证券期货业系统安全标准设计方案
（2019 版）

全国金融标准化技术委员会证券分技术委员会

系统安全专业工作组

（WG51）

参与人员名单

设计方案修订单位：

中国证监会信息中心、国泰君安证券、上海市信息安全测评认证中心

设计方案修订人员：

张野、刘铁斌、周云晖、高红洁、俞枫、陈凯晖、李宏达

目　　录

1. 目标

为适应证券期货业各类业务的创新与发展，降低行业整体信息安全风险与成本，进一步规范行业信息安全标准的制定与应用，提高信息安全标准化水平，特制定证券期货业系统安全标准设计方案（以下简称“设计方案”）。

本设计方案描绘了证券行业信息安全标准全貌和标准化活动蓝图，是行业未来一段时间所需信息安全标准的整体设计方案，是标准制修订计划的主要依据和标准化工作的重要参考，对证券期货行业信息系统的建设运维、检测评估、行业监督管理等具有基础支持作用。

2. 范围

本设计方案适用于制定证券期货业信息安全标准。

信息安全标准制定过程中，各相关立项、承办、参与单位等，应充分理解本设计方案，按照本设计方案制定的标准体系，有计划地推进标准制定工作。

3. 设计原则

3.1基于风险评估的思想和模型

从标准体系本身以及标准本身均应体现风险评估的思想：一是标准体系应覆盖风险管理的每个部分。二是标准内容（特别是以业务应用为主体）编制应以风险分析为前提。

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，以国标（GB/T 20984-2007《信息安全技术 信息安全风险评估规范》）为指导，同时把技术风险的识别与业务风险的评估有机统一起来，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，为行业提供更全面，更有效的风险信息。

标准体系的主要设计依据是《GBZ 24364-2009 信息安全风险管理指南》，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。从具体标准体系的构建角度，引入PPDRR模型。PPDRR模型是典型的、公认的安全控制模型。它是一种动态的、自适应的安全控制模型，可适应安全风险和安全需求的不断变化，提供持续的安全保障。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。

3.2优先关注行业高风险点

在信息安全标准体系的设计方案过程中，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，充分发现本行业与其他行业所不同的风险所在，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突出行业应用及新技术

由于证券期货行业的特殊性，其应用系统的特点、信息安全的关注点也不同于其他行业。行业标准体系设计方案在制定过程中，应突出证券期货行业的特定应用，把握该应用的相关特性，优先保证证券期货行业内应用系统的信息安全。

此外，本设计方案还应关注证券期货行业的新技术。新技术的引入往往带来新的风险点，在进行行业标准体系设计方案时，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，需优先进行信息安全统一规范。

3.4突出行业普适性，落实行业政策

行业标准体系设计方案在制定过程中，应突出行业的普适性，保证证券期货行业内大部分的信息系统可参考本设计方案的信息安全标准体系。同时也要求本设计方案的信息安全标准体系基本全覆盖证券期货行业内的重要信息系统及相关方面。

此外，本设计方案还应落实证券期货行业的相关政策。第一保证本设计方案不与现有的政策相冲突；第二要求本设计方案的相关标准能够尽快落实政策要求，完善证券期货行业信息安全的动态循环。

3.5参考现有标准，统筹协调

行业标准体系在设计过程中，应充分考虑现有标准体系，在风险评估的思想模型中，尽可能参考现有的信息安全标准，为今后发展设计方案做好准备。

统筹协调现有信息安全标准主要考虑以下两点：

a)与其他信息安全标准之间：对于基础性信息安全标准以及其他行业共性的安全标准原则上采取标准参考借鉴；对于具备行业特点需要细化和创新的列入标准制定计划目录。

b)与其他信息化标准之间：做好标准之间的统筹和协调，为其他信息化标准提供支撑，防止出现标准之间术语不统一，相互矛盾情况。

在统筹协调的过程中，还需综合考虑现有标准的实用性、应用成本和应用范围等因素。

4.设计方法

4.1总体方法

本设计方案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设计方案：

a)从安全策略、安全保护、安全检测、响应恢复四个方面，对行业信息安全进行分析，得出证券期货行业信息安全体系框架图，具体结果参见附录 A 证券期货行业信息安全体系框架图；

