ICS 03.060
A 11

JR

中华人民共和国金融行业标准

JR/T 0146.5—2016

证券期货业信息系统审计指南
第5部分：证券公司

Securities and futures industry audit guideline for information system —

Part5: Securities companies

2016-11-08 发布　　2016-11-08 实施

中国证券监督管理委员会　发布

目　　次

前言 II
1　范围 1
2　规范性引用文件 1
3　术语和定义 1
4　信息系统审计概述 2
附录A（规范性附录）　信息技术治理审计底稿 4
附录B（规范性附录）　机房管理审计底稿 25
附录C（规范性附录）　网络管理审计底稿 35
附录D（规范性附录）　运维管理审计底稿 48
附录E（规范性附录）　信息系统安全等级保护相关工作审计底稿 69
附录F（规范性附录）　软件正版化审计底稿 74
附录G（规范性附录）　集中交易系统审计底稿 78
附录H（规范性附录）　网上信息系统审计底稿 108
附录I（规范性附录）　第三方存管系统审计底稿 144
附录J（规范性附录）　重要信息系统审计底稿 173
附录K（规范性附录）　A型营业部审计底稿 200
附录L（规范性附录）　B型营业部审计底稿 210
附录M（规范性附录）　C型营业部审计底稿 220
附录N（规范性附录）　信息系统托管审计底稿 223
附录O（规范性附录）　信息系统调查表 259

前　言

JR/T 0146-2016《证券期货业信息系统审计指南》标准按适用对象分为以下7部分：

——第 1 部分：证券交易所；

——第 2 部分：期货交易所；

——第 3 部分：证券登记结算机构；

——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。

本部分为JR/T 0146.5-2016《证券期货业信息系统审计指南》的第5部分。

本部分按照GB/T 1.1-2009给出的规则起草。

本部分由全国金融标准化技术委员会(SAC/TC180）提出并归口。

本部分起草单位：中国证券监督管理委员会信息中心、中国证券监督管理委员会会计部、中国证券监督管理委员会纪委监察局，上海证券交易所、深圳证券交易所、上海期货交易所、郑州商品交易所、大连商品交易所、中国金融期货交易所、中国证券登记结算有限责任公司、中国证券投资者保护基金有限责任公司、中国证券金融股份有限公司、中国期货市场监控中心有限责任公司、中证资本市场运行统计监测中心有限责任公司、全国中小企业股份转让系统有限责任公司、中证信息技术服务有限责任公司，深圳证券通信有限公司、上海期货信息技术有限公司、大连飞创信息技术有限公司、国泰君安证券股份有限公司、海通证券股份有限公司。

本部分主要起草人：张野、刘铁斌、王东明、陈炜、陈建斌、金浦芳、蒲晓明、龚定贵、陈国红、王欣、吕德旭、焦东亮、丛日权、吴忠华、马维杰、孙立、周桉、黄韦、徐楠、李毅、吴宁、朱家根、赵明、颜梦、李杰、杜佳铠、郭赫然。

证券期货业信息系统审计指南
第5部分：证券公司

1 范围

本部分给出了证券公司开展信息系统审计的实施指南。

本部分适用于中华人民共和国境内设立的证券公司及下属公司开展信息系统审计工作。

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。本标准将根据规范性引用文件的最新版本定期更新并发布。

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）

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）

JR/T 0099—2012 证券期货业信息系统运维管理规范

JR/T 0112—2014 证券期货业信息系统审计规范

JR/T 0133—2015 证券期货业信息系统托管基本要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

审计底稿 information system audit manuscript

对获取的相关审计证据，实施的审计程序，以及得出的审计结论作出的记录。

3.2

审计程序 audit procedure

在具体的审计过程中采取的行动和步骤。

3.3

审计结论 audit conclusion

在具体的审计过程中提出的应由被审计单位执行的审计建议和审计意见或决定。

3.4

审计证据 audit evidence

审计部门和审计人员获取的，用以证明审计事实真相，形成审计结论的证明材料，包括相关制度、日志文件、配置文件、运维记录、测评报告、商业合同、各种统计数据等。

4 信息系统审计概述

4.1 总则

信息系统审计框架由三部分构成：审计输入、审计过程和审计输出。

审计输入包括JR/T 0112-2014的附录A、附录B、附录C。过程组件为一组与输入组件中所标识的安全控制相关的特定审计对象和审计方法，输出组件包括一组由审计人员使用的用于确定安全控制有效性的程序化陈述。图1给出了框架。

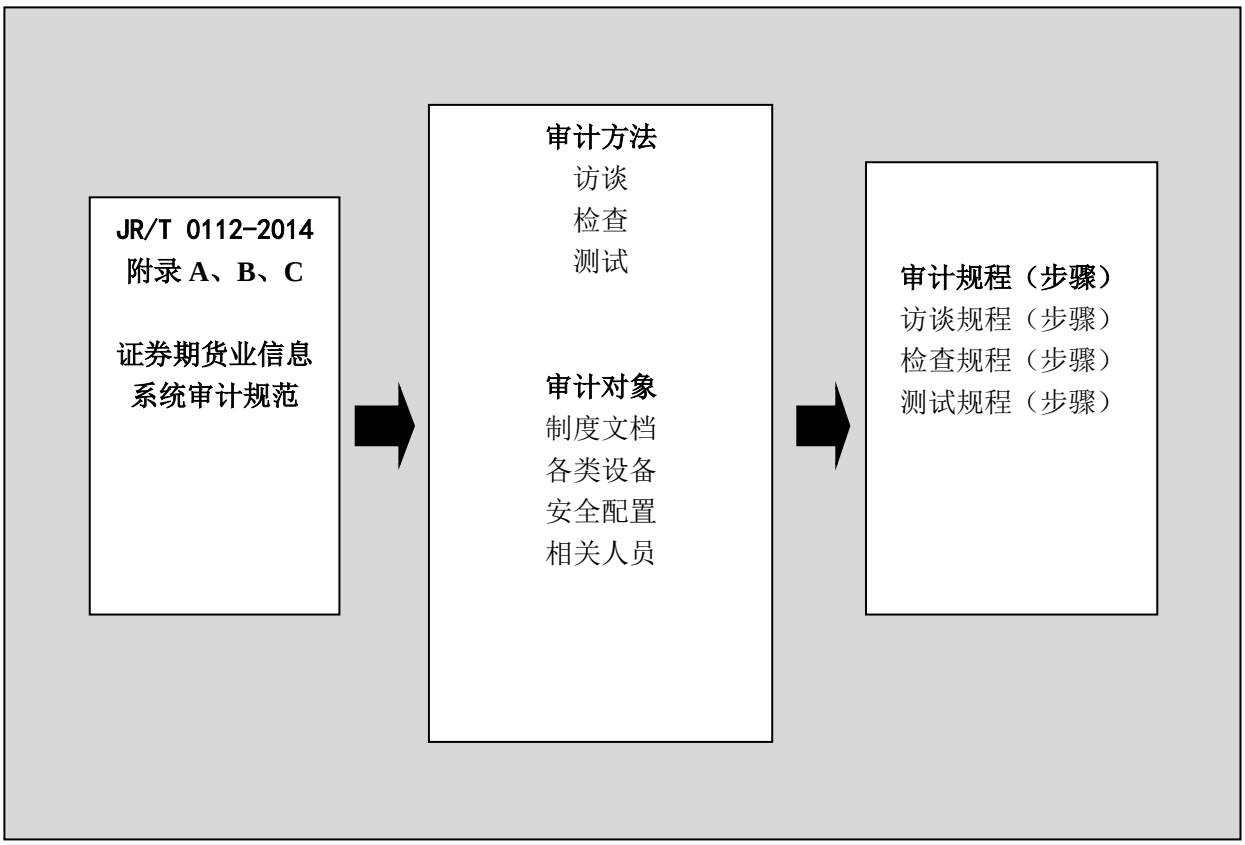

图1 概念性框架

审计对象是指审计实施的对象，即审计过程中涉及到的制度文档、各类设备及其安全配置和相关人员等。制度文档是指针对信息系统所制定的相关联的文件（如：政策、程序、计划、系统安全需求、功能规格及建筑设计）。各类设备是指安装在信息系统之内或边界，能起到特定保护作用的相关部件（如：硬件、软件、固件或物理设施）。安全配置是指信息系统所使用的设备为了贯彻安全策略而进行的设置。相关人员或部门，是指应用上述制度、设备及安全配置的人。

