 标准体系框架

基于信息安全风险评估的思想和模型，结合行业发展现状，优先关注行业高风险点，突出行业应用和新技术，融合数据安全标准体系，以安全管理为基础支撑，筑牢安全保护、安全检测、安全运营三道防线，并加强数据安全、行业关键信息基础设施重点保护，从以上六个方面进行分析，找出需要补充、加强的标准项，细化完善证券期货行业信息安全体系框架。

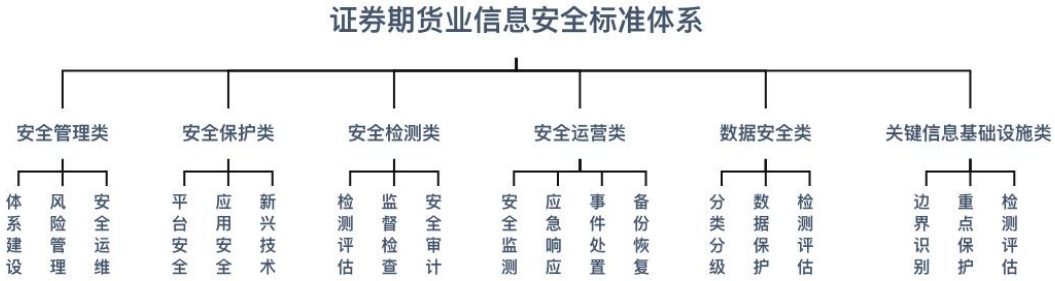

图 1 证券期货行业信息安全标准体系框架

1) 将安全管理类分为体系建设、风险管理、安全运维管理等内容；
2) 将安全保护类分为应用安全、平台安全、新技术等内容；
3) 将安全检测类分为检测评估、监督检查以及安全审计等内容；
4) 将安全运营类分为安全监测、应急响应、事件处置、备份恢复等内容；
5) 参考国家标准和金融数据安全行业标准，结合证券期货业数据属性和业务需求，研究制定数据分类分级、数据安全要求、数据安全评估等标准；
6) 根据国家及行业主管监管部门要求对关键信息基础设施进行重点保护，研究制定关键信息基础设施边界范围的识别确定、重点环节安全保护、检测评估等。

4.2.3 分析结果

通过分析证券期货业信息安全体系框架各相关标准类别，统筹考虑标准的适用性、先进性和前瞻性，明确了需补充和完善的标准内容，规划中包括已发布标准15项、在建标准7项（含行标升级国标1项）、启动标准研究课题7项、有一定需求尚处于前期调研工作阶段的待立项标准17项，合计45项，分析结果如表3所示：

表 3 证券期货业信息安全标准体系分析结果

序号	标准类别	标准名称	状态	备注
1	安全管理	证券期货业信息安全管理体系要求	待立项	
2		证券期货业信息系统风险评估规范	待立项	

序号	标准类别	标准名称	状态	备注
3		证券期货业客户信息保护指南	待立项	
4		证券期货业软件开发安全管理指引	待立项	
5		证券期货业软件供应链安全指南	标准研究课题	BZKT-2022-053
6	安全保护	证券期货业网络安全等级保护基本要求	已发布	JR/T 0060-2021
7		证券期货业第三方交易系统接入技术管理规范	在建	
8		证券期货业互联网应用程序接口安全规范	在建	
9		证券期货业互联网接入安全要求	待立项	
10		证券期货业信息系统上线安全要求	待立项	
11		证券期货业移动互联网应用程序安全规范	已发布	JR/T 0192-2020
12		证券期货行业程序化交易安全管理规范	待立项	
13		证券期货业支撑管理系统安全要求	待立项	
14		证券支付服务业务系统安全要求	待立项	
15		证券期货业软件系统密码技术应用指引	在建	
16		基于多方安全计算的证券风险信息共享技术规范	标准研究课题	BZKT-2022-049
17		证券期货业开源技术应用与风险管理指南	标准研究课题	BZKT-2022-051
18	安全检测	证券期货业移动互联网应用软件安全检测规范	已发布	JR/T 0240-2021
19		证券期货业软件测试指南 软件安全测试	已发布	JR/T 0191-2020
20		证券期货业信创产品及应用软件检测体系标准	标准研究课题	BZKT-2022-047
21		证券期货业数据库测试标准	标准研究课题	BZKT-2022-048
22		证券期货业信息技术安全能力评估标准	标准研究课题	BZKT-2022-050
23		证券期货业个人隐私合规检测规范指南	标准研究课题	BZKT-2022-052

