ICS 03.060
A11
备案号

JR

中华人民共和国金融行业标准

JR/T 0099—2012

证券期货业信息系统运维管理规范

Information system operation and maintenance management specification for securities and futures industry

2013－1-31 发布　　2013－1-31 实施

中国证券监督管理委员会　发布

目　　次

前　言

本标准依据GB/T 1.1-2009给出的规则起草。

本标准由全国金融标准化技术委员会提出并归口。

本标准起草单位：中国证监会信息中心、上海证券交易所、深圳证券交易所、上海期货交易所、中国金融期货交易所、中信建投证券股份有限公司、国泰君安证券股份有限公司、海通证券股份有限公司、长城证券有限责任公司、兴业证券股份有限公司、南方基金管理有限公司。

本标准主要起草人：张野、罗凯、严少辉、黎峰、马晨、赵亮、张斗刚、支晓繁、杨威、戴晖、肖钢、黄韦、王洪涛、兰朝晖、王伟强、葛峰、张引。

证券期货行业信息系统运维管理规范

1 范围

本标准规定了证券期货业信息系统运维管理工作的要求。

本标准适用于证券期货机构，包括：承担证券期货市场公共职能的机构、承担证券期货行业信息技术公共基础设施运营的机构等证券期货市场核心机构及其下属机构（以下简称核心机构），以及证券公司、基金管理公司、期货公司、证券期货服务机构等证券期货经营机构（以下简称经营机构）。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 20269—2006 信息安全技术 信息系统安全管理要求

GB/T 22080—2008 信息技术 安全技术 信息安全管理体系 要求

GB/T 24405.1—2009 信息技术 服务管理 第1部分 规范

ISO 31000:2009 风险管理 原则和指南（Risk management -- Principles and guidelines）

3 术语和定义

下列术语和定义适用于本文件。

3.1

交易业务系统 trading business system

承载证券期货交易、结算相关的各类业务系统。按照其重要性，交易业务系统可分为核心交易业务系统和非核心交易业务系统。

3.2

核心交易业务系统 core trading business system

承载面向客户和对外服务的最基本、最核心交易业务的系统。

注：这类业务对运维保障的要求很高，一旦出现中断，将直接影响证券期货市场。如：证券公司的集中交易系统、网上交易系统、银证（第三方存管）系统、结算系统、行情系统、融资融券系统等；期货公司的集中交易系统、网上交易系统、银期转账系统、结算系统、行情系统、风控系统等；基金管理公司的注册登记系统、基金估值系统、直销与网上交易系统、投资交易系统等。

3.3

非核心交易业务系统 non-core trading business system

承载除核心交易业务外与交易业务有数据交换的其他业务的系统。

注：这类业务重要性相对较低，一旦出现中断，可能间接或不一定影响证券期货市场。如：稽核系统、呼叫中心系统、客户关系管理系统、证券公司的风控系统等。

3.4

交易业务网 trading business network

承载交易业务系统的计算机网络统称交易业务网，承载核心交易业务系统的计算机网络统称核心交易业务网，承载非核心交易业务系统的计算机网络统称非核心交易业务网。

3.5

生产环境 production environment

支持日常业务活动的基础设施、网络、主机、存储、数据库及应用等。

3.6

在线数据 online data

在生产环境中使用的所有数据。

3.7

离线数据 offline data

脱离生产环境用于存储备份的所有数据。

3.8

事件 incident

不属于某项服务的标准操作，导致或可能导致服务中断或服务质量降低的任一事态。
[GB/T 24405.1—2009，定义2.7]

3.9

问题 problem

一个或多个事件的未知的潜在原因。
[GB/T 24405.1—2009，定义2.8]

3.10

交付 delivery

负责规划、安排、控制发布的构建、测试和部署，以及在保护现有服务完整性的同时，提供业务所需新功能的流程。

3.11

关键岗位 key position

负责交易业务系统运行维护的机房管理员、系统管理员、网络管理员、数据库管理员、安全管理员等岗位。

3.12

配置项 configuration item

处于或将处于配置管理之下的基础设施部件或项。

[GB/T 24405.1-2009，定义2.4]

注：配置项在复杂性、规模和类型方面变化可能很大，配置项可以是整个系统包括所有的硬件、软件和文档，也可以是单个模块或很小的硬件部件。

3.13

风险 risk

对目标不确定性的影响。

[ISO 31000:2009，定义2.1]

3.14

技术风险 technical risk

因信息技术发展、信息系统变更、人员操作失误等导致的风险。

3.15

业务风险 business risk

因流程变化、业务发展、市场环境改变等导致的风险。

3.16

信息安全事态 information security event

信息安全事态是指系统、服务或网络的一种可识别的状态的发生，它可能是对信息安全策略的违反或防护措施的失效，或是和安全关联的一个先前未知的状态。

[GB/T 22080-2008，定义3.5]