b)分析和统计证券期货行业现有的标准和相关政策，得出附录 B 现有证券期货行业信息安全标准及相关政策；

c)基于风险评估的思想和模型，结合行业实际现状，优先关注行业高风险点，在安全策略、安全保护、安全检测、响应恢复四个方面上进行分析，找出哪些方面标准需要加强，得出附录 C 证券期货业信息安全标准体系分析结果。

d)根据证券期货业信息安全标准体系分析结果，以及实际情况等因素，选择目前最需要编制的相关标准，得出附录 D 证券期货行业信息安全标准体系标准编制工作设计方案。

每项标准设计方案，均包括标准名称、标准范围、优先级、牵头单位、实施计划等内容。以便协调标准化工作的开展。

4.2安全管理类设计方法（基础支撑类）

在安全管理类中进行分析设计方案的详细方法和步骤如下：

a)基于风险评估的思想和模型，将安全管理类分为体系建设、风险管理、机构管理、运维管理以及工程管理等内容（其中机构管理、工程管理的相关内容由其他专业工作组整理和设计方案）；

b)对每个安全管理类标准进行深入分析，给出该类别的标准定义。结合附录 B 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，找出哪些方面标准需要加强；

c)对每个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安全保护类设计方法（技术防护类,第一道防线）

在安全保护类中进行分析设计方案的详细方法和步骤如下：

a)基于风险评估的思想和模型，将安全保护类分为环境安全、应用安全、平台安全、数据安全以及新技术等内容（其中数据安全的相关内容由其他工作组整理和设计方案）；

b)对每个安全保护类标准进行深入分析，给出该类别的标准定义。结合附录 B 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，找出哪些方面标准需要加强；

c)对每个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。

4.4安全检测类设计方法（监督检查,第二道防线）

在安全检测类中进行分析设计方案的详细方法和步骤如下：

a)基于风险评估的思想和模型，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；

b)对每个安全检测类标准进行深入分析，给出该类别的标准定义。结合附录 B 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，找出哪些方面标准需要加强；

c)对每个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。

4.5响应恢复类设计方法（第三道防线）

在响应恢复类中进行分析设计方案的详细方法和步骤如下：

a)基于风险评估的思想和模型，将响应恢复类分为应急响应、事件处置以及备份恢复等内容；

b)对每个响应恢复类标准进行深入分析，给出该类别的标准定义。结合附录 B 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，找出哪些方面标准需要加强；

c)对每个响应恢复类标准进行深入分析，制定具体的响应恢复类标准设计方案。

5. 设计内容

5.1总体设计

证券期货业系统安全标准设计方案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，得出证券期货行业信息安全体系框架图，具体结果参见附录A。设计方案数量统计如表1所示。具体包括：已制定标准6个（证券期货行业已发布的金融行业标准）；已立项标准13个（全国金融标准化技术委员会证券分技术委员会正在组织

制定的金融行业标准和国家标准）；待立项标准11个（有一定需求，正处于调研工作阶段的项目），共计31个标准。

表1 证券期货业系统安全标准设计方案统计表

类别	已制定	已立项	待立项	小计
安全管理类	1	3	3	7
安全保护类	1	5	5	11
安全检测类	3	4	0	7
响应恢复类	1	1	3	5
合计	6	13	11	31

5.2安全管理类标准设计

本设计方案基于风险评估的思想和模型，对现有的安全管理类标准进行了统计分析（详见附录B: 现有证券期货行业信息安全标准及相关政策），对证券期货行业的相关政策进行解读，并优先关注行业高风险点，突出行业应用、新技术和普适性。最终该类标准设计方案为7个，其中已制定标准为1个，已立项标准为3个，待立项标准为3个，详见附录C证券期货业信息安全标准体系分析结果。

具体的工作设计方案内容详见附录D证券期货行业信息安全标准体系标准编制工作设计方案。

5.3安全保护类标准设计

本设计方案基于风险评估的思想和模型，对现有的安全保护类标准进行了统计分析（详见附录B现有证券期货行业信息安全标准及相关政策），对证券期货行业的相关政策进行解读，并优先关注行业高风险点，突出行业应用、新技术和普适性。最终该类标准设计方案为11个，其中已制定标准为1个，已立项标准为5个，待立项标准为5个，详见附录C证券期货业信息安全标准体系分析结果。