审计方法包括：访谈、检查和测试，审计人员通过这些方法试图获取证据。上述三种审计方法（访谈、检查和测评）的审计结果都用以对安全控制的有效性进行评估。

审计输出是审计报告，审计报告应给出审计结论：如果审计结果中没有不符合项，则审计结论为“符合”；如果审计结果存在不符合项，但所产生的安全问题不会导致信息系统存在高等级安全风险，则审计结论为“基本符合”；如果审计结果存在不符合项，且所产生的安全问题导致信息系统存在高等级安全风险，则审计结论为“不符合”。

4.2 使用方法

本标准附录A至附录N分别描述了信息技术治理、机房管理、网络管理、运维管理、信息系统安全等级保护相关工作、软件正版化、集中交易系统、网上信息系统、第三方存管系统、重要信息系统、A型营业部、B型营业部、C型营业部、信息系统托管的审计方法。附录O给出了实施信息系统审计时需要的调查数据。

审计实施时，审计人员需参考附录A至附录O，完成信息系统审计工作。对于机房管理、网络管理，需每一个机房给出完整的审计底稿。对于重要信息系统，需审计包括但不限于等级保护二级及以上系统，并对每一个重要信息系统给出完整的审计底稿。对于A型营业部、B型营业部、C型营业部，审计部门应对每一个营业部给出完整的审计底稿。对于信息系统托管，需每一个提供托管服务的机房给出完整的审计底稿。

审计过程中，审计人员需注意对审计记录和证据的采集、处理、存储和销毁，保护其在审计期间免遭破坏、更改或遗失，并保守秘密。

附 录 A
（规范性附录）
信息技术治理审计底稿

表A.1至表A.2给出了信息技术治理审计的程序、内容及相关记录要求。

表A.1 信息技术治理审计底稿

被审计部门：	索引号：XXJSZL
审计主题：信息技术治理	审计年度：
审计结论、意见及建议： 编制人： 年 月 日 （部门盖章）	
复核意见： 复核人： 年 月 日 （部门盖章）	
被审计部门意见： 年 月 日 （部门盖章）	

表 A.1　信息技术治理审计底稿（续）

审计证据列表：

表A.2　信息技术治理审计底稿

序号	审计项	审计程序	审计结论	备注
1.	**制度和文档管理**			
1.1.	**管理制度**			
1.1.1.	是否制定信息安全工作的总体方针和安全策略，说明机构安全工作的总体目标、范围、原则和安全框架等。	检查公司信息安全工作的总体方针和安全策略，查看文件是否明确机构安全工作的总体目标、范围、原则和安全框架等。	是□ 否□ 不适用□	
1.1.2.	是否建立交付管理、配置管理、值班管理、监控管理、关联单位关系管理等制度。	检查运维管理制度是否涵盖交付管理、配置管理、值班管理、监控管理、关联单位关系管理等制度。	是□ 否□ 不适用□	
1.1.3.	是否根据行业规划和本机构发展战略，制定信息化与信息安全发展规划，满足业务发展和信息安全管理的需要。	检查信息化与信息安全发展规划，判断是否规划中根据行业规划和本机构发展战略，制定信息化与信息安全发展规划，满足业务发展和信息安全管理的需要。	是□ 否□ 不适用□	
1.1.4.	是否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。	检查供应商管理制度，查看是否有对供应商支持运维服务的相关活动进行统一管理的规定。	是□ 否□ 不适用□	
1.1.5.	是否制定安全审核和安全检查制度规范安全审核和安全检查工作，定期按照程序进行安全审核和安全检查活动。	a)检查是否制定信息安全审核和检查制度； b)检查安全审核和安全检查报告，确定是否定期按照程序进行安全审核和安全检查活动。	是□ 否□ 不适用□	
1.1.6.	是否制定有关管理规范，严格规范人员离岗过程，及时终止离岗员工的所有访问权限。	a)访谈负责人员调岗和离职管理的人事管理人员，询问员工离岗是否遵循严格的调离手续，离岗员工的访问权限是否及时终止； b)IT技术人员岗位管理相关制度中是否包含制定有关管理规范，严格规范人员离岗过程，及时终止离岗员工的所有访问权限； c)抽查审计期内离岗员工的离岗记录，是否具有按照离岗程序办理调离手续的记录，对应的权限取消记录是否留痕； d)抽查审计期内离岗员工使用的主要系统中的用户权限列表，离岗员工使用的账号是否已禁用或取消。	是□ 否□ 不适用□	
1.1.7.	是否建立机房安全管理制度，对有关机房设备和人员出入，供电，空调，消防，安防等基础设施的运行维护，机房工作人员等进行规范管理。	a)是否有机房安全管理制度； b)查看其内容是否覆盖机房设备和人员出入（含物品带进/带出），供电、空调、消防、安防等基础设施的运行维护及机房工作人员管理。	是□ 否□ 不适用□	

表 A.2　信息技术治理审计底稿（续）

序号	审计项	审计程序	审计结论	备注
1.1.8.	是否指定专门部门负责信息系统的安全建设总体规划、近期和长期安全建设计划。	a)检查IT组织构架管理，是否指定专门部门负责信息系统的安全建设总体规划、制定近期和长期安全建设计划； b)检查信息系统的安全建设总体规划、近期和长期安全建设计划文档。	是□ 否□ 不适用□	
1.1.9.	是否制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则。	检查是否有软件开发方面的管理制度，查看文件是否明确软件设计、开发、测试、验收过程的控制方法和人员行为准则，是否明确哪些开发活动应经过授权、审批等。	是□ 否□ 不适用□	
1.1.10.	是否制定工程实施管理制度，明确实施过程的控制方法和人员行为准则。	检查工程实施管理制度，查看其是否包括工程实施过程的控制方法、实施参与人员的行为准则等方面内容。	是□ 否□ 不适用□	
1.1.11.	是否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。	检查运维值班管理制度，判断是否对日常操作、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。	是□ 否□ 不适用□	
1.1.12.	是否建立文档管理制度，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。	a)检查是否建立文档管理制度； b)是否对文档的分类、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。	是□ 否□ 不适用□	
1.1.13.	是否建立资产安全管理制度，规定信息系统资产管理的责任人员或责任部门，并规范资产管理和使用的行为。	a)检查是否建立资产安全管理制度； b)资产安全管理制度是否规定信息系统资产管理的责任人员或责任部门，并规范资产管理和使用的行为。	是□ 否□ 不适用□	
1.1.14.	是否建立介质安全管理制度，明确责任人，对介质的存放环境、使用、维护和销毁等方面作出规定。	a)是否建立介质安全管理制度； b)制度中明确责任人，对介质的存放环境、使用、维护和销毁等方面作出规定。	是□ 否□ 不适用□	
1.1.15.	是否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。	a)检查是否建立信息系统数据管理制度； b)数据管理制度是否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。	是□ 否□ 不适用□	
1.1.16.	是否建立基于申报、审批和专人负责的设备安全管理制度，对信息系统的各种软硬件设备的选型、采购、发放和领用等过程进行规范化管理。	a)文档审阅，是否建立了基于申报、审批和专人负责的设备安全管理制度； b)文档审阅，设备安全管理是否对信息系统的各种软硬件设备的选型、采购、发放和领用等过程进行规范化管理。	是□ 否□ 不适用□	

表 A.2　信息技术治理审计底稿（续）

序号	审计项	审计程序	审计结论	备注
1.1.17.	是否建立配套设施、软硬件维护方面的管理制度，明确维护人员的责任、涉外维修和服务的审批、维修过程的监督控制等。	a)文档审阅，是否建立了配套设施、软硬件维护方面的管理制度； b)文档审阅，设备管理制度是否明确维护人员的责任、涉外维修和服务的审批、维修过程的监督控制等。	是□ 否□ 不适用□	
1.1.18.	是否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。	a)文档审阅，是否建立了计算机相关设备和软件管理制度； b)文档审阅，管理制度是否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。	是□ 否□ 不适用□	
1.1.19.	是否建立变更管理制度，系统发生变更前，向主管领导申请，变更和变更方案经过评审、审批后方可实施变更，并在实施后将变更情况向相关人员通告。	a)文档审阅，是否建立变更管理制度； b)系统发生变更前，是否向主管领导申请； c)变更和变更方案是否经过评审、审批后方可实施变更，并在实施后将变更情况向相关人员通告。	是□ 否□ 不适用□	
1.1.20.	是否建立检查审计制度，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。	a)检查是否有与IT检查审计相关的管理制度，查看其是否要求对IT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； b)检查审计期内的IT检查和审计记录，是否每年至少每年进行一次IT 运维审计。	是□ 否□ 不适用□	
1.1.21.	是否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。	检查IT运维管理方面的制度，查看制度中是否包括人工巡检方面的内容，是否明确巡检内容、频度、人员、报告等要求，巡检内容是否覆盖审计项中列示的内容。	是□ 否□ 不适用□	
1.1.22.	是否建立网络安全管理制度，对网络安全配置、日志保存时间、安全策略、升级与打补丁、口令更新周期等方面作出规定。	a)查看是否有网络安全管理制度，覆盖网络安全配置、日志保存时间、安全策略、升级与打补丁、口令更新周期等方面； b)访谈网络管理员，了解是否知悉网络安全管理的相关规定。	是□ 否□ 不适用□	