3.17

网络与信息安全事件 network and information security incident

网络与信息安全事件是突发事件的一种，也被称为信息安全事件,一个信息安全事件由单个的或一系列的有害或意外信息安全事态组成，它们具有损害业务运作和威胁信息安全的极大可能性。

注：改写 GB/T 22080-2008，定义3.6。

3.18

敏感性 sensitivity

表征资源价值或重要性的特征，也可能包含这一资源的脆弱性。

[GB/T 20269—2006，定义3.6]

4 基本要求

4.1 运维组织

4.1.1 证券期货机构应设立信息系统运维组织，负责信息系统的运行维护工作。

4.1.2 证券期货机构应任命运维组织负责人，负责组织、协调、管理信息系统的运行维护工作。

4.1.3 证券期货机构应合理设置运维岗位，规定岗位职责及技能要求，并符合如下要求：

a) 运维岗位应至少包括机房管理员、网络管理员、系统管理员、数据库管理员、安全管理员等关键岗位，并设置主备岗；

b) 关键岗位应进行分离，兼岗时应满足岗位相互制约的要求。

4.1.4 证券期货机构应配备足够的运维人员。运维人员应具备一定的计算机基础理论知识和专业技术经验。经营机构运维人员应具有相应的从业资格。

4.1.5 证券期货机构应与运维人员签署保密协议，保密协议应至少包括保密范围、保密期限等内容。

4.1.6 证券期货机构应制定年度培训计划，对运维人员进行必要的技术、业务、安全等培训，并留存培训记录。

4.2 经费管理

4.2.1 证券期货机构应制定信息系统运行维护年度预算计划，每年进行核算。预算和核算应接受监督和审计。

4.2.2 证券期货机构应将信息系统运行维护的各项费用纳入预算管理。费用至少应包括：机房物理环境、信息系统软硬件、网络与通信设施的使用费和维修费，以及应急保障费用、技术服务费用、人员培训费用等。

4.3 制度和流程管理

4.3.1 证券期货机构应制定覆盖运维工作各个环节的、体系化的运维管理制度和操作流程。运维管理制度应包括但不限于：机房管理、网络与系统管理、数据和介质管理、交付管理、测试管理、配置管理、安全管理、值班管理、监控管理、文档管理、设备和软件管理、供应商管理、关联单位关系管理、检查审计等制度。运维操作流程应包括但不限于日常操作、事件处理、问题处理、系统变更、应急处置等流程。

4.3.2 证券期货机构应建立运维管理制度和操作流程的制定、发布、维护和更新的机制。至少每年一次评审、修订运维管理制度和操作流程。

4.4 文档管理

4.4.1 证券期货机构应建立文档管理制度，对文档的分类、命名规则、编写人、审批人、版本、敏感性标识、发布时间、存放方式、修订记录、废止等做出规定。

4.4.2 证券期货机构应明确文档管理的责任人。

4.4.3 证券期货机构应对运维过程中涉及的各类文档进行分类管理，可按照制度文档、技术文档、合同文档、审批记录、日志记录等进行分类，并统一存放。

4.4.4 证券期货机构应规范文档的发布管理，对文档的版本应当进行控制。文档应标识敏感性、使用范围、使用权限、审批权限等。文档在使用时应能读取、使用最新版本，防止作废文件的逾期使用。

4.4.5 证券期货机构对超范围、超权限使用文档时应保存相关审批、使用记录。

4.5 设备和软件管理

4.5.1 证券期货机构应建立计算机相关设备和软件管理制度，对设备和软件的验证性测试、出入库、安装、盘点、维修（升级）、报废等进行规范。

4.5.2 证券期货机构应明确设备和软件管理责任人。

4.5.3 证券期货机构应在设备和软件投入使用前进行必要的验证性测试，并保留测试记录。

4.5.4 证券期货机构应编制信息系统设备清单，主要包括设备名称、设备编号、入库时间、设备主要参数、设备序列号、设备状态、设备保修期、设备位置、设备用途和设备使用责任人等内容，并保留设备启用、转移、维修、报废等过程的记录。

4.5.5 证券期货机构应使用正版软件并保存软件授权证书和许可协议，应编制软件清单，主要包括软件名称、软件编号、入库时间、软件版本，授权和许可情况、软件序列号、软件状态、软件维护期、软件安装设备、用途和使用责任人等内容，并保留软件启用、转移、升级、报废等过程的记录。

4.5.6 证券期货机构应对设备进行标识，标识应放在设备明显位置。

4.5.7 证券期货机构应规定设备和软件的使用年限，定期进行盘点，并对设备状态进行评估和更新。

4.5.8 证券期货机构应对外送设备的维修进行严格管理，防止数据泄露。

4.5.9 证券期货机构应对拟下线和拟报废设备的存储介质中的全部信息进行清除或销毁。对正式下线设备和软件交指定部门统一管理、保存或处置，并保留相应记录。设备和软件报废应符合资产管理规定。