具体的工作设计方案内容详见附录D证券期货行业信息安全标准体系标准编制工作设计方案。

5.4安全检测类标准设计

本设计方案基于风险评估的思想和模型，对现有的安全检测类标准进行了统计分析（详见附录B现有证券期货行业信息安全标准及相关政策），对证券期货行业的相关政策进行解读，并优先关注行业高风险点，突出行业应用、新技术和普适性。最终该类标准设计方案为7个，其中已制定标准为3个，已立项标准为4个，详见附录C证券期货业信息安全标准体系分析结果。

具体的工作设计方案内容详见附录D证券期货行业信息安全标准体系标准编制工作设计方案。

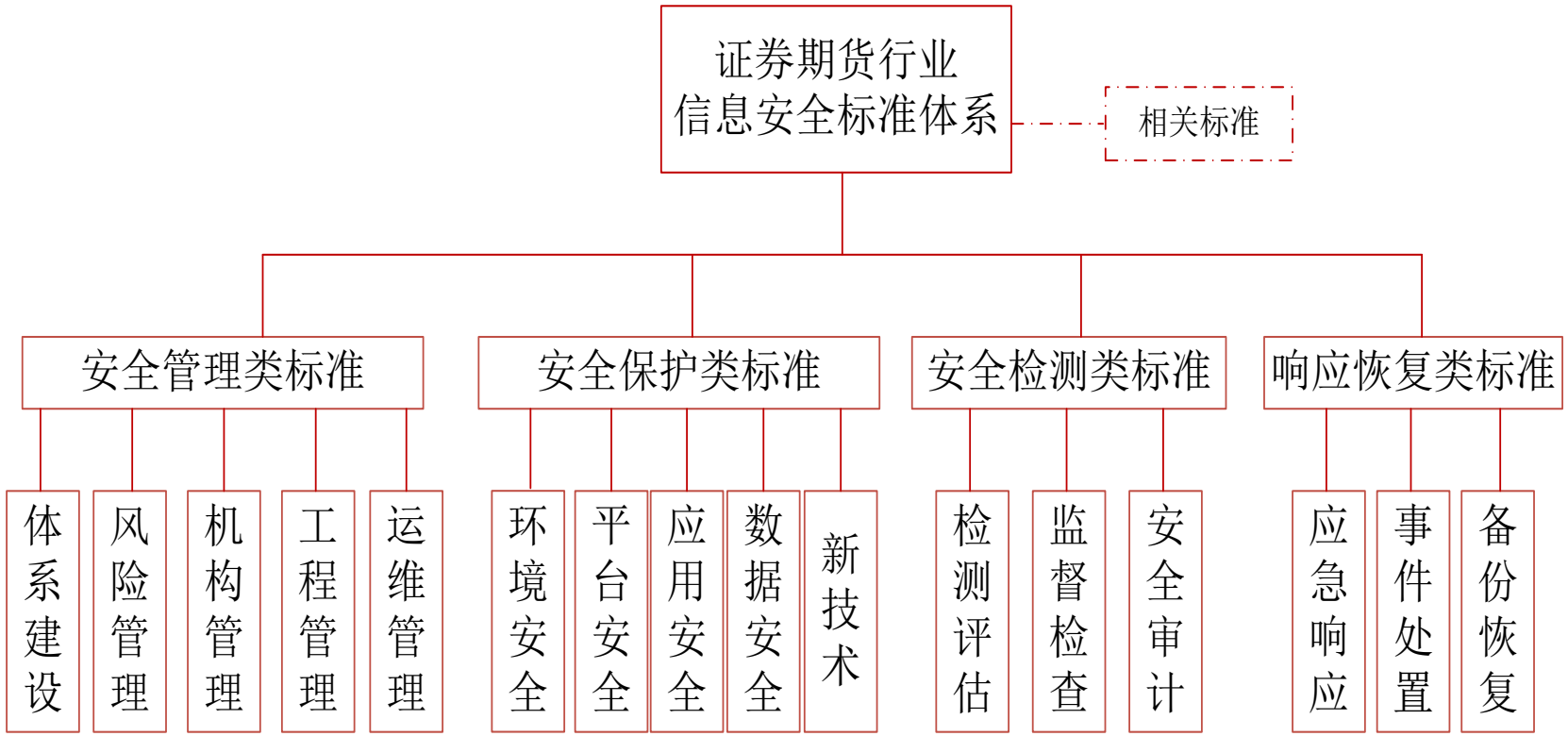
5.5响应恢复类标准设计

本设计方案基于风险评估的思想和模型，对现有的响应恢复类标准进行了统计分析（详见附录B:现有证券期货行业信息安全标准及相关政策），对证券期货行业的相关政策进行解读，并优先关注行业高风险点，突出行业应用、新技术和普适性。最终该类标准设计方案为5个，其中已制定标准为1个，已立项1个，待立项标准为3个，详见附录C证券期货业信息安全标准体系分析结果。

具体的工作设计方案内容详见附录D证券期货行业信息安全标准体系标准编制工作设计方案。

附录 A 证券期货行业信息安全标准体系框架图

本文对证券期货行业信息安全标准体系框架定义如下图所示：



附录 B 现有证券期货行业信息安全标准及相关政策

证券期货行业标准体系现有信息安全标准见下表：

序号	标准名称	标准范围	状态（已发布、待发布）	归口单位	备注
1	证券期货业信息系统安全等级保护基本要求	规定了证券期货业不同安全保护等级信息系统安全的基本保护要求，包括基本技术要求和基本管理要求，适用于指导证券期货业分等级信息系统的安全建设整改、测评和监督管理。	已发布	全国金融标准化技术委员会	JR/T 0060-2010
2	证券公司信息技术管理规范	规定了证券公司信息技术管理的：信息技术管理工作中应遵循的基本原则；信息技术管理的组织架；信息技术人员管理和安全管理；机房和设备管理；网络通信、软件和数据；信息系统运行管理、技术事故的防范预处理。	已发布	全国金融标准化技术委员会	JR/T 0023-2004
3	证券期货业信息系统运维管理规范	规定了证券期货业信息系统运维管理工作的要求。	已发布	全国金融标准化技术委员会	JR/T 0099-2012