序号	标准类别	标准名称	状态	备注
24		证券期货业信息安全风险评估指标体系	待立项	
25		证券期货业信息系统审计规范	已发布	JR/T 0112-2014
26 – 32		证券期货业信息系统审计指南 第 1 部分：证券交易所 第 2 部分：期货交易所 第 3 部分：中国证券登记结算公司 第 4 部分：其他核心机构 第 5 部分：证券公司 第 6 部分：基金管理公司 第 7 部分：期货公司	已发布	JR/T 0146-2016
33		证券期货业渗透测试指南	已发布	JR/T 0276-2023
34	安全运营	证券期货业信息安全运营管理指南	在建	
35		证券期货业应急响应计划规范	待立项	
36		证券期货业网络安全事件应急演练指南	在建	
37		证券期货业信息安全事件分类分级指南	待立项	
38		证券期货业信息系统灾难恢复规范	待立项	
39	数据安全	证券期货业数据分类分级指引	已发布	JR/T 0158-2018
40		证券期货业数据安全风险防控 数据分类分级指引	在建	国家标准 [a)]
41		证券期货业数据安全管理与保护指引	已发布	JR/T 0250-2022
42		证券期货业数据脱敏管理指南	待立项	
43		证券期货业数据安全评估指南	待立项	
44	关键信息基础设施类	证券期货业关键信息基础设施安全防护要求	待立项	
45		证券期货业关键信息基础设施安全评估指南	待立项	
《证券期货业数据安全风险防控 数据分类分级指引》国家标准计划在 JR/T 0158-2018 的基础上进行转化，目前尚未发布，待国家标准发布后 JR/T 0158-2018 自动废止。				

4.3 具体设计方法

4.3.1 安全管理类设计方法（基础支撑类）

安全管理类标准设计：

对每项安全管理类标准进行深入分析，给出该类别的标准定义。结合现有证券期货行业信息安全标准及相关政策，结合行业实际现状，优先关注行业高风险点，找出需要加强的标准项；对每项安全管理类标准进行深入分析，制定具体的安全管理类标准设计方案。

4.3.2 安全保护类设计方法（技术防护类，第一道防线）

安全保护类标准设计：

对每项安全保护类标准进行深入分析，给出该类别的标准定义。结合现有证券期货行业信息安全标准及相关政策，结合行业实际现状，优先关注行业高风险点，找出需要加强的标准项；对每项安全保护类标准进行深入分析，制定具体的安全保护类标准设计方案。

4.3.3 安全检测类设计方法（监督检查，第二道防线）

安全检测类标准设计：

对每项安全检测类标准进行深入分析，给出该类别的标准定义。结合现有证券期货行业信息安全标准及相关政策，结合行业实际现状，优先关注行业高风险点，找出需要加强的标准项； 对每项安全检测类标准进行深入分析，制定具体的安全检测类标准设计方案。

4.3.4 安全运营类设计方法（安全运营，第三道防线）

安全运营类标准设计：

对每项安全运营类标准进行深入分析，给出该类别的标准定义。 结合现有证券期货行业信息安全标准及相关政策，结合行业实际现状，优先关注行业高风险点，找出需要加强的标准项； 对每项安全运营类标准进行深入分析，制定具体的安全运营类标准设计方案。

4.3.5 数据安全类设计方法（重点防护）

数据安全类标准设计：

对每项数据安全类标准进行深入分析，给出该类别的标准定义。 结合现有证券期货行业信息安全标准及相关政策，结合行业实际现状，优先关注行业高风险点，找出需要加强的标准项； 对每项数据安全类标准进行深入分析，制定具体的数据安全类标准设计方案。

4.3.6 关键信息基础设施类设计方法（重点防护）

关键信息基础设施类标准设计：

对每项关键信息基础设施类标准进行深入分析，给出该类别的标准定义。 结合现有证券期货行业信息安全标准及相关政策，结合行业实际现状，优先关注行业高风险点，找出需要加强的标准项；对每项关键信息基础设施类标准进行深入分析，制定具体的关键信息基础设施类标准设计方案。