4.6 供应商管理

4.6.1 证券期货机构应建立供应商管理制度，对供应商支持运维服务的相关活动进行统一管理。

4.6.2 证券期货机构应在与供应商签订的合同中明确其应承担的责任、义务，并约定服务要求和范围等内容。

4.6.3 证券期货机构应与供应商签署保密协议，不得泄露所服务机构的保密信息，并要求供应商签署承诺书，承诺产品不存在恶意代码或未授权的功能，不提供违反我国法律法规的功能模块，并符合证券期货行业有关技术规范和技术指引。

4.6.4 证券期货机构应在涉及证券期货交易、行情、开户、结算等软件产品或技术服务的采购合同中，明确供应商应接受证券期货行业监管部门的信息安全延伸检查。

4.6.5 证券期货机构应定期收集、更新供应商信息，组织对供应商的服务质量、合同履行情况、人员工作情况等内容进行评价，形成评价报告，并跟踪和记录供应商改进情况。

4.6.6 证券期货机构应加强运维外包服务管理，主要包括：

a) 与外包公司及外包人员签订保密协议；
b) 明确外包公司应当承担的责任及追究方式；
c) 明确界定外包人员的工作职责、活动范围、操作权限；
d) 对外包人员工作情况进行监督和检查，并保留相应记录；
e) 对驻场外包人员的入场和离场进行管理；
f) 定期评估外包的服务质量；
g) 制定外包服务意外终止的应急措施。

4.7 关联单位关系管理

4.7.1 证券期货机构应建立关联单位联系制度。关联单位包括证券期货行业监管部门、协会，当地政府部门，公安机关，交易所等市场核心机构，其他证券期货经营机构，银行机构，电力和通信设施保障机构，软硬件供应商，技术服务商和物业公司等。

4.7.2 证券期货机构应建立关联单位联系表，表的内容至少包括单位名称、业务事项、联系人、联系方式、备注等，并及时更新。

4.8 督促检查

4.8.1 证券期货机构应建立检查审计制度，对运维制度的执行情况和运维工作开展情况定期进行检查和审计，以督促运维工作持续改进。

4.8.2 证券期货机构应指定人员负责对日常操作执行情况进行每日检查，确保运维管理制度和操作流程有效执行。

4.8.3 证券期货机构应每季组织开展内部检查，形成检查报告。

4.8.4 证券期货机构应在每年审计工作中包含信息系统运维管理工作审计项目，并形成审计报告。

4.8.5 检查和审计范围至少包括对运维管理制度和操作流程的合理性和完整性进行评估，对运维管理制度和操作流程的执行情况进行评估，对文档、配置、数据的有效性进行评估，对整体安全状况进行评估，对运维人员履职能力进行评估等。

4.8.6 证券期货机构应对检查和审计的结果采取纠正性和预防性的措施。

5 运行保障

5.1 运维值班管理

5.1.1 证券期货机构应建立运维值班管理制度，对日常操作、监控管理、事件处理、问题处理、数据和介质管理、机房管理、安全管理、应急处置进行规范。

5.1.2 证券期货机构应指定运维值班负责人。运维值班负责人负责日常操作的部署、检查、风险控制、业务衔接等工作。运维值班负责人应有备岗。主备岗不得同时离岗。

5.1.3 证券期货机构应制定运维值班安排表，可根据实际情况实施倒班制度。在值班期间值班人员不得擅离岗位。

5.1.4 证券期货机构应制定交接班流程，并严格执行，留存记录。

5.1.5 证券期货机构应设置运维值班电话，并保持畅通。

5.2 日常操作

5.2.1 证券期货机构应制定操作手册。操作手册的内容应至少包括信息系统日常运行操作的各个环节。针对各个操作环节制定操作规程。

5.2.2 交易业务系统的操作规程应至少包括操作的对象、时间、步骤、指令、操作要点、复核要点、操作人、复核人等基本要素。

5.2.3 证券期货机构应严格按照操作手册执行运维操作，对交易业务系统的操作过程应进行记录留痕，记录的保存时间不少于一年。

5.2.4 特殊操作、临时操作应经批准后方可双岗执行。操作过程应进行记录留痕，记录的保存时间不少于一年。

5.2.5 证券期货机构应依据业务、信息系统的变化对操作手册及规程进行及时修订，经审批通过后遵照执行。

5.2.6 证券期货机构应对核心交易业务系统设置独立的操作和监控环境，并与开发、测试等其他操作环境严格分离。

5.3 监控分析

5.3.1 证券期货机构应采取监控措施，配备监控和报警工具，对影响信息系统正常运行的关键对象，包括机房环境、网络、通信线路、主机、存储、数据库、核心交易业务相关的应用系统、安全设备等进行监控。报警方式可包括声光、电话、短信、邮件等。

5.3.2 证券期货机构应采取人工值守和自动化工具相结合的方式，对交易业务系统进行 24 小时监控。交易时段应指定人员对交易业务系统进行监控，交易时段以外如无法做到人工监控，应开启自动监控系统和自动报警系统。