4	证券期货业信息系统安全等级保护测评要求	规定了对证券期货业信息系统安全等级保护状况进行安全测试评估的要求，包括对第一级信息系统、第二级信息系统、第三级信息系统和第四级信息系统进行安全测试评估的单元测评要求和信息系统整体测评要求。本标准略去对第五级信息系统进行单元测评的具体内容要求。	已发布	全国金融标准化技术委员会	JR/T 0067-2011
5	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。	已发布	全国金融标准化技术委员会	JR/T 0112-2014
6	证券期货经营机构信息系统备份能力标准	明确了证券期货经营机构信息系统备份能力的含义，定义了备份能力的等级。是证券期货经营机构信息系统备份能力建设的设计标准，用于指导信息系统备份能力建设工作。	已发布	全国金融标准化技术委员会	JR/T 0059-2010

证券期货行业信息安全的相关政策见下表：

序号	名称	描述	发布单位	执行日期	备注
1	证券期货业信息安全保障管理办法	保障证券期货信息系统安全运行，加强证券期货业信息安全管理工作，促进证券期货市场稳定健康发展，保护投资者合法权益。	中国证券监督管理委员会	2012 年 11 月 1 日	证监会令第 82 号
2	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	2013 年 2 月 1 日	证监会公告[2012]46 号
3	中国证券监督管理委员会公告〔2011〕39 号	规定了证券期货业不同安全保护等级信息系统的基本保护要求，包括基本技术要求和基本管理要求，适用于指导证券期货业分等级信息系统的安全建设整改、测评和监督管理。	中国证券监督管理委员会	2011 年 11 月 22 日	证监会公告[2011]39 号
4	中国证券监督管理委员会公告〔2011〕10 号	引导证券期货经营机构加强备份能力建设，规范开展信息系统备份工作，提高抗风险能力，确保信息系统安全稳定运行和重要数据安全。	中国证券监督管理委员会	2011 年 4 月 14 日	证监会公告[2011]10 号
5	关于发布《证券公司网上证券信息系统技术指引》的通知	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	——