5 问题与挑战

5.1 网络安全形势严峻

当前，金融科技迅猛发展，行业数字化转型向更深层次推进，以大数据、云计算、人工智能等新兴技术为基础，场景化、个性化、智能化的高效金融服务不断涌现。数字化时代所具有的开放性和互动性，使得行业领域更容易产生业务、技术、数据、网络等多重风险的叠加。

一方面，网络空间安全面临日益复杂严峻的形势与挑战。网络安全攻击事件频发，关键信息基础设施相关的软硬件设备与重要系统安全漏洞频出，遭受网络攻击的范围、强度不断

增加，影响到证券期货业的正常运行。同时，安全风险造成的影响日益增大，个人信息与重要商业数据频繁遭遇违规利用事件、信息数据泄露事件、网络欺诈勒索等牟利恶意攻击事件，给人民生活带来严重威胁。另一方面，大数据、人工智能、云计算、物联网等新兴技术领域在证券期货业广泛应用，对其风险、威胁和安全问题的研究仍然不足，移动互联网、物联网等领域爆发的安全问题越来越多，缺少对新兴技术大规模应用的安全风险分析与防控，新技术和新的互联网应用形态下的安全防护能力亟待加强。

5.2 数据安全体系融合需求迫切

近年来，证券期货业在快速发展过程中，积累了大量的数据资产，数据已成为证券期货业的重要资产和核心竞争力，充分发挥数据价值、用数据驱动创新、实现高质量发展已成为行业共识。证券期货行业掌握的大量高敏感性、高重要性数据，需要施以适当的数据安全保障措施，来保障投资者权益及证券市场的公平性和稳定性。

调研显示，部分行业机构尚未建立健全的数据安全管理组织架构；技术手段未能全面覆盖数据采集、数据传输、数据存储、数据处理、数据交换、数据销毁等数据处理过程。证券期货业数据管理的标准化水平有待进一步提升。

信息安全专业工作组为合并成立，需要融合并完善原系统安全与数据安全标准体系，体系内各标准应有明确定位，不同标准之间内在的关联关系需清晰明确，标准内容之间应协调一致。

5.3 标准的国际化水平有待提高

高质量的标准是接轨国际、提升国际话语权和增强国际竞争力的技术支撑。需要深化标准化交流合作，推动信息安全标准与证券期货行业的国际先进标准接轨，提高我国标准与国际标准的一致性程度、与国际标准体系的兼容性。同时保证信息安全标准体系的开放式、普适性，基本覆盖证券期货行业内的重要信息系统及数据处理全过程，保证标准能够尽快落实现有法律法规等政策要求，完善证券期货行业信息安全的动态循环。

5.4 标准协同研究机制尚需探索

专业工作组与产、学、业各界及各类标准机构的交流合作机制还在完善。同时，专业领域与数据治理、技术管理、金融科技等多领域存在交叉区域，需加强与各专业工作组的沟通与协调，厘清相关职责边界与分工合作，防止行业标准体系出现疏漏或重合。

6 重点任务

6.1 安全管理类

证券期货行业需要建立健全的信息安全管理体系，围绕制度、组织、人员、建设、安全运维等落实安全管理措施。重点从以下方面开展安全管理类标准建设：

1) 体系建设-为行业相关信息安全的体系建设提供策略类的要求和指引；
2) 风险管理-为行业信息安全相关的风险管理提供技术上和管理上的策略类指引；
3) 安全运维-以保障信息安全为目的，为行业信息系统的安全运维管理工作，提供策略类的指导性建议和规范。

6.2 安全保护类

行业需要加强安全保护，根据信息系统可能出现的安全问题而采取防御措施，采用一切可能的方法、技术和手段防止信息系统遭受安全威胁，减少和降低遭受入侵和攻击的可能或危害。重点从以下方面开展安全保护类标准建设：

1) 应用安全-从应用层面，如开发管理、代码规范、身份认证技术、系统互联规范等方面，为行业内信息安全的保护工作提供相关要求。
2) 平台安全-从网络、主机技术管理层面，为行业内系统平台的信息安全的保护工作提供指导和要求。
3) 新兴技术-为人工智能、区块链/分布式账本、隐私计算、零信任等新技术在行业信息安全保护工作的实践、应用提供指导性建议和规范。