5.3.3 证券期货机构应建立辅助的人工巡检制度，规定巡检内容、频度、人员等。巡检内容应覆盖电力、空调、消防、安防等机房设施，主机、网络、通信、安全等设备的运行状况。巡检结果应及时记录，如遇异常应及时处理，并按规定要求进行报告。

5.3.4 证券期货机构应正确设置自动化监控工具的预警阈值，并定期进行检查和评估。

5.3.5 主要监控指标具体如下：

a) 机房：电力状态、空调运行状态、消防设施状态、温湿度、漏水、人员及设备进出等；
b) 网络与通信：设备运行状态、中央处理器使用率、通信连接状态、网络流量、核心节点间网络延时、丢包率等；
c) 主机：设备运行状态、中央处理器使用率、内存利用率、磁盘空间利用率、通信端口状态等；
d) 存储：设备运行状态、数据交换延时、存储电池状态等；
e) 安全设备：设备运行状态、中央处理器使用率、内存利用率、端口状态、数据流量、并发连接数、安全事件记录情况等；
f) 数据库：日志信息、表空间使用率、连接数等；
g) 核心交易业务相关的应用系统：进程的活动状态、日志信息、中央处理器使用率、内存利用率、并发线程数量、并发处理量、关键业务指标等；
h) 门户网站：网页内容、日均访问量等。

5.3.6 证券期货机构应针对不同系统设置合理的监测频度。

5.3.7 证券期货机构应记录并集中分类存储必要的操作日志、系统日志、应用日志、安全日志等，留存日志应满足审计的需要。

5.3.8 证券期货机构应保存监控产生的日志，保存时间不少于一年。

5.3.9 证券期货机构应每日分析核心交易业务系统监控日志及巡检记录，形成评估记录，跟踪处理日志分析中发现的异常事件。应至少每季度全面评估监控日志和操作记录，分析异常情况，形成评估报告。

5.4 数据与介质管理

5.4.1 证券期货机构应建立信息系统数据管理制度，对在线和离线数据的使用、备份、存放、保护及恢复验证等活动进行规范。

5.4.2 证券期货机构应明确数据管理责任人，负责数据的收集、使用、备份、检查等策略的制定和执行工作。

5.4.3 证券期货机构应按照国家和监管部门的有关要求，制定数据备份及验证策略，明确备份范围、备份方式、备份频度、存放地点、存放时限、有效性验证方式和管理责任人。

5.4.4 在线数据管理，应做到如下要求：

a) 交易业务系统数据应至少每交易日备份一次；
b) 交易业务系统历史数据至少保留一年；
c) 未经授权不得访问、复制；
d) 对数据的修改应通过审批，双岗操作并记录操作日志。

5.4.5 离线数据管理，应做到如下要求：

a) 离线数据不得更改；
b) 应至少每季度对核心交易业务系统的备份数据进行一次有效性验证，如发现问题应采取措施修复备份数据，并查明原因；
c) 离线数据的调阅、复制、传输、查询，应按照拟定的流程办理审批手续，并进行登记；
d) 备份数据带离存储环境时应采取必要的安全措施。

5.4.6 在线数据和离线数据用于非生产环境时，应进行脱敏处理；用于模拟测试时如无法进行脱敏处理，测试环境应采取与生产环境相当的安全措施。

5.4.7 证券期货机构应建立介质管理制度，对介质的存放、使用、维护和销毁等活动进行规范。

5.4.8 证券期货机构应明确责任人，对介质的使用、转储、送修、销毁及存储环境进行管理。

5.4.9 介质管理，应做到如下要求：

a) 应在安全环境中存放介质，并采取控制和保护措施；
b) 离线备份介质应当在本地机房、同城、异地安全可靠存放；
c) 应对介质在物理传输过程中的打包、交付进行控制；
d) 应根据所承载数据和软件的重要程度对介质进行分类和标识管理，并对介质进行归档登记，对存档介质依目录清单定期核对；
e) 涉及敏感信息的介质送修时应由专人全程陪同，并保证修复过程可控；
f) 介质销毁前应清除介质中的敏感数据；涉密信息的存储介质不得自行销毁，应按国家相关规定另行处理；
g) 在交易业务网使用的移动介质应专网专用，不得接入可以访问互联网的主机。

5.5 机房管理

5.5.1 证券期货机构应建立机房管理制度，对机房环境，供电、空调、消防、安防等基础设施的运行维护，设备和人员出入，机房工作人员等进行规范管理。

5.5.2 证券期货机构应指定机房管理负责人。

5.5.3 证券期货机构应确保机房环境整洁和安全，包括：

a) 应定期检查防水、防雷、防火、防潮、防尘、防鼠、防静电、防电磁辐射等措施的有效性；
b) 应保持机房环境卫生，采取防尘措施，定期进行除尘处理；
c) 交易时间内不得进行机房施工、保洁操作。