附录 C 证券期货业信息安全标准体系分析结果

根据标准体系内的标准进行类别分析，结果见下表：

序号	标准类别（一级）	标准类别（二级）	覆盖领域	标准名称	兼容方式
1	安全管理类	体系建设	为证券期货行业相关信息安全的体系建设提供策略类的要求和指引。	证券期货业信息安全管理体系要求	待立项
2				JR/T 0023-2004 证券公司信息技术管理规范移动互联网	已制定
3		风险管理	为证券期货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。	证券期货业信息系统风险评估规范	待立项
4				证券期货业客户信息保护指南	待立项
5				证券期货业信息技术统计标准	已立项
6				证券期货业信息技术供应商管理规范	已立项
7				证券期货业软件开发安全管理指引	已立项
8		机构管理	为证券期货行业信息安全工作中的机构管理提供策略类的指导和规范。	*该领域由其他工作组整理和设计方案	——
9		工程管理	为证券期货行业信息安全工作中的工程管理提供策略类的指导和规范。	*该领域由其他工作组整理和设计方案	——
10		运维管理	以保障信息安全保障为目的，为证券期货行业的运维管理工作（如日常运维、设备管理、安全事件处置等），提供策略类的指导性建议和规范。	JR/T 0099-2012 证券期货业信息系统运维管理规范	已制定

序号	标准类别（一级）	标准类别（二级）	覆盖领域	标准名称	兼容方式
11		运营管理	指导各证券期货业机构保障信息安全有效性及合规有效落地，提升安全工程化及发现安全防护缺陷能力，将安全服务质量保持在稳定区间，全面衡量评价安全管理和防护体系质量水平。	证券期货业信息安全运营管理指南	已立项
12	安全保护类	环境安全	以信息安全保障为目的，为信息系统所部属的物理环境提供指导和要求。	证券期货业托管机房技术指引（在建）	已立项
13		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。	JR/T 0060-2010 证券期货业信息系统安全等级保护基本要求	已制定
14				《证券期货业第三方交易系统接入技术管理规范》	已送审
15				证券期货业互联网接入安全要求	待立项
16				证券期货业信息系统上线安全要求	待立项
17		应用安全	从应用安全层面，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。	《证券期货业身份鉴别等级》	已送审
18				《证券期货业移动互联网应用程序安全规范》	已送审
19				证券期货行业程序化交易安全管理规范	已立项
20				证券期货业支撑管理系统安全要求	待立项
21		数据安全	从数据层面，如数据接口、传输接口、通信协议方面，为行业内系统数据安全提供指导和要求。	证券期货业商业秘密信息系统安全技术指引 *该领域由其他工作组整理和设计方案	——

序号	标准类别（一级）	标准类别（二级）	覆盖领域	标准名称	兼容方式
22		新技术	针对行业内信息系统引入的新技术及新业务模式，如云计算、支付业务等，提供相关的安全指南和安全能力要求，为行业内信息系统的安全性提供保护。	证券支付服务业务系统安全要求	待立项
23				《证券期货业云技术应用安全规范》	已送审
24	安全检测类	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。	JR/T 0067-2011 《证券期货业信息系统安全等级保护测评要求》	已制定
25				《证券期货业移动互联网应用软件安全检测规范》	已立项
26				《证券期货业软件测试指南：软件安全测试》	已送审
27		监督检查	为行业信息安全监管决策提供审核和评估方面的指导和体系规范。	《证券期货业信息安全风险评估指标体系》	已立项
28				《证券期货业信息安全审查规范》	已立项
29		安全审计	为证券期货行业内信息系统的安全审计工作提供规范和标准。	JR/T 0112-2014 《证券期货业信息系统审计规范》	已制定
30		安全审计	为证券期货行业内信息系统的安全审计工作提供指南。	JR/T 0146—2016《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	已制定

序号	标准类别（一级）	标准类别（二级）	覆盖领域	标准名称	兼容方式
31	响应恢复类	应急响应	为信息系统相关应急响应工作的计划制定提供规范化的指导或要求。	证券期货业应急响应计划规范	待立项
32			为行业网络安全事件应急演练提供指南	证券期货业网络安全事件应急演练指南	已立项
33		事件处置	为信息安全事件的分类处置、安全保障的框架设计提供指导和要求。	证券期货业信息安全事件分类分级指南	待立项
34		备份恢复	从信息系统的备份和恢复方面出发，提供相关的规范和技术/管理能力要求。	证券期货业信息系统灾难恢复规范	待立项
35				JR/T 0059-2010 《证券期货经营机构信息系统备份能力标准》	已制定