表 A.2　信息技术治理审计底稿（续）

序号	审计项	审计程序	审计结论	备注
1.1.23.	是否建立系统安全管理制度，对系统安全策略、安全配置、日志管理和日常操作流程等方面作出规定。	a)访谈负责信息技术规划和信息安全管理的跨部门机构负责人，检查其是否清楚信息安全管理职责； b)检查其是否有信息安全的管理制度文档，是否对系统安全策略、安全配置、日志管理和日常操作流程等方面作出规定。	是□ 否□ 不适用□	
1.1.24.	是否建立定期的网上信息系统安全风险评估机制和整改的工作制度，及时发现SQL注入漏洞、弱口令账户、绕过验证、目录遍历、文件上传、跨站脚本、Session欺骗、拒绝式服务攻击和缓冲区溢出等系统存在的安全隐患和漏洞，并进行改进和完善。	a)检查是否建立定期的网上信息系统安全风险评估机制和整改的工作制度； b)查看内部风险评估报告和外部风险评估报告，确认是否实时监控SQL注入漏洞、弱口令账户、绕过验证、目录遍历、文件上传、跨站脚本、Session欺骗、拒绝式服务攻击和缓冲区溢出等系统存在的安全隐患和漏洞； c)查看整改工作报告，确认对发现的风险隐患进行了改进和完善。	是□ 否□ 不适用□	
1.1.25.	是否建立密码使用管理制度，使用符合国家密码管理规定的密码技术和产品。	a)访谈安全管理员，了解其是否知道密码使用的相关规定； b)查看国家密码管理局批准使用的密码技术和产品列表，检查是否使用符合国家密码管理规定的密码技术和产品。	是□ 否□ 不适用□	
1.1.26.	是否建立备份与恢复管理相关的安全管理制度，对备份信息的备份方式、备份频度、存储介质和保存期等进行规范。	检查是否建立备份与恢复管理相关的安全管理制度，对备份信息的备份方式、备份频度、存储介质和保存期等进行规范。	是□ 否□ 不适用□	
1.1.27.	是否针对信息的运行制定专项管理制度和操作流程。	检查信息技术部门是否针对信息系统备份能力的运行制定专项管理制度和操作流程，查看其内容是否覆盖数据备份、故障备份和灾难备份等方面。	是□ 否□ 不适用□	
1.1.28.	是否建立问题管理制度，对运维活动中发现的问题进行根本解决，并建立问题库。	查看问题管理制度，是否对运维活动中发现的问题建立问题库。	是□ 否□ 不适用□	
1.1.29.	是否建立软件资产管理制度，或将软件资产纳入本单位资产管理体系，对软件采购、安装、升级等工作流程有严格管理。	a)访谈信息技术负责人，是否将软件资产纳入资产管理体系，并对软件采购、安装、升级等流程进行管理； b)检查固定资产管理办法，是否包含软件购置、安装、升级等流程。	是□ 否□ 不适用□	

表 A.2　信息技术治理审计底稿（续）

序号	审计项	审计程序	审计结论	备注
1.1.30.	是否制定安全事件报告和处置管理制度，明确安全事件类型，规定安全事件的现场处理、事件报告和后期恢复的管理职责。	a)检查是否有安全事件报告和处置管理制度，查看其是否明确安全事件的级别，明确不同级别安全事件的报告和处置方式等内容； b)检查安全事件处理记录，查看其是否记录引发安全事件的原因，是否记录事件处理过程，是否与管理规定的处理要求一致等。	是□ 否□ 不适用□	
1.2.	**评审修订**			
1.2.1.	是否组织相关人员对制定的安全管理制度进行论证和审定。	a)访谈安全主管，询问是否组织相关人员对制定的安全管理制度进行论证和审定 b)检查安全管理制度评审记录，查看是否有相关人员的评审意见。	是□ 否□ 不适用□	
1.2.2.	信息安全领导小组每年至少组织一次安全管理制度体系的合理性和适用性审定。	a)访谈信息安全领导小组负责人，询问信息安全领导小组是否每年至少一次对安全管理制度体系的合理性和适用性进行审定； b)检查安全管理制度体系的评审记录，是否记录了相关人员的评审意见，是否至少每年对安全管理制度体系进行评审。	是□ 否□ 不适用□	
1.2.3.	每年或在发生重大变更时对安全管理制度进行检查，对存在不足或需要改进的安全管理制度进行修订。	a)检查安全管理制度的检查或评审记录，判断是否至少每年或在发生重大变更时，对安全管理制度进行检查； b)检查安全管理制度的修订记录，判断是否对存在不足或需要改进的安全管理制度进行了修订。	是□ 否□ 不适用□	
1.2.4.	是否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。	a)检查运维管理制度和操作流程维护办法，是否有关于制定、发布、维护和更新的规定； b)检查评审、修订运维管理制度和操作流程的记录，是否每年对运维管理制度和操作流程进行了评审、修订。	是□ 否□ 不适用□	
1.3.	**日常操作**			
1.3.1.	是否妥善保存客户开户资料、委托记录、交易记录和内部管理、业务经营有关的各项资料，不得隐匿、伪造、篡改或者毁损。上述资料的保存期限不得少于20年。	a)审阅客户资料保管制度，确认客户资料的保存期限。 b)随机抽查最早年限的客户资料，确认是否完整保存。	是□ 否□ 不适用□	

表 A.2　信息技术治理审计底稿（续）

序号	审计项	审计程序	审计结论	备注
1.3.2.	是否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。	a)检查文档管理制度； b)检查实际文档； c)判断是否对运维过程中涉及的各类文档进行分类管理。	是□ 否□ 不适用□	
1.3.3.	是否对超范围、超权限使用文档时，保存相关审批、使用记录。	检查超范围、超权限使用文档审批和使用记录。	是□ 否□ 不适用□	
1.4.	**制定发布**			
1.4.1.	安全管理制度是否通过正式、有效的方式发布。	检查安全管理制度的收发登记记录，判断安全管理制度是否能够发布到相关人员手中。	是□ 否□ 不适用□	
1.4.2.	安全管理制度是否注明发布范围，并对收发文进行登记。	a)检查安全管理制度是否是注明发布范围； b)检查安全管理制度的收发文登记记录。	是□ 否□ 不适用□	
1.4.3.	是否规范文档的发布管理，对文档的版本进行控制。文档标识敏感性、使用范围、使用权限、审批权限等。文档在使用时能读取、使用最新版本，防止作废文件的逾期使用。	a)检查文档管理制度； b)检查实际文档； c)判断是否对文档的版本进行控制。 d)是否标识文档敏感性、使用范围、使用权限、审批权限等。	是□ 否□ 不适用□	
2.	**供应商管理**			
2.1.	是否确保安全服务商的选择符合国家、行业的有关规定。	访谈安全管理员，询问安全服务商是否通过国家、行业认可的信息安全资质认证。	是□ 否□ 不适用□	
2.2.	是否与选定的安全服务商签订与安全相关的协议，对合作方服务人员提出明确的信息安全要求。	检查与安全服务商签订的安全责任合同书或保密协议等文档，查看其内容是否包含保密范围、安全责任、违约责任、协议的有效期限和责任人的签字等。	是□ 否□ 不适用□	
2.3.	是否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。	检查与供应商签订的合同，查看是否明确其应承担的责任、义务，并约定服务要求和范围等内容。	是□ 否□ 不适用□	

表 A.2　信息技术治理审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.4.	是否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。	a)检查供应商签署的保密协议，查看是否禁止供应商泄露所服务机构的保密信息； b)检查供应商签署的承诺书，查看供应商是否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。	是□ 否□ 不适用□	
2.5.	是否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，明确供应商是否接受证券期货行业监管部门的信息安全延伸检查。	检查软件产品或技术服务的采购合同，查看是否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。	是□ 否□ 不适用□	
2.6.	是否定期收集、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。	a)检查供应商列表，访谈信息技术负责人，判断是否定期收集、更新供应商信息； b)检查供应商评价报告，判断是否定期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，并跟踪和记录供应商改进情况。	是□ 否□ 不适用□	
2.7.	是否与外包公司及外包人员签订保密协议。	检查与外包公司及外包人员签订的保密协议，确认是否与外包公司及外包人员签订了保密协议。	是□ 否□ 不适用□	
2.8.	是否明确外包公司应当承担的责任及追究方式。	检查与外包公司签订的合同，确认合同中明确了外包公司应当承担的责任及追究方式。	是□ 否□ 不适用□	
2.9.	是否明确界定外包人员的工作职责、活动范围、操作权限。	检查与外包公司签订的合同，确认合同中明确了明确界定外包人员的工作职责、活动范围、操作权限。	是□ 否□ 不适用□	
2.10.	是否对外包人员工作情况进行监督和检查，并保留相应记录。	查看监督和检查记录，确认对外包人员工作情况进行了监督和检查。	是□ 否□ 不适用□	
2.11.	是否对驻场外包人员的入场和离场进行管理。	查看驻场外包人员入场和离场记录，确认对驻场外包人员的入场和离场进行了管理。	是□ 否□ 不适用□	
2.12.	是否定期评估外包的服务质量。	检查外包服务的评估报告，确认定期对外包的服务质量进行了评估。	是□ 否□ 不适用□	