5.5.4 证券期货机构应加强用电安全管理。至少包括：

a) 机房管理员应根据国家有关规定和标准进行用电管理，应重点保障核心交易业务系统用电安全。
b) 机房管理员应掌握常规用电安全操作和知识，了解机房内部供电、用电设备的操作规程，掌握机房用电应急处理步骤、措施和要领。有条件的可配备专业电工或与相关电力机构或物业机构签署服务协议；
c) 应在危险性高的位置张贴相应的用电安全操作方法、警示及指引；
d) 应每季度至少一次对机房供配电、备用电源系统进行全面检查和维护管理，及时更换老化的电路元件及线缆，应定期测试备用供电系统，确保持续供电设施的有效性，并保存相关检查和维护记录；
e) 未经审批不得接入其它用电设备。

5.5.5 证券期货机构应每季度至少一次对空调设备进行全面检查和维护，保存维护记录。

5.5.6 证券期货机构应制定符合国家规范的机房消防安全管理制度，至少包括：

a) 机房工作人员应熟悉逃生路线和自我保护措施，防止发生人身安全意外；

b) 应将消防安全警示和指示张贴于机房明显位置，将消防设施的操作要点张贴于消防设施旁边；
c) 机房工作人员应熟悉消防设施及操作要点，掌握消防应急措施；
d) 应每季度至少一次对机房内消防报警设备进行检查，保证其有效性；
e) 应定期进行消防设施的使用培训和演习。

5.5.7 证券期货机构应对设备和人员出入进行严格管理，包括：
a) 应指定人员负责控制、鉴别和记录设备和人员的进出情况，记录进出人员、进出时间、工作内容，并留存记录至少 90 天；
b) 机房出入口的监控录像至少保存 90 天；
c) 外来人员进入机房应经过申请和审批流程，并限制和监控其活动范围，并有专人陪同；
d) 外来设备未经批准不得接入生产环境。

5.6 网络与系统管理

5.6.1 证券期货机构应建立网络与系统管理制度，对网络、系统的运行维护进行规范。

5.6.2 证券期货机构网络管理应包括：
a) 应合理设置安全域，绘制网络拓扑图，并保持更新；
b) 应定期检查安全隔离情况，确保各安全域之间有效隔离；
c) 应保持网络设备的可用性，及时维修、更换故障设备；
d) 应负责网络系统的参数配置、调优；
e) 应定期对系统容量进行检查和评估，形成评估报告；
f) 应定期检查网络设备的用户、口令及权限设置的正确性；
g) 应定期对整个网络连接进行检查，确保所有交换机端口处于受控状态；
h) 应对网络信息点进行管理，编制信息点使用表，并及时维护和更新，确保与实际情况一致。计算机网络跳线应整齐干净，跳线标识清晰；
i) 应制定网络访问控制策略，应合理设置网络隔离设施上的访问控制列表，关闭与业务无关的端口；编制文档并保持更新；访问控制策略的变更应履行审批手续。

5.6.3 证券期货机构系统管理应包括：
a) 应保持系统的可用性，及时维修、更换故障设备和更新软件；
b) 应负责应用系统、操作系统的参数配置、调优，编制文档并保持更新；
c) 应定期对系统容量进行检查和评估，形成评估报告；
d) 应负责管理系统和应用程序服务进程，并关闭与业务无关的服务；
e) 应定期检查应用系统、操作系统的用户、口令及权限设置的正确性。

5.6.4 证券期货机构数据库管理应包括：
a) 应保持数据库的可用性，及时维护、更新软件；
b) 应负责数据库的参数配置、调优，编制文档并保持更新；
c) 应定期对数据库容量进行检查和评估，形成评估报告；
d) 应负责管理数据库、表、索引、存储过程，数据库的升级、优化、扩容、迁移；
e) 应定期检查数据库的用户、口令及权限设置的正确性。

5.6.5 证券期货机构用户和口令管理应符合如下要求：
a) 不得设置弱口令，若系统条件允许，口令应采用数字、字母、符号混排且无规律的方式，管理员口令长度原则上不低于 12 位；核心交易业务系统应提示并阻止用户使用弱口令登录；
b) 应每季度对管理员口令进行修改，更新的管理员口令至少 5 次内不能重复；
c) 应用系统的账户及口令应采用加密方式存储、传输；加密产品的使用应符合国家有关规定；

d) 应重点加强对匿名/默认用户的管理，防止被非法使用；
e) 应及时注销不再使用的账户；
f) 应明确责任人，负责统一保管、安全存放管理员口令，不得泄漏。

5.6.6 证券期货机构权限管理应包括如下要求：
a) 权限分配应履行审批手续，权限设置后应复核；
b) 应按照最小安全访问原则分配用户权限；
c) 应建立权限分配表，对用户的访问权限进行合理分配，对文件系统访问权限进行合理设置，编制文档并保持更新；
d) 应在用户账户变化时，同时变更或撤销其权限；
e) 应定期检查权限设置的有效性。