附录 D 证券期货行业信息安全标准体系标准编制工作设计方案

证券期货行业信息安全标准体系的标准编制工作设计方案见下表：

序号	标准分类	标准中文名称	制定/修订目的	兼容方式（制定/修订/延续）	优先级	牵头单位	实施计划
1	安全管理类	证券期货业信息安全管理体系要求	建立一套相关要求，用以帮助组织明确其在整体或特定范围内建立信息安全方针和目标，以及完成这些目标所用方法的信息安全管理体系。	制定	高		
2	安全管理类	证券期货业信息系统风险评估规范	根据证券期货业现有技术的发展水平，提出证券期货业信息安全风险评估的方法，规定不同信息安全风险保护能力的具体评估指标。	制定	高		
3	安全管理类	证券期货业客户信息保护指南	随着信息技术的广泛应用和互联网的不断普及，个人信息在社会、经济活动中的地位日益凸显，滥用个人信息的现象随之出现，给社会秩序和个人切身利益带来了危害。为促进个人信息的合理利用，指导和规范利用信息系统处理个人信息的活动，制定本指导性技术文件。	制定	高		
4	安全管理类	证券期货业信息技术统计标准	建立相对完整、合理、开放的信息技术统计指标体系，对披露信息、投资者保护信息、行业性基础设施数据、信息技术基础运行数据进行收集，有助于全面、持续地识别、监测、分析、评估行业信息技术安全风险。	制定	很高		

序号	标准分类	标准中文名称	制定/修订目的	兼容方式（制定/修订/延续）	优先级	牵头单位	实施计划
5	安全管理类	证券期货业信息技术供应商管理规范	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，提高重点领域外包服务的安全管控能力。	制定	高		
6	安全管理类	证券期货业软件开发安全管理指引	组织制定软件开发安全管理标准与规范，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。	制定	高		
7	安全管理类	JR/T 0023-2004 证券期货业信息系统运维管理规范	规定了证券期货业信息系统运维管理工作的要求。	延续			
	安全管理类	证券期货业信息安全运营管理指南	指导各证券期货业机构保障信息安全有效性及合规有效落地，提升安全工程化及发现安全防护缺陷能力	制定	高		
8	安全保护类	证券期货业托管机房技术指引	为了对向证券期货行业提供租赁服务的数据中心，包括所涉及的计算机房、网络接入、机架布线和运行管理等方面进行规范，同时也为了提升行业内提供租赁服务的数据中心服务水平，提高服务质量，降低系统运行风险。	制定	很高		
9	安全保护类	JR/T 0060-2010 证券期货业信息系统安全等级保护基本要求	规定了证券期货业不同安全保护等级信息系统安全的基本保护要求，包括基本技术要求和基本管理要求，适用于指导证券期货业分等级信息系统的安全建设整改、测评和监督管理。	延续			

序号	标准分类	标准中文名称	制定/修订目的	兼容方式（制定/修订/延续）	优先级	牵头单位	实施计划
10	安全保护类	证券期货业第三方交易接入规范	随着业务的发展，程序化交易、量化交易、高频交易等系统越来越多的接入现有的传统的交易体系，建设系统接入标准，防止程序化交易等引起后台系统超载、系统缺陷、市场价格异常偏离等问题，规范化系统接入的认证、接入信任、监视、控制、安全、应急等一系列的管理。	制定	很高		
11	安全保护类	证券期货业互联网接入安全要求	随着互联网、移动互联网的发展，越来越多的证券期货业业务系统需要接入互联网。应建设行业业务系统接入互联网的标准，防止互联网引入的安全风险利用行业业务系统存在的安全漏洞导致出现拒绝服务、数据篡改、数据泄露等安全事件，规范化系统接入的认证、接入信任、审计、访问控制、安全建设和运维、灾备、应急等一系列的管理。	制定	很高		
12	安全保护类	证券期货业信息系统上线安全要求	证券期货业目前在系统上线方面没有定义专门的安全规范。因为系统上线运行是一个很关键的环节，若对此环节未予以安全控制，很可能会出现业务合规/信息安全等方面的问题，所以应建立相关方面的标准予以规范，防范风险。	制定	中		