表 A.2　信息技术治理审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.13.	是否制定外包服务意外终止的应急措施。	检查应急预案，确认有外包服务意外终止的应急措施。	是□ 否□ 不适用□	
2.14.	是否建立产品提供、系统开发和运营服务厂商的退出机制，以保障其退出之后集中交易系统的持续运行和系统重要数据的安全。	检查信息系统外包管理制度和应急预案，确认有产品提供、系统开发和运营服务厂商的退出机制，以保障其退出之后集中交易系统的持续运行和系统重要数据的安全措施。	是□ 否□ 不适用□	
3.	**关联单位管理**			
3.1.	是否建立关联单位联系制度，定期与关联单位进行合作与沟通。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。	a)检查关联单位联系表，是否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； b)检查合作与沟通的会议纪要或往来函件，判断是否定期与关联单位进行合作与沟通。	是□ 否□ 不适用□	
3.2.	各类管理人员之间、组织内部机构之间以及信息安全职能部门内部是否有内部合作沟通机制，定期或根据需要召开协调会议，协作处理信息安全问题。	检查合作与沟通的会议纪要或来往函件，判断各类管理人员之间、组织内部机构之间以及信息安全职能部门内部是否有合作与沟通，定期或根据需要召开协调会议，协作处理信息安全问题。	是□ 否□ 不适用□	
3.3.	是否加强与供应商、业界专家、专业的安全公司、安全组织的合作与沟通。	检查合作与沟通的邮件、会议纪要等，判断与供应商、业界专家、专业的安全公司、安全组织是否有合作与沟通。	是□ 否□ 不适用□	
3.4.	是否聘请信息安全专家作为常年的安全顾问，指导信息安全建设，参与安全规划和安全评审等。	a)检查信息安全专家的简历和聘书，判断是否聘请信息安全专家作为常年的安全顾问，指导信息安全建设，参与安全规划和安全评审等； b)检查安全规划和安全评审会议纪要，判断安全专家是否参与安全规划和安全评审会议。	是□ 否□ 不适用□	
3.5.	是否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。	检查关联单位联系表，是否包括单位名称、业务事项、联系人、联系方式、备注等，并及时更新。	是□ 否□ 不适用□	

表 A.2　信息技术治理审计底稿（续）

序号	审计项	审计程序	审计结论	备注
4.	**经费管理**			
4.1.	最近三个财政年度IT投入平均数额是否不少于最近三个财政年度平均净利润的6%或不少于最近三个财政年度平均营业收入的3%。	检查“a)表0.2-合计（万元）”、“b)表0.2-净利润（万元）”、“c)表0.2-营业收入（万元）”，判断最近三个财政年度IT投入平均数额是否不少于最近三个财政年度平均净利润的6%或不少于最近三个财政年度平均营业收入的3%。	是□ 否□ 不适用□	
4.2.	是否制定信息系统运行维护年度预算计划，每年进行核算。预算和核算是否接受监督和审计。	a)检查是否有信息系统运行维护年度预算计划； b)检查是否有预算审批记录和审计记录。	是□ 否□ 不适用□	
4.3.	是否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。	检查“表0.2-信息技术投入情况”，是否有信息系统运行维护年度预算计划，费用包括：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。	是□ 否□ 不适用□	
4.4.	是否落实软件采购经费，做好软件正版化工作。	a)检查“表0.2-软件投入（万元）”，访谈正版化相关人员，是否制定了软件采购的经费，并纳入预算； b)检查软件采购经费说明，是否按照预算执行。	是□ 否□ 不适用□	
5.	**客户关系管理**			
5.1.	是否在与客户签订的服务合同、经纪合同及补充协议、风险揭示书等中载明，客户使用网上交易可能面临的风险、公司采取的风险控制措施、客户应采取的风险控制措施以及相关风险对应的责任承担。（如防止用于网上交易的计算机或手机终端感染木马、病毒，以免被恶意程序窃取口令；加强帐号、口令的保护，不使用简单口令、定期修改口令、输入口令时防止他人偷看、不对他人泄露口令等）。	检查与客户签订的服务合同、经纪合同及补充协议、风险揭示书等，确定这些文档中载明，客户使用网上交易可能面临的风险、公司采取的风险控制措施、客户应采取的风险控制措施以及相关风险对应的责任承担。（如防止用于网上交易的计算机或手机终端感染木马、病毒，以免被恶意程序窃取口令；加强帐号、口令的保护，不使用简单口令、定期修改口令、输入口令时防止他人偷看、不对他人泄露口令等）。	是□ 否□ 不适用□	

表 A.2　信息技术治理审计底稿（续）

序号	审计项	审计程序	审计结论	备注
5.2.	是否在门户网站或固定营业场所公告短信服务号码、移动证券门户网站地址等信息，提醒客户防范他人利用移动通讯设备进行欺诈。	检查门户网站或固定营业场所是否公告短信服务号码、移动证券门户网站地址等信息，提醒客户防范他人利用移动通讯设备进行欺诈。	是□ 否□ 不适用□	
5.3.	是否根据移动证券业务的网络延迟时间、链路稳定状况、信号衰减程度等风险因素，对行情或交易数据可能出现明显滞后或产生数据丢失的情况，事先对客户进行风险提示。	检查客户签署的开户协议或移动终端服务协议中是否存在风险提示。	是□ 否□ 不适用□	
5.4.	是否尽可能使用统一的网上证券服务电话、域名、短信号码等，并应在与投资者签订的协议或合同中明确告知客户使用网上证券信息系统的合法途径、意外事件的处理办法，以及证券公司联系方式等。	检查与投资者签订的协议或合同是否明确告知客户使用网上证券信息系统的合法途径、意外事件的处理办法，以及证券公司网上证券服务电话、域名、短信号码等联系方式。	是□ 否□ 不适用□	
5.5.	是否根据投资者需要开启或关闭网上交易方式。	检查与投资者签订的协议或合同是否根据投资者需要开启或关闭网上交易方式。	是□ 否□ 不适用□	
6.	**人员管理**			
6.1.	**教育培训**			
6.1.1.	是否为IT部门提供足够的资金支持，为IT人员提供履行其岗位职责所需要的岗位技能培训及业务培训，制定合理的考核体系、激励机制和奖惩措施。	检查“表0.2-信息技术培训费用（万元）”、IT技术人员的业务培训、考核、激励和奖惩记录。	是□ 否□ 不适用□	
6.1.2.	是否对各类人员进行安全意识教育、岗位技能培训和相关安全技术培训。	a)访谈安全主管，询问是否制定安全教育和培训计划； b)检查安全教育和培训计划文档，查看计划是否明确了培训方式、培训对象、培训内容、培训时间和地点等； c)检查培训内容是否包含信息安全基础知识、岗位操作规程等； d)检查安全教育和培训记录，查看记录是否有培训人员、培训内容、培训结果等的描述。	是□ 否□ 不适用□	