5.7 安全管理

5.7.1 证券期货机构应建立安全管理制度，覆盖安全策略的制定、实施、检查、评估、改进等全过程。

5.7.2 证券期货机构应指定专人担任安全管理员，负责信息安全管理工作；在自身能力不足的情况下，可外聘安全机构协助完成。

5.7.3 证券期货机构应采取安全防护措施，包括：
a) 应对所有服务器和终端设备安装防木马、病毒软件，建立统一病毒和木马防护机制。因故不能安装防病毒软件的，应采取其他等效的安全防护措施；
b) 应在充分评估的基础上，对所有服务器和终端设备进行补丁升级；补丁升级前进行测试验证；
c) 应综合运用防火墙、入侵检测等安全设备，保护网络与系统；应正确设置安全设备的接口参数和过滤规则；
d) 应对新上线的设备在接入运行网络前进行全面的安全检查；
e) 应采取限制 IP 登录等手段，控制对交易业务主机、主干网络设备、安全设备等的访问；
f) 原则上不得通过互联网对防火墙、网络设备、服务器进行远程管理和维护，特殊紧急情况下应采取限制登录 IP、数字证书或动态口令认证、全程监控等措施，在操作完成后应及时关闭，并对维护过程进行监控并留存记录；
g) 原则上不得在交易时段对交易业务网的网络设备、安全设备、系统设备进行更换或变更配置；
h) 原则上不允许通过无线网络对交易业务网进行网络管理；
i) 应设置抵御连续猜测等对客户账户恶意攻击行为的策略；
j) 应对门户网站建立防篡改机制，防止网页内容、可下载的客户端软件等被未经授权的修改；
k) 门户网站不得存放客户资料、交易数据等客户敏感数据；

5.7.4 证券期货机构应定期进行安全检查，包括：
a) 应定期对服务器进行全面病毒扫描，但不得在交易时段内进行；
b) 应建立定期扫描并修补漏洞的工作机制，定义扫描检测的内容和程序，明确漏洞扫描工具和扫描频率，记录扫描结果及处理情况；
c) 应按规定开展信息系统安全等级保护自查或测评；

5.7.5 对证券期货行业内通报的重大安全隐患，应立即进行专项安全检查。

5.7.6 证券期货机构应对安全检查情况进行评估，形成评估报告。

5.7.7 证券期货机构安全管理员应督促解决检查、测评、评估中发现的风险隐患。

5.8 事件与问题管理

5.8.1 证券期货机构应建立事件管理流程，对信息系统运维事件的处理进行规范。

5.8.2 证券期货机构应指定人员负责设计和管理事件的记录、分级、分派、处理、监控和结束整个流程。

5.8.3 证券期货机构应记录运维过程中发生的所有事件，根据事件的影响程度和影响范围评估事件处理优先级及时处理。

5.8.4 证券期货机构应对所有事件响应、处理、结束等过程进行跟踪、督促及检查。

5.8.5 证券期货机构应每月回顾、分析事件处理记录，完成事件分析报告。

5.8.6 证券期货机构应将运维过程中重复发生的事件、重大事件纳入问题管理。

5.8.7 证券期货机构应建立问题管理制度，对运维活动中发现的问题进行根本解决，并建立问题库。

5.8.8 证券期货机构应对问题的处理过程进行跟踪和管理，包括问题的识别、提交、分析、处理、升级、解决、结束。

5.8.9 证券期货机构应将监控、分析、自查、检查、测评、评估和事件处理中发现的问题进行汇总，并纳入问题库。

5.8.10 证券期货机构应组织对问题进行分析、提出解决方案、通过变更管理审批后部署实施，并将解决过程归纳整理并纳入问题库。

6 系统维护

6.1 交付管理

6.1.1 证券期货机构应建立交付流程，对建成的信息系统交付运行维护的活动进行规范。

6.1.2 证券期货机构应制定交付工作清单，作为双方交付依据，清单包括信息系统相关的软件、硬件、技术文档、管理手册、使用手册、培训材料、相关工具、协议和合同等。

6.1.3 证券期货机构应对运维人员和所涉及的相关各方进行培训和说明，包括交付事项的目的、范围、背景、测试要求、上线实施要求、验收要求、运维要求等。

6.1.4 证券期货机构应制定交付实施计划，划定交付双方的职责，交付的步骤，并对交付过程留存记录。

6.2 系统测试

6.2.1 证券期货机构应建立系统测试流程，对系统上线前进行的模拟环境测试和生产环境测试进行规范。

6.2.2 证券期货机构应为系统测试配备必要的人员和设备资源，需要时应协调关联单位配合测试。

6.2.3 证券期货机构应根据系统上线要求制定测试方案，确定采用的测试方法和测试流程。测试方案及测试用例应覆盖功能、性能、容量、安全性、稳定性等方面。测试完成后应对测试结果进行分析评估，并给出测试报告。