6.3 安全检测类

安全检测是根据安全策略对实施保护的信息系统进行监控和检测。监控是对系统运行状态进行监视和控制，发现异常，并可能作出动态调整。检测是对已部署的系统及其安全防护进行检查测量，是动态响应和加强防护的依据，是强制落实安全策略的手段。重点从以下方面开展安全检测类标准建设：

1) 检测评估-以行业内信息系统（包括物理环境、网络结构、网络设备、服务器设备、数据库系统、应用软件、信息安全管理）的安全检测、风险评估为入口，提供指导和要求规范；
2) 安全审计-为行业信息系统的安全审计工作提供规范、指南和标准，指导行业通过检查、评价信息安全控制措施的充分性、有效性和适宜性，揭示问题，提出完善措施的意见和建议。

6.4 安全运营类

推进行业相关网络安全防护和监测体系建设，持续建设、完善常规威胁监测发现、应急响应、安全事件处置、备份恢复等安全能力，为信息系统相关应急响应工作的计划制定、应急演练等，为网络安全事件的分类处置、安全保障的框架设计及信息系统的备份和恢复方面等，提供规范化的指导、技术及管理等能力要求。

基于以上基础，总结参与各级网络安全实战攻防演练的行业各方经验，探索行业安全运营常态化思路，将短期的突击性的防守保障工作转化为常态化、实战化、体系化的安全运营能力，以人为中心，以技术为辅佐，推动常态化的监控、研判、溯源、处置流程，将运营机制纳入日常流程中，提升行业实战对抗水平。

重点探索具备行业特色的网络安全态势感知、主动防御、欺骗防御、异常行为分析、威胁狩猎、情报共享、安全编排与自动化、联防协同等进阶安全能力等方面的安全运营类标准建设。

6.5 数据安全类

数据安全类标准建设应在信息安全标准建设基础上重点关注数据安全领域特有问题，由于证券业务类型多样化的行业特征，行业数据的复杂程度较高。承接外部监管政策要求及内部数据安全保障诉求等，以数据分类分级作为全生命周期数据保护框架的基础，搭建科学、规范、统一的数据分类分级方法，可以帮助行业机构厘清数据资产，确定数据重要性或敏感度，合理分配数据保护资源和成本。在数据分类分级标准的基础上，辅以配套管理技术手段，

落实数据安全保护、数据安全成熟度评估、数据安全能力评估等要求，实现数据安全风险管理，有效控制并降低数据安全风险事件的发生概率，形成一套完善的数据资产管理与保护机制。重点从以下方面开展数据安全类标准建设：

1) 数据分类分级-以术语定义、数据安全框架、数据分类分级提供基础支撑，目前已完成行业标准，正转化为国家标准《证券期货业数据安全风险防控 数据分类分级指引》。
2) 数据安全保护-从数据采集、传输、存储、处理、交换（共享）、删除、销毁等数据生命周期维度规范数据安全保护要求。
3) 数据安全评估-指导行业落实数据安全管理要求，包括数据安全成熟度评估、数据安全能力认证等。

6.6 关键信息基础设施保护类

关键信息基础设施保护，在网络安全等级保护基础上，实行重点保护。以安全管理为基础支撑，筑牢安全保护、安全检测、安全运营三道防线，加强数据安全保护，并对关键信息基础设施实施重点保护。

标准是规范行业关键信息基础设施保护工作的具体依据，是指导关键信息基础设施保护工作的实施指南。需要统筹优化，开展关键标准研制，并不断强化标准实施应用，以标准助力提升关键信息基础设施综合防护水平。

坚持以关键业务为核心的整体防控、以风险管理为导向的动态防护和以信息共享为基础的协同联防的基本原则，从分析识别、安全防护、检测评估、监测预警、主动防御、事件处置等方面，加强行业关键信息基础设施保护的标准研究与制定。

7 任务计划

7.1 持续跟踪国内外网络安全政策要求

近年来，各国相继颁布网络安全、数据安全政策，我国也陆续推出法律法规、国家标准、行业标准和技术规范，对此类政策的分析和总结将有助于理解前瞻性的网络安全管理要求，可对信息安全工作组的标准制定和推广工作进行指导。