表 A.2　信息技术治理审计底稿（续）

序号	审计项	审计程序	审计结论	备注
6.1.3.	是否对安全责任和惩戒措施进行书面规定并告知相关人员，并对违反违背安全策略和规定的人员进行惩戒。	a)检查安全责任和惩戒措施管理文档，查看是否包含具体的安全责任和惩戒措施； b)检查安全责任惩戒记录，是否对违反安全策略和规定的人员进行惩戒。	是□ 否□ 不适用□	
6.1.4.	是否对年度安全教育和培训进行书面规定，针对运维人员等不同岗位制定不同的培训计划，对信息安全基础知识、岗位操作规程、机房消防及相关应急内容等进行培训，并留存培训记录。	a)检查安全教育和培训计划文档，查看计划是否明确了培训方式、培训对象、培训内容、培训时间和地点等，培训内容是否包含信息安全基础知识、岗位操作规程、机房消防及相关应急内容等； b)检查安全教育和培训记录，查看记录是否有培训人员、培训内容、培训结果等的描述。	是□ 否□ 不适用□	
6.1.5.	是否对安全教育和培训的情况和结果进行记录并归档保存。	检查安全教育和培训记录，查看记录是否有培训人员、培训内容、培训结果等的描述。	是□ 否□ 不适用□	
6.2.	**人员考核**			
6.2.1.	是否定期对各个岗位的人员进行安全技能及安全认知的考核。安全技能及安全认知的考核是否至少每年一次。	a)访谈安全主管，询问是否定期对各个岗位人员进行安全技能及安全知识的考核； b)检查考核记录，查看考核人员是否包括各个岗位的人员，考核内容是否包含安全知识、安全技能等。检查相关岗位的安全技能和安全认知的考核记录，查验安全技能和安全认知的考核是否至少每年一次。	是□ 否□ 不适用□	
6.2.2.	是否对关键岗位的人员进行全面、严格的安全审查和技能考核。	a)访谈安全主管，询问是否对关键岗位人员定期进行安全审查和技能考核； b)检查考核记录，查看是否考核关键岗位人员，考核内容是否包含安全知识、安全技能等，考核是否至少每年一次。	是□ 否□ 不适用□	
6.2.3.	是否对考核结果进行记录并保存。	a)检查是否对岗位人员的安全审查和技能考核结果进行记录； b)记录是否得到妥善保存。	是□ 否□ 不适用□	
6.3.	**人员离岗**			
6.3.1.	人员离岗是否取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备。	检查人员离岗记录是否包含取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备等记录。	是□ 否□ 不适用□	
6.3.2.	是否办理严格的调离手续，关键岗位人员离岗须承诺调离后的保密义务后方可离开。	a)检查IT技术人员录用考评相关制度是否包含严格的调离手续。 b)检查关键岗位人员保密承诺书是否有关于离岗后保密承诺的相关规定。	是□ 否□ 不适用□	

表 A.2　信息技术治理审计底稿（续）

序号	审计项	审计程序	审计结论	备注
6.4.	**人员录用**			
6.4.1.	运维人员是否具备一定的计算机基础理论知识和专业技术经验，并具有相应的从业资格。	查看运维人员简历，访谈相关人员，判断运维人员是否具备一定的计算机基础理论知识和专业技术经验，并具有相应的从业资格。	是□ 否□ 不适用□	
6.4.2.	公司是否配备足够的信息技术人员，公司的IT工作人员总数不少于公司员工总人数的6%。	a)检查“表0.1-人员基本情况”、技术部门员工的情况说明，应包括总部技术部门人员名单及占比情况计算； b)检查正式员工花名册及员工人数统计（以与公司签订劳动合同，且具有从业资格为准）； c)检查技术部门技术人员的简历，是否符合情况说明。	是□ 否□ 不适用□	
6.4.3.	是否指定或授权专门的部门或人员负责人员录用。	a)访谈人事管理人员，是否由专门的部门或人员负责人员的录用工作； b)查看对应部门的部门职责，是否有对该职责的明确描述。	是□ 否□ 不适用□	
6.4.4.	是否严格规范人员录用过程，对被录用人员的身份、背景和专业资格等进行审查，对其所具有的技术技能进行考核。	a)访谈负责人员录用的人事管理人员，是否对被录用人员的身份、背景和专业资格等进行审查，对其所具有的技术技能进行考核； b)抽查审计期内人员录用管理文档，查看是否说明录用人员应具备的条件(如学历、学位要求，技术人员应具备的专业技术水平，管理人员应具备的安全管理知识等)； c)抽查审计期内录用的人员审查记录，是否具有人员录用时对录用人身份、背景和专业资格等进行审查的相关文档或记录，查看是否记录审查内容和审查结果等； d)抽查审计期内人员录用时的技能考核文档或记录，查看是否记录考核内容和考核结果等。	是□ 否□ 不适用□	

表 A.2　信息技术治理审计底稿（续）

序号	审计项	审计程序	审计结论	备注
6.4.5.	证券期货机构是否与人员签署保密协议，保密协议应至少包括保密范围、保密期限等内容。	a)访谈负责人员录用的人事管理人员，是否与被录用人员签署保密协议，保密协议是否至少包括保密范围、保密期限等内容； b)检查IT技术人员岗位管理相关制度中是否含有与开发、运维等关键岗位人员签署保密协议，保密协议应至少包括保密范围、保密期限等内容； c)检查保密协议记录是否覆盖了开发和运维等关键岗位的全部人员。	是□ 否□ 不适用□	
6.4.6.	是否从内部人员中选拔从事关键岗位的人员，并签署岗位安全协议。	a)检查IT技术人员岗位管理相关制度中是否要求从内部人员中选拔从事关键岗位的人员； b)检查关键岗位人员的工作经历是否满足要求； c)检查关键岗位人员是否签署了岗位安全协议。	是□ 否□ 不适用□	
6.5.	**外部人员管理**			
6.5.1.	是否确保在外部人员访问受控区域前先提出书面申请，批准后由专人全程陪同或监督，并登记备案。	检查重要区域外部人员访问记录，判断外部人员访问重要区域（如访问机房、重要服务器或设备区等）是否经有关部门或负责人批准，并由专人全程陪同或监督。	是□ 否□ 不适用□	
6.5.2.	对外部人员允许访问的区域、系统、设备、信息等内容是否进行书面的规定，并按照规定执行。	a)检查外部人员访问管理文档，查看是否具有规范外部人员访问机房等重要区域需经过相关部门或负责人批准的管理要求； b)检查外部人员访问重要区域的申请文档，登记记录，查看是否记录了外部人员访问重要区域的进入时间、离开时间、访问区域及陪同人等信息。	是□ 否□ 不适用□	
7.	**组织管理**			
7.1.	**岗位设置**			
7.1.1.	是否指定或授权专门的部门或人员负责安全管理制度的制定。	a)访谈安全主管，询问由哪个部门或人员负责制定安全管理制度； b)查阅公司正式发文，是否指定或授权专门的部门或人员负责安全管理制度的制定。	是□ 否□ 不适用□	

表 A.2　信息技术治理审计底稿（续）

序号	审计项	审计程序	审计结论	备注
7.1.2.	是否设立信息安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责。	a)访谈安全主管，询问是否设立信息安全管理工作的职能部门、安全主管、安全管理各个方面的负责人岗位； b)检查岗位职责文档，查看文档是否明确设置安全主管、安全管理各个方面的负责人、各个岗位的职责范围是否清晰、明确。	是□ 否□ 不适用□	
7.1.3.	是否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。	a)访谈运维组织负责人，询问是否知悉其职责范围； b)查阅公司正式发文，是否明确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。	是□ 否□ 不适用□	
7.1.4.	是否制定文件明确安全管理机构各个部门和岗位的职责、分工和技能要求。	检查安全管理制度，查看是否明确安全管理机构各个部门和岗位的职责、分工和技能要求。	是□ 否□ 不适用□	
7.1.5.	运维岗位是否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。	a)检查“表0.1-按岗位人员情况”，检查运维岗位分工及岗位职责说明，是否包括机房管理员、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)访谈机房管理员、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人员，了解信息系统运行维护情况。	是□ 否□ 不适用□	
7.1.6.	关键岗位是否进行分离，兼岗时是否满足岗位相互制约的要求。	检查运维岗位分工及岗位职责说明，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的职责范围是否清晰、明确，有相互制约的要求。	是□ 否□ 不适用□	
7.1.7.	是否设立总工程师岗位、IT总监或其他类似职位的IT专职负责人。	a)查阅公司正式发文，是否设立总工程师岗位、IT总监或其它类似职位的IT专职负责人； b)访谈总工程师岗位、IT总监或其它类似职位的IT专职负责人，询问是否知悉其职责范围。	是□ 否□ 不适用□	
7.1.8.	是否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。	a)检查运维岗位分工及岗位职责说明，是否设置安全管理员岗位； b)访谈安全管理员，询问是否知悉其职责范围； c)如果外聘安全机构协助完成安全管理工作，查看外聘机构联系表，确认有外聘的安全机构。	是□ 否□ 不适用□	