6.2.4 模拟环境测试的要求如下：

a) 应建立独立的模拟环境。模拟环境应在逻辑架构上和生产环境一致。模拟环境应与生产环境进行分离，不得对生产环境进行干扰；

b) 应根据测试方案的设计，合理配置测试所需的设备，识别设备不同可能带来的测试结果正确性风险；

c) 可根据需要，要求生产系统运维人员和业务部门组织业务人员参与测试；

d) 模拟环境使用的密码应与生产系统严格区分，系统管理员宜由不同的人员担任。

6.2.5 生产环境测试的要求如下：

a) 测试前应备份当前系统的数据和配置；

b） 应提前发布系统测试公告；
c） 应由生产系统运维人员在生产环境下组织完成；
d） 应根据需要，要求业务部门组织业务人员参与测试；
e） 根据测试的结果设计系统升级过程及应急预案；
f） 如果测试内容涉及其他相关系统，应协调其他系统用户参与测试；
g） 涉及核心交易业务系统的上线测试，应组织全市场或全公司各相关部门测试；
h） 测试后应恢复生产环境并验证恢复的有效性；
i） 交易时段不得使用生产环境进行测试。

6.3 系统变更

6.3.1 证券期货机构应建立系统变更流程，对信息系统的变更活动进行规范。
6.3.2 证券期货机构应明确系统变更中的角色，至少包括：申请人、审批人、实施人、复核人。
6.3.3 变更申请人应提交正式的变更申请，申请中应有明确的变更方案，内容至少包括：目标、对象、时间、人员、紧急程度、操作步骤、测试方案、实施方案、风险防控措施、应急预案、回退方案等。
6.3.4 变更审批人应在充分评估变更的技术风险和业务风险的基础上进行审批，审批记录应留痕并满足审计需要。
6.3.5 变更审批人应确定变更实施时间窗口，除紧急变更外，不得在交易时段进行变更实施。
6.3.6 应按照测试方案，组织变更前后的测试，测试后应提交测试记录或报告。
6.3.7 变更实施人应按照变更实施方案进行变更，并及时更新配置库。
6.3.8 变更复核人应对变更记录和变更结果进行评估，评估内容应至少包括变更目标的达成情况、对生产环境的影响、配置库更新情况。

6.4 配置管理

6.4.1 证券期货机构应制定配置管理流程，明确配置管理负责人。
6.4.2 证券期货机构应建立配置库，对交易业务系统的服务器、存储、网络、安全设备，操作系统、应用软件、数据库等进行管理。
6.4.3 证券期货机构应合理设置配置库中配置项的属性，要求如下：

a） 配置项属性至少包括编号、名称、描述、维护责任人、运行状态、关联关系等；
b） 配置项编号应唯一；
c） 配置项的添加、修改、替换、删除应有变更记录；
d） 应保存配置项历史记录，确保与事件管理、问题管理、变更管理等流程记录的关联性。

6.4.4 证券期货机构应定期对配置库进行备份。
6.4.5 证券期货机构应及时检查并定期审计配置库，对发现的不一致情况及时纠正，并留存记录。

7 应急管理

7.1 应急准备

7.1.1 证券期货机构应建立健全网络与信息安全事件应急处置组织体系，明确网络与信息安全事件的应急指挥决策机构和执行机构，负责网络与信息安全事件的预防预警、应急处置、报告和调查处理工作。
7.1.2 证券期货机构网络与信息安全事件应急处置指挥决策机构应由主要领导负责，成员包括但不限于业务、技术、风险控制、结算、财务、客服、安保及综合等有关部门的负责人。

7.1.3 证券期货机构应明确网络与信息安全事件应急决策机制，以及决策递补顺序，确保各种情况下，有人负责决策和报告。

7.1.4 网络与信息安全事件应急管理应遵循“谁主管谁负责、谁运行谁负责”，“统一指挥、密切协同；注重预防、减少风险；科学处置、及时报告；以人为本、公平优先”的原则。

7.1.5 证券期货机构应制定网络与信息安全事件应急预案，内容至少包括：

a) 应急预案编制的目的和依据；
b) 应急预案的适用范围；
c) 应急处置的组织体系及职责；
d) 预防措施、保障措施与应急准备；
e) 预警监测、处置和信息报送；
f) 网络与信息安全事件的分级分类；
g) 网络与信息安全事件的报告流程；
h) 网络与信息安全事件处置的一般原则；
i) 网络与信息安全事件处置的具体方案；
j) 网络与信息安全事件内部调查处理以及分析总结的要求。

7.1.6 应急预案应符合如下要求：

a) 网络与信息安全事件处置的具体方案应包括各种可能发生的技术故障的应急处置流程、报告流程等；
b) 应针对各种技术故障拟定统一的解释口径和通知公告模板；
c) 应每年至少进行一次评估，并及时修订；
d) 应根据应急演练的情况进行评估和更新；
e) 核心机构应向中国证监会报备；经营机构应向住所地证监局报备；
f) 在应急预案发生重大变化时，应及时重新报备。