7.2 关注行业需求调整标准规划重点任务

工作组结合行业需求，突出行业应用，根据本规划制定行业信息安全标准体系建设重点任务，并结合各标准建设的紧迫程度和优先级，制定 2023—2025 年信息安全标准建设任务计划见表 4：

表 4 证券期货行业信息安全标准建设任务计划

序号	标准分类	标准名称	标准层级	紧迫程度	计划时间（年）
1	安全管理类	证券期货业客户信息保护指南	行业标准	***	2024
2	安全管理类	证券期货业软件供应链安全指南	行业标准	****	2023

3	安全管理类	证券期货业软件开发安全管理指引	行业标准	***	2024
4	安全保护类	证券期货业互联网应用程序接口安全规范	行业标准	****	2023
5	安全保护类	证券期货业软件系统密码技术应用指引	行业标准	****	2023
6	安全保护类	证券期货业互联网接入安全要求	行业标准	**	2025
7	安全保护类	证券期货业信息系统上线安全要求	行业标准	**	2025
8	安全保护类	证券期货业开源技术应用与风险管理指南	行业标准	****	2023
9	安全保护类	基于多方安全计算的证券风险信息共享技术规范	行业标准	****	2023
10	安全检测类	证券期货业信息技术安全能力评估指南	行业标准	****	2023
11	安全检测类	证券期货业数据库测试指南	行业标准	***	2024
12	安全检测类	证券期货业个人隐私合规检测规范	行业标准	****	2023
13	安全检测类	证券期货业信创产品及应用软件检测规范	行业标准	***	2024
14	安全运营类	证券期货业信息安全运营管理指南	行业标准	****	2023
15	安全运营类	证券期货业网络安全事件应急演练指南	行业标准	***	2024
16	数据安全类	证券期货业数据安全风险防控 数据分类分级指引	国家标准	****	2023
17	数据安全类	证券期货业数据安全评估指南	行业标准	**	2025
18	数据安全类	证券期货业数据脱敏管理指南	行业标准	****	2023
19	关键信息基础设施类	证券期货业关键信息基础设施安全防护要求	行业标准	***	2024
20	关键信息基础设施类	证券期货业关键信息基础设施安全评估指南	行业标准	**	2025

8 实施保障

8.1 规范流程

信息安全专业工作组严格按照行业标准的制度原则，邀请多方参与，充分发挥民主优势，从申请、立项、起草到征求意见，做到三稿定标，即征求意见稿、送审稿、报批稿。不仅行业标准制定单位和人员要包含行业产业链各环节的企业，还要广泛征求行业内外专家的意见，做到及时反馈，确保制定的标准具有权威性、科学性和实用性。

8.2 沟通交流

为保障行业标准研制的顺利开展，信息安全专业工作组要求各标准起草工作组定期召开工作小组会议，小组成员汇报工作进展，分享各自收集的信息，提出现阶段难题，部署下一阶段的工作安排。会议决议应通过会议纪要的形式留存，并发送证标委及工作组成员知悉。在行业标准研制阶段，根据需要可以寻求监管部门在行业调研、意见征集等方面的支持。在征求意见阶段，分次提请行业专家从专业角度给予意见，并及时答复相关意见。

8.3 协同合作

为了避免行业标准研制过程中出现中断情况，信息安全专业工作组要求各标准起草工作组从标准起草初期就开始建立工作协同机制，采用牵头单位负责制，明确分工，各就其职，协同合作，及时处理分歧，层层把关，破解制定过程中的难题，共同推进标准研制工作顺利进行。

9 组织保障

9.1 加强能力建设

向证券期货业内有关单位宣传标准化建设的目的意义，组织开展标准化专业培训活动，树立各单位管理层的标准化意识，提高技术人员的标准化能力，利用标准促进行业知识推广，显性化、体系化，以降低行业知识门槛，从而显著推动行业治理工作的开展。

9.2 完善物资配备

加强对信息安全标准化建设工作的经费投入力度，证券分技术委员会和信息安全工作组有关单位应设置标准化专项资金。鼓励发挥市场机制作用，带动多方投入，为标准化工作提供资金保障。