表 A.2　信息技术治理审计底稿（续）

序号	审计项	审计程序	审计结论	备注
7.1.9.	安全管理员是否督促解决检查、测评、评估中发现的风险隐患。	查看安全管理员督促解决检查、测评、评估中发现的风险隐患的记录，判断安全管理员是否履行其职责。	是□ 否□ 不适用□	
7.1.10.	第三方存管系统安全稳定运行的第一责任人是否为总部主要负责人。	a)查阅公司正式发文，是否设立第三方存管系统第一责任人； b)判断第三方存管系统第一责任人是否为总部主要负责人； c)访谈第三方存管系统第一责任人，询问是否知悉其职责范围。	是□ 否□ 不适用□	
7.1.11.	是否指定专门的第三方存管系统技术联络员，具体负责与监管机构、技术协调小组、第三方存管相关参与方之间的对口联络。	a)查阅公司正式发文，是否设立专门的第三方存管系统技术联络员； b)访谈技术联络员，询问是否知悉其职责范围； c)查看与监管机构、技术协调小组、第三方存管相关参与方的联络记录，判断技术联络员是否履行其职责。	是□ 否□ 不适用□	
7.1.12.	是否指定部门负责机房安全，并配备机房安全管理人员，对机房的出入、服务器的开机或关机等工作进行管理。	访谈系统运维负责人，询问是否有专门的部门或人员对机房的出入、服务器开机/关机等日常工作进行管理，由何部门/何人负责。	是□ 否□ 不适用□	
7.1.13.	是否指定机房管理负责人。	查阅公司正式发文，是否设立机房管理负责人。	是□ 否□ 不适用□	
7.1.14.	是否指定人员负责控制、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。	a)检查运维岗位分工及岗位职责说明，是否指定人员负责控制、鉴别和记录设备和人员的进出情况； b)抽查90天内的机房进出记录，确认是否记录设备和人员的进出情况，记录进出人员、进出时间、工作内容等。	是□ 否□ 不适用□	
7.1.15.	是否指定或授权专门的部门或人员负责工程实施过程的管理。	访谈系统建设负责人，询问是否指定专门部门或人员对工程实施过程进行进度和质量控制，由何部门/何人负责。	是□ 否□ 不适用□	
7.1.16.	是否指定专门的部门或人员负责管理系统定级的相关材料，并控制这些材料的使用。	访谈系统建设负责人，询问是否有专门的部门或人员负责管理系统定级的相关文档，由何部门/何人负责；询问对系统定级相关备案文档使用的控制方式。	是□ 否□ 不适用□	
7.1.17.	是否指定或授权专门的部门或人员负责等级测评的管理。	访谈系统建设负责人，询问是否有专门的部门或人员负责等级测评的管理，由何部门/何人负责。	是□ 否□ 不适用□	

表 A.2　信息技术治理审计底稿（续）

序号	审计项	审计程序	审计结论	备注
7.1.18.	是否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。运维值班负责人是否有备岗，主备岗是否不得同时离岗。	a)查阅运维值班负责人及备岗人员名单； b)访谈运维值班负责人及备岗人员，询问是否知悉其职责范围包括：日常操作的部署、检查、风险控制、业务衔接等工作； c)查看运维值班负责人及备岗人员值班记录，判断是否没有同时离岗。	是□ 否□ 不适用□	
7.1.19.	是否明确文档管理的责任人。	访谈文档管理责任人，询问是否知悉其职责范围。	是□ 否□ 不适用□	
7.1.20.	是否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。	访谈数据管理责任人，询问是否知悉其职责范围，包括数据的收集、使用、备份、检查等策略的制定和执行工作。	是□ 否□ 不适用□	
7.1.21.	是否明确设备和软件管理责任人。	访谈设备和软件管理责任人，询问是否知悉其职责范围。	是□ 否□ 不适用□	
7.1.22.	是否明确责任人，负责统一保管、安全存放管理员口令，不得泄漏。	访谈管理员口令管理责任人，询问是否知悉其职责范围。	是□ 否□ 不适用□	
7.1.23.	是否指定人员对网络进行管理，负责运行日志、网络监控记录的日常维护和报警信息分析和处理工作。	a)访谈网络管理员，询问是否知悉其职责范围，包括：负责运行日志、网络监控记录的日常维护和报警信息分析和处理工作； b)查看网络维护记录，判断是否对重要操作步骤进行了记录，对报警信息进行了分析和处理。	是□ 否□ 不适用□	
7.1.24.	是否指定专人对网络和主机进行恶意代码检测并保存检测记录。	a)访谈安全管理员，询问是否对网络和主机进行了恶意代码检测； b)查看恶意代码检测记录，确认对网络和主机进行了恶意代码检测。	是□ 否□ 不适用□	
7.1.25.	是否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。	a)访谈事件与问题管理人员，询问是否记录、分级、分派、处理、监控和结束事件； b)查看事件与问题记录，确认对事件进行了记录、分级、分派、处理、监控，并结束事件。	是□ 否□ 不适用□	
7.1.26.	是否明确部门或责任人，负责本单位软件正版化工作。	检查“表0.11-基本情况”，访谈系统建设负责人，询问是否有专门的部门或人员负责本单位软件正版化工作，由何部门/何人负责。	是□ 否□ 不适用□	

表 A.2　信息技术治理审计底稿（续）

序号	审计项	审计程序	审计结论	备注
7.1.27.	是否指定通报联络人，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。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。	a)查看应急处置联络手册，确认指定了通报联络人，至少包括信息技术负责人及其备岗；确认通报人联络方式至少包括应急值守电话与传真； b)访谈通报联络人，询问是否知悉其职责范围； c)查阅通报联络人正式发文，确认将通报联络人及其联络方式及时通知了监管部门、行业协会和相关单位。	是□ 否□ 不适用□	
7.2.	**机构设置**			
7.2.1.	是否设立信息系统运维组织，负责信息系统的运行维护工作。	a)检查设立信息系统运维组织的正式发文，查看运维岗位分工及岗位职责说明，了解信息系统运维岗位设立情况； b)访谈相关人员，询问是否知悉其职责范围。	是□ 否□ 不适用□	
7.2.2.	是否设立IT治理委员会或类似机构，负责公司IT治理工作。	检查设立IT治理委员会的正式发文，查看是否明确IT治理委员会负责公司IT治理工作。	是□ 否□ 不适用□	
7.2.3.	IT治理委员是否包括公司IT治理直接责任人、IT总监、IT部门负责人、相关业务负责人、财务负责人、内部控制负责人以及部分技术骨干等人员，其中IT人员的比例是否在30%以上。	a)检查设立IT治理委员会的正式发文，查看“表0.1- IT治理委员会或类似机构组成人员”，确定委员包括公司IT治理直接责任人、IT总监、IT部门负责人、相关业务负责人、财务负责人、内部控制负责人以及部分技术骨干等人员，其中IT人员的比例是否在30%以上； b)访谈IT治理委员会委员，询问是否知悉其职责范围。	是□ 否□ 不适用□	
7.2.4.	IT治理委员会是否拟订公司IT治理目标和IT治理工作计划。	检查公司IT治理目标和IT治理工作计划，判断IT治理委员会是否拟订公司IT治理目标和IT治理工作计划。	是□ 否□ 不适用□	
7.2.5.	IT治理委员会是否审议公司IT发展规划。	检查公司IT发展规划审议记录，判断IT治理委员会是否审议公司IT发展规划。	是□ 否□ 不适用□	
7.2.6.	IT治理委员会是否审议公司年度IT工作计划和IT预算。	检查公司年度IT工作计划和IT预算审议记录，判断IT治理委员会是否审议公司年度IT工作计划和IT预算。	是□ 否□ 不适用□	
7.2.7.	IT治理委员会是否审议公司重大IT项目立项、投入和优先级。	检查公司重大IT项目立项、投入和优先级审议记录，判断IT治理委员会是否审议公司重大IT项目立项、投入和优先级。	是□ 否□ 不适用□	

表 A.2　信息技术治理审计底稿（续）

序号	审计项	审计程序	审计结论	备注
7.2.8.	IT治理委员会是否审议公司IT管理制度和重要流程。	检查公司IT管理制度和重要流程审议记录，判断IT治理委员会是否审议公司IT管理制度和重要流程。	是□ 否□ 不适用□	
7.2.9.	IT治理委员会是否制订与IT治理相关的培训和教育工作计划。	检查与IT治理相关的培训和教育工作计划，判断IT治理委员会是否制订与IT治理相关的培训和教育工作计划。	是□ 否□ 不适用□	
7.2.10.	IT治理委员会是否检查所拟订和审议事项的落实和执行情况。	检查拟订和审议事项的落实和执行情况的说明，判断IT治理委员会是否检查所拟订和审议事项的落实和执行情况。	是□ 否□ 不适用□	
7.2.11.	IT治理委员会是否组织评估公司IT重大事项并提出处置意见。	检查公司IT重大事项评估和处置意见，判断IT治理委员会是否组织评估公司IT重大事项并提出处置意见。	是□ 否□ 不适用□	
7.2.12.	IT治理委员会是否向公司管理层报告IT治理状况。	检查IT治理状况报告，判断IT治理委员会是否向公司管理层报告IT治理状况。	是□ 否□ 不适用□	
7.2.13.	是否实现系统开发、系统运维管理和系统的合规检查相互分离。	a)检查组织架构说明和岗位职责说明，判断系统开发、系统运维管理和系统的合规检查在岗位和人员设置上是否相互分离； b)访谈上述岗位人员，询问是否知悉其职责范围。	是□ 否□ 不适用□	
7.2.14.	是否有应急技术支援队伍。	查看应急技术支援队伍名单，访谈应急技术支援队伍成员，了解其是否知悉其职责。	是□ 否□ 不适用□	
7.3.	**审核检查**			
7.3.1.	是否由内部人员或上级单位定期进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等；全面安全检查是否至少每年一次。	a)查看安全检查记录，判断检查内容是否包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等； b)判断全面安全检查是否至少每年一次。	是□ 否□ 不适用□	
7.3.2.	是否制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报。	a)检查是否有安全检查工作表格； b)检查是否有安全检查报告，是否汇总了安全检查数据； c)检查是否有安全检查结果通报。	是□ 否□ 不适用□	