7.1.7 应急准备应符合如下要求：

a) 值班负责人和信息技术负责人应负责信息安全应急值守；
b) 系统管理员、网络管理员、数据库管理员、安全管理员等关键岗位应熟练掌握应急预案，能有效处置网络与信息安全事件；
c) 在自身力量不足以满足应急要求的情况下，应与相关单位签订通信、消防、电力设备、空调设备、软硬件产品、安全服务等的应急响应及服务保障协议。协议内容应包括双方联系人、联系方式、服务内容及范围、应急处理方式等。应定期检查和评估协议的执行情况，确保服务保障措施落实到位，确保在应急处置中相关单位能提供及时有效的技术支持；
d) 应建立有效的应急通讯联络系统，确保信息畅通；
e) 应制定应急处置联络手册，明确详细的联络方式，并及时更新，在发生变化时及时通知相关单位。应急处置联络手册至少包括应急处置组织体系及相关关联单位的应急联络方式；
f) 应指定通报联络人，明确联络方式。通报联络人至少包括信息技术负责人及其备岗。通报联络方式至少包括应急值守电话与传真。应将通报联络人及其联络方式及时通知监管部门、行业协会和相关单位；
g) 应实行 7×24 小时联络制度，通报联络人必须保持应急值守电话可用；
h) 应对本单位有关领导和员工定制应急工作卡片，明确有关领导和员工在网络与信息安全事件应急处置中的关键任务、主要的应急联络人和联络方式；
i) 应准备信息系统技术资料和软件备份。至少包括网络拓扑图、设备配置参数、各种系统软件和应用程序、安装使用手册、应急操作手册等；

j） 应准备充足的重要设备备品配件，并进行定期评估、检测和维护；
k） 应事先储备一定数量的通讯、消防、应急照明等应急设备或物资并定期盘点，对于有时效性的应急物资应做到及时更新；
l） 应准备应急保障资金，确保应急处置中能及时采购应急设备或物资。

7.1.8 应急演练应符合如下要求：
a） 应根据应急预案的内容，制定详细的应急演练计划。计划至少包括演练的目的、内容、时间、参与方、方式、前期准备情况、统计与记录要求、系统恢复与验证要求等内容；
b） 每半年应至少组织一次网络与信息安全应急演练；
c） 应记录演练情况，演练记录至少保存两年；
d） 应对演练中发现的问题进行改进；
e） 核心机构应每年向中国证监会报告年度应急演练情况；经营机构应每年向住所地证监局报告年度应急演练情况。

7.1.9 应急培训应符合如下要求：
a） 应定期开展应急培训；
b） 培训内容应包括应急预案、证券期货业信息安全应急处置的有关规定。

7.2 应急处置

7.2.1 证券期货机构应在发现可能导致异常的风险隐患时，尽快加以核实，立即采取必要的防范措施，如有重要情况应按照有关规定进行预警报告。解除预警后，按相同路径进行报告。

7.2.2 证券期货机构应在发生网络与信息安全事件后，立即启动应急预案，迅速采取应急措施，尽快恢复信息系统正常运行。

7.2.3 证券期货机构应在应急处置中注意保证工作人员的人身安全。

7.2.4 证券期货机构应在应急处置结束前，保证专人 24 小时值班。

7.2.5 应急处置人员应保持联系方式畅通，及时向有关方面通报事件处置进展情况。

7.2.6 证券期货机构应及时向投资者说明事件的真实情况，引导投资者采取应急措施，取得投资者的理解与配合，配合媒体的采访报道。

7.2.7 证券期货机构应做好应急处置的相关记录，保留有关证据。

7.2.8 证券期货机构应在网络与信息安全事件发生后，按有关规定报告事件情况，并保持持续报告，直至系统恢复正常运行，报告要素应完备、及时、准确，不得迟报、漏报、谎报或瞒报。

7.3 调查处理

7.3.1 证券期货机构应建立事故调查处理机制，在网络与信息安全事件应急处置结束后，进行内部调查、责任追究和采取整改措施，并形成事件总结报告。

7.3.2 证券期货机构应按照有关规定报送事件总结报告。暂时无法确定事件原因、责任和结论的，应先给出事件的初步分析判断，并组织力量尽快查找原因，认定事件责任，给出事件结论，采取整改措施，追究责任，并提交补充报告。

7.3.3 证券期货机构应积极配合监管部门和相关单位组织的事件调查工作，如实说明情况，提供证据，不得拒绝、阻碍、干扰调查和取证工作。

参 考 文 献

[1] GB/T 22081—2008 信息技术 安全技术 信息安全管理实用规则
[2] GB/T 24405.2—2009 信息技术 服务管理 第2部分 实践规则
[3] JR-T 0059—2010 证券期货经营机构信息系统备份能力标准
[4] JR-T 0060—2010 证券期货业信息系统安全等级保护基本要求（试行）
[5] JR-T 0067—2011 证券期货业信息系统安全等级保护测评要求（试行）