序号	标准分类	标准中文名称	制定/修订目的	兼容方式（制定/修订/延续）	优先级	牵头单位	实施计划
13	安全保护类	《证券期货业身份鉴别等级》	身份认证是实现信息安全的基本技术，与信息安全的各个范畴紧密相关，而互联网金融的发展使得应用安全中的身份认证变得尤为重要，相关的标准建设已成为行业迫切的需求。	制定	很高		
14	安全保护类	《证券期货业移动互联网应用程序安全规范》	当前移动互联网应用服务发展十分迅速，产业规模和用户数量越来越大，一旦应用服务存在缺陷或安全问题，将影响系统的运行安全和用户的个人信息安全。相关安全防护要求有待完善，对移动互联网联网应用的安全防护能力进行要求。	制定	很高		
15	安全保护类	证券期货行业程序化交易安全管理规范	由于程序化交易的特殊性，一旦发生故障可能导致严重的安全事件。故制定程序化交易技术标准，规范程序化交易的范围、方法、流程等内容，有效控制程序化交易风险。	制定	中		
16	安全保护类	证券期货业支撑管理系统安全要求	针对行业内重要业务支撑和内部管理的信息系统，提供相关的安全管理指南和安全能力要求，为行业内信息系统的安全性提供保护。	制定	低		
17	安全保护类	证券支付服务业务系统安全要求	随着证联相关支付业务的发展，其相关互联网支付服务业务系统的安全性也将成为安全服务保障的重点之一。可参考银行或非金融支付机构的相关互联网支付系统的	制定	中		

序号	标准分类	标准中文名称	制定/修订目的	兼容方式（制定/修订/延续）	优先级	牵头单位	实施计划
			相关安全要求，对证券业互联网支付业务系统的安全性要求进行标准建立。				
18	安全保护类	证券期货业云技术应用安全规范	证券期货业有些重要系统可能会逐步部署在云（私有云/公有云）上。证券期货业有着自己的业务特点或要求，比如说“交易速度快”就是其中一个。为了适应行业业务开展的需要，在参考国家标准的基础上，应逐步明确行业内 IaaS/PaaS/SaaS 的安全服务标准。	制定	中	深交所	
19	安全检测类	JR/T 0067-2011 证券期货业信息系统安全等级保护测评要求	规定了对证券期货业信息系统安全等级保护状况进行安全测试评估的要求，包括对第一级信息系统、第二级信息系统、第三级信息系统和第四级信息系统进行安全测试评估的单元测评要求和信息系统整体测评要求。本标准略去对第五级信息系统进行单元测评的具体内容要求。	延续			
20	安全检测类	证券期货业移动互联网应用软件安全检测规范	当前移动互联网应用服务发展十分迅速，产业规模和用户数量越来越大，一旦应用服务存在缺陷或安全问题，将影响系统的运行安全和用户的个人信息安全。除了对服务提供者的安全防护能力需要进行要求，相关安全检测方面（如：检测范围、	制定	中		

序号	标准分类	标准中文名称	制定/修订目的	兼容方式（制定/修订/延续）	优先级	牵头单位	实施计划
			检测方法、评定准则等）也需要有一个统一的标准作为规范或参考。				
21	安全检测类	《证券期货业软件测试指南：软件安全测试》	组织制定软件开发安全测试指南，参考软件开发最佳实践，为软件开发安全测试提供有效指导。	制定	高	大商所	
22	安全检测类	证券期货业信息安全风险评估指标体系	为了有效识别行业信息安全风险，需要建设一套风险评估指标体系，合理评估行业机构信息安全状态，为行业信息安全监管决策提供科学、准确的数据依据。	制定	很高		
23	安全检测类	证券期货业信息安全审查规范	以国家网络安全审查相关政策为依据，制定行业信息安全审查标准，统一行业内审查内容，加强行业专用信息技术、产品和服务的安全审查和检测。	制定	中		
24	安全检测类	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。	延续			
25	安全检测类	证券期货业信息系统审计指南		修订	中		
26	响应恢复类	证券期货业应急响应计划规范	用于规定证券期货业编制信息安全应急响应计划的前期准备，确立信息安全应急响应计划文档的基本要素、内容要求和格式规范。为负责制定和维护信息安全应急响应计划的人员提供指导。	制定	高		