表 A.2　信息技术治理审计底稿（续）

序号	审计项	审计程序	审计结论	备注
7.3.3.	安全管理员是否负责定期进行安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况。安全检查是否至少每季度一次。	a)查看安全检查记录，确定检查内容是否包括系统日常运行、系统漏洞和数据备份等情况； b)确定安全检查是否至少每季度一次。	是□ 否□ 不适用□	
7.4.	**授权审批**			
7.4.1.	是否根据各个部门和岗位的职责明确授权审批部门及批准人；对系统投入运行、网络系统接入和重要资源的访问等事项进行审批；重要审批授权记录应留档备查。	a)检查审批管理制度，查看文档是否明确审批部门、审批人和审批事项； b)检查审批授权记录，判断是否对信息系统中的重要活动进行了审批。	是□ 否□ 不适用□	
7.4.2.	是否针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序，按照审批程序执行审批过程，对重要活动建立逐级审批制度。	a)检查审批管理制度文档，查看文档是否对系统变更、重要操作、物理访问和系统接入等事项建立审批程序； b)检查审批授权记录，判断是否按照审批程序执行审批过程，对重要活动建立逐级审批制度。	是□ 否□ 不适用□	
7.4.3.	每年至少审查一次审批事项。	检查审批事项的审查记录，判断是否每年至少审查一次审批事项。	是□ 否□ 不适用□	
7.4.4.	是否记录审批过程并保存审批文档。	检查审批授权记录，判断是否记录审批过程并保存审批文档。	是□ 否□ 不适用□	

附 录 B
（规范性附录）
机房管理审计底稿

表B.1至表B.2给出了机房管理审计的程序、内容及相关记录要求。

表B.1 机房管理审计底稿

被审计部门：	索引号：JFGL
审计主题：机房管理	审计年度：
审计结论、意见及建议： 编制人： 年 月 日 （部门盖章）	
复核意见： 复核人： 年 月 日 （部门盖章）	
被审计部门意见： 年 月 日 （部门盖章）	

表 B.1　机房管理审计底稿（续）

审计证据列表：

表B.2　机房管理审计底稿

序号	审计项	审计程序	审计结论	备注
1.	**电磁防护**			
1.1.	电源线和通信线缆是否铺设在不同的桥架或管道，避免互相干扰。	a)检查机房布线，查看是否做到电源线和通信线缆隔离； b)检查电源线和通信线缆是否铺设在不同的桥架或者管道内。	是□ 否□ 不适用□	
1.2.	机房或机房所在的大楼是否有接地措施，并且接地电阻必须小于1欧姆。	a)访谈机房管理员，询问机房或机房所在的大楼是否有接地措施，并且接地电阻必须小于1欧姆； b)检查机房供电线路图，是否机房是否有接地措施；检查机房验收报告，确认接地电阻是否小于1欧姆。	是□ 否□ 不适用□	
2.	**电力**			
2.1.	是否在机房供电线路上配置稳压器和过电压防护设备。	a)检查机房供电系统图及相关说明材料，机房供电线路上是否设置了稳压器和过电压防护设备； b)检查机房维护记录，稳压器和过电压防护设备是否正常运行。	是□ 否□ 不适用□	
2.2.	机房是否配备UPS，是否定期检查和维护，UPS实际供电能力是否能够满足主要设备在断电情况下正常运行2个小时以上。	a)检查“表0.3-UPS”，现场检查UPS实际供电能力是否能够满足主要设备在断电情况下正常运行2个小时以上； b)检查UPS设备运行记录、定期检查和维护记录。	是□ 否□ 不适用□	
2.3.	机房是否自备或租用发电机，能够保障持续供电。	a)检查“表0.3-发电机”，现场是否配备了发电机，检查发电机储油是否能够确保发电机持续供电，是否采取了有效措施确保发电机用油的及时补充； b)如果是租用发电机，检查租用发电机的合同或相关证明材料；该合同或相关证明材料可以确保持续供电； c)检查发电机设备的运行记录、定期检查和维护记录。	是□ 否□ 不适用□	
2.4.	机房是否采用双路市电，双路市电是否能实现自动切换。	a)检查“表0.3-电力情况-供电方式（可多选）”，访谈机房管理员，询问机房是否采用了双路市电； b)检查双路市电线路切换记录或供电部门相关协议，查看双路市电是否能够自动切换。	是□ 否□ 不适用□	

表 B.2　机房管理审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.5.	机房是否配备单独的配电柜。	访谈机房管理员，询问机房是否配备单独的配电柜。	是□ 否□ 不适用□	
2.6.	机房是否有独立于一般照明电的专用供配电线路。	检查机房供电线路图，是否有独立于一般照明电的专用供配电线路。	是□ 否□ 不适用□	
3.	**防火**			
3.1.	机房是否设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火；机房的火灾自动消防系统是否向当地公安消防部门备案。	a)查看“表0.3-消防情况”，火灾自动报警系统是否是经消防检测部门检测合格的产品，是否处于正常运行状态，是否有火灾自动报警系统的运行记录； b)检查机房的火灾自动报警系统向当地公安消防部门备案的相关材料。	是□ 否□ 不适用□	
3.2.	机房及相关的工作房间和辅助房是否采用具有耐火等级的建筑材料。	a)访谈物理安全负责人，询问机房及相关的工作房间和辅助房是否采用具有耐火等级的建筑材料； b)检查机房验收合格证明，是否有耐火等级建筑材料的说明。	是□ 否□ 不适用□	
3.3.	机房是否采取区域隔离防火措施，将重要设备与其他设备隔离开。	a)访谈物理安全负责人，询问机房是否采取区域隔离防火措施，将重要设备与其他设备隔离开； b)检查机房验收合格证明，是否将放置重要设备的区域与放置其他设备的区域隔离开。	是□ 否□ 不适用□	
3.4.	机房工作人员是否熟悉逃生路线和自我保护措施，防止发生人身安全意外。	a)查看机房逃生路线图等资料； b)访谈机房工作人员，了解其是否熟悉逃生路线和自我保护措施。	是□ 否□ 不适用□	
3.5.	是否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。	现场检查是否将消防安全警示和指示张贴于机房明显位置，是否将消防设施的操作要点张贴于消防设施旁边。	是□ 否□ 不适用□	
3.6.	机房工作人员是否熟悉消防设施及操作要点，掌握消防应急措施。	检查消防演练记录，访谈机房工作人员，确认是否熟悉消防设施及操作要点，掌握消防应急措施。	是□ 否□ 不适用□	
3.7.	是否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。	检查机房维护记录，确定是否每季度至少一次对机房内消防报警设备进行检查。	是□ 否□ 不适用□	