序号	标准分类	标准中文名称	制定/修订目的	兼容方式（制定/修订/延续）	优先级	牵头单位	实施计划
27	响应恢复类	证券期货业信息安全事件分类分级指南	为信息安全事件的分类分级提供指导，用于信息安全事件的防范与处置，为事前准备、事中应对、事后处理提供一个基础指南，可供证券期货业信息系统和基础信息传输网络的运营和使用单位以及信息安全主管部门参考使用。	制定	高		
28	响应恢复类	证券期货业信息系统灾难恢复规范	用于规定证券期货业信息系统灾难恢复应遵循的基本要求。	制定	高		
29	响应恢复类	JR/T 0059-2010 证券期货经营机构信息系统备份能力标准	明确了证券期货经营机构信息系统备份能力的含义，定义了备份能力的等级。是证券期货经营机构信息系统备份能力建设的设计标准，用于指导信息系统备份能力建设工作。	延续			
30	响应恢复类	证券期货业网络安全事件应急演练指南	为证券期货业网络安全事件应急演练提供指南	制定	中		

附录 E 证券期货行业信息安全标准体系相关标准

相关标准类与证券期货行业标准化工作密切相关，是证券期货行业信息安全标准体系类目的补充。

序号	标准编号	标准名称
1	GB 17859-1999	计算机信息系统安全保护等级划分准则
2	GB/T 22239-2008	信息系统安全等级保护基本要求
3	GB/T 28448-2012	信息系统安全等级保护测评要求
4	JR/T 0071-2012	金融行业信息系统信息安全等级保护实施指引
5	JR/T 0072-2012	金融行业信息系统信息安全等级保护测评指南
6	JR/T 0073-2012	金融行业信息安全等级保护测评服务安全指引
7	GB/T 27911-2011	银行业务安全和其它金融服务金融系统的安全框架
8	GB/T 27910-2011	金融服务 信息安全指南
9	GB/T 27913-2011	用于金融服务的公钥基础设施实施和策略框架
10	GB/T 27928.1-2011	金融业务 证书管理 第 1 部分：公钥证书
11	GB/T 27912-2011	金融服务 生物特征识别 安全框架
12	JR/T 0095-2012	信息安全技术 应用安全规范
13	JR/T 0098-2012	信息安全技术 中国金融移动支付 检测规范
14	YD/T 2694-2014	移动互联网联网应用安全防护要求

序号	标准编号	标准名称
15	YD/T 2695-2014	移动互联网联网应用安全防护检测要求
16	GB/T 20272-2006	信息安全技术 操作系统安全技术要求
17	GB/T 28452-2012	信息安全技术 应用软件系统通用安全技术要求
18	GB/T 30271-2013	信息安全技术 信息安全服务能力评估准则
19	GB/T 17579-1998	信息安全技术 开放系统互连 虚拟终端基本类服务
20	GB/T 25058-2010	信息系统安全等级保护实施指南
21	GB/T 22240-2008	信息系统安全保护等级定级指南
22	GB/T 22081-2008	信息技术安全技术信息安全管理实用规则
23	GB/T 20282-2006	信息系统安全工程管理要求
24	GB/Z 20985-2007	信息安全技术 信息安全事件管理指南
25	GB/T 21052-2007	信息安全技术 信息系统物理安全技术要求
26	GB/T 25070-2010	信息系统等级保护安全设计技术要求
27	GB/T 20271-2006	信息安全技术 信息系统通用安全技术要求
28	GB/T 20270-2006	信息安全技术 网络基础安全技术要求
29	GB/T 20269-2006	信息安全技术 信息系统安全管理要求
30	GB/T 18336-2001	信息技术 安全技术 信息技术安全性评估准则

序号	标准编号	标准名称
31	GB/T 28449-2012	信息系统安全等级保护测评过程指南
32	GB/T 20984-2007	信息安全技术 信息安全风险评估规范
33	GB/T 20987-2007	信息安全技术 网上证券交易系统信息安全保障评估准则
34	GB/T 20009-2005	信息安全技术 数据库管理系统安全评估准则
35	GB/T 28450-2012	信息安全技术 信息安全管理体系审核指南
36	GB/T 20274-2008	信息安全技术 信息系统安全保障评估框架