表 B.2　机房管理审计底稿（续）

序号	审计项	审计程序	审计结论	备注
4.	**防静电**			
4.1.	主要设备是否采用必要的接地防静电措施。	检查机房验收合格证明，主要设备是否有接地构造或其他静电泄放措施。	是□ 否□ 不适用□	
4.2.	机房是否采用防静电地板。	检查机房验收合格证明，是否采用了防静电地板或敷设防静电地板。	是□ 否□ 不适用□	
5.	**防雷击**			
5.1.	机房或机房所在大楼，是否设计并安装防雷击措施，防雷措施是否至少包括避雷针或避雷器等。	a)访谈物理安全负责人，询问机房所在建筑物是否设置了避雷装置，是否通过验收或国家有关部门的技术检测； b)检查机房所在建筑物的防雷验收文档中是否有设置避雷装置的说明。	是□ 否□ 不适用□	
5.2.	机房是否设置交流电源地线。	a)访谈物理安全负责人，询问机房是否设置有交流电源地线； b)检查机房验收合格证明，是否有设置交流电源地线的说明。	是□ 否□ 不适用□	
5.3.	是否设置防雷保安器，防止感应雷。	a)访谈物理安全负责人，询问机房是否设置有防雷保安器，防止感应雷； b)检查机房验收合格证明，是否有设置防雷保安器的说明。	是□ 否□ 不适用□	
6.	**防水防潮**			
6.1.	水管安装，是否穿过机房屋顶和活动地板下。	a)访谈物理安全负责人，询问机房水管安装，是否穿过机房屋顶和活动地板下； b)检查机房验收合格证明，是否水管安装穿过机房屋顶和活动地板下。	是□ 否□ 不适用□	
6.2.	与机房设备无关的水管是否禁止穿过机房屋顶和活动地板下。	a)访谈物理安全负责人，询问与机房设备无关的水管是否禁止穿过机房屋顶和活动地板下； b)检查机房验收合格证明，与机房设备无关的水管是否禁止穿过机房屋顶和活动地板下。	是□ 否□ 不适用□	
6.3.	机房屋顶和活动地板下铺有水管的，是否采取有效防护措施。	a)访谈物理安全负责人，询问机房屋顶和活动地板下铺有水管的，是否采取有效防护措施； b)检查机房验收合格证明，机房屋顶和活动地板下铺有水管的，是否采取有效防护措施。	是□ 否□ 不适用□	

表 B.2　机房管理审计底稿（续）

序号	审计项	审计程序	审计结论	备注
6.4.	是否采取措施防止雨水通过机房窗户、屋顶和墙壁渗透。	a)检查机房验收合格证明，是否采取措施防止雨水通过机房窗户、屋顶和墙壁渗透。 b)检查机房的窗户、屋顶和墙壁等是否未出现过漏水、渗透和返潮现象，机房的窗户、屋顶和墙壁是否进行过防水防渗处理。	是□ 否□ 不适用□	
6.5.	是否采取措施防止机房内水蒸气结露和地下积水的转移与渗透。	a)访谈物理安全负责人，询问机房是否采取措施防止机房内水蒸气结露和地下积水的转移与渗透； b)检查机房验收合格证明，机房是否采取措施防止机房内水蒸气结露和地下积水的转移与渗透。	是□ 否□ 不适用□	
6.6.	是否安装对水敏感的检测仪表或元件，对机房进行防水检测和报警。	a)检查机房验收合格证明，是否设置对水敏感的检测仪表或元件，对机房进行防水检测和报警。 b)查看对水敏感的检测仪表或元件是否有运行维护记录。	是□ 否□ 不适用□	
7.	**机房安保**			
7.1.	机房是否按照消防要求和管理要求进行合理分区，区域和区域之间设置物理隔离装置。	检查机房平面图，并现场检查，是否在不同区域间设置了物理隔离装置。	是□ 否□ 不适用□	
7.2.	机房重要区域前是否设置专门的过渡区域，用于设备的交付或安装。（重要区域包括：主机房、辅助区、支持区等功能区域）	检查机房平面图，并现场检查，重要区域（包括：主机房、辅助区、支持区等功能区域）之前是否设置专门的过渡区域。	是□ 否□ 不适用□	
7.3.	机房是否合理划分区域，包括主机房、辅助区、支持区等功能区域。	检查机房平面图，并现场检查，是否包括：主机房、辅助区、支持区等功能区域。	是□ 否□ 不适用□	
7.4.	重要区域是否配置电子门禁系统，控制、鉴别和记录进入的人员。	a)检查机房的设计、验收文档或相关证据，查看机房重要区域是否配置电子门禁系统； b)检查电子门禁系统记录，查看是否能够控制、鉴别和记录进入人员； c)现场检查门禁系统是否能正常工作。	是□ 否□ 不适用□	
7.5.	操作间与设备间是否分隔。	检查机房平面图，并现场检查，操作间与设备间是否有效分隔。	是□ 否□ 不适用□	
7.6.	是否将主要设备放置在机房内。	a)获取主要设备清单列表； b)现场检查主要设备等是否放置在机房内。	是□ 否□ 不适用□	

表 B.2　机房管理审计底稿（续）

序号	审计项	审计程序	审计结论	备注
7.7.	机房主要设备是否安装、固定在机柜内或机架上。	现场检查机房主要设备是否安装、固定在机柜内或机架上。	是□ 否□ 不适用□	
7.8.	主要设备、机柜、机架应有明显且不易除去的标识，如粘贴标签或铭牌。	现场查看主要设备、机柜、机架是否有明显不易除去的标签或铭牌。	是□ 否□ 不适用□	
7.9.	是否将通信线缆铺设在隐蔽处，通信线缆可铺设在管道或线槽、线架中。	现场检查通信线缆是否铺设在管道或线槽、线架中。	是□ 否□ 不适用□	
7.10.	是否利用光、电等技术设置机房防盗报警系统。	a)查看机房的设计、验收文档或相关证据，查看机房是否安装利用光、电等技术的防盗报警系统； b)现场检查是否有利用光、电等技术的防盗报警系统。	是□ 否□ 不适用□	
7.11.	机房出入口的监控录像是否保存90天。	检查机房监控录像，确认是否有有效的机房出入口监控录像，并存有最近90天记录。	是□ 否□ 不适用□	
7.12.	外来人员进入机房是否经过申请和审批流程，是否限制和监控其活动范围，是否有专人陪同。	检查外来人员进出机房的申请和审批记录，是否有外来人员机房活动范围的限制，并有专人陪同。	是□ 否□ 不适用□	
7.13.	是否实行外来设备未经批准不得接入生产环境。	检查设备上线审批相关材料，确认外来设备是否都经过审批才能接入生产环境。	是□ 否□ 不适用□	
8.	**机房运维**			
8.1.	是否每季度对机房供配电、空调、UPS等设施进行维护管理并保存相关维护记录。	检查维护记录，查验是否每季度对机房供配电、空调、UPS等设备进行维护管理。	是□ 否□ 不适用□	
8.2.	是否每年对防盗报警、防雷、消防等装置进行检测维护并保存相关维护记录。	检查维护记录，查验是否每年对防盗报警、防雷、消防等装置进行检测维护。	是□ 否□ 不适用□	
8.3.	是否定期检查防水、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。	检查机房维护记录，判断是否定期检查防水、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。	是□ 否□ 不适用□	
8.4.	是否保持机房环境卫生，采取防尘措施，定期进行除尘处理。	a)检查机房的设计、验收文档或相关证据，查看是否采取防尘措施； b)检查机房维护记录，是否定期进行除尘处理。	是□ 否□ 不适用□	

表 B.2　机房管理审计底稿（续）

序号	审计项	审计程序	审计结论	备注
8.5.	交易时间内是否未进行机房施工、保洁操作。	检查机房维护记录，是否未在交易时间进行机房施工和保洁。	是□ 否□ 不适用□	
8.6.	是否采取监控措施，配备监控和报警工具，报警方式可包括声光、电话、短信、邮件等。	检查“表0.3-机房监控情况”，访谈运维负责人，判断是否采取监控措施，配备监控和报警工具，报警方式可包括声光、电话、短信、邮件等。	是□ 否□ 不适用□	
8.7.	机房监控指标是否包括电力状态、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。	查看“表0.3-机房监控情况-机房环境”和机房环境监控日志文件，查看监控指标是否包括：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。	是□ 否□ 不适用□	
8.8.	网络与通信监控指标是否包括设备运行状态、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。	查看“表0.3-机房监控情况-网络通信”和网络与通信设备监控日志文件，查看监控指标是否包括：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。	是□ 否□ 不适用□	
8.9.	安全设备监控指标是否包括：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。	查看“表0.3-机房监控情况-安全设备”和安全设备监控日志文件，查看监控指标是否包括：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。	是□ 否□ 不适用□	
9.	**空调**			
9.1.	机房是否设置温、湿度自动调节设施，机房温度是否控制在22℃-24℃。	a)检查机房内是否配备了温湿度自动调节设施，温湿度自动调节设施是否能够正常运行； b)检查机房温湿度记录，机房温度是否控制在22℃-24℃。	是□ 否□ 不适用□	
9.2.	机房是否设置温、湿度自动调节设施，机房相对湿度是否控制在40%-55%。	a)检查机房内是否配备了温湿度自动调节设施，温湿度自动调节设施是否能够正常运行； b)检查机房温湿度记录，机房相对湿度是否控制在40%-55%。	是□ 否□ 不适用□	
9.3.	是否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。	审阅空调设备检查维护记录，是否每季度至少一次对空调设备进行全面检查和维护。	是□ 否□ 不适用□	
9.4.	是否安装独立的空调设备。	检查“表0.3-空调”和机房空调情况说明，判断是否安装了独立的空调设备。	是□ 否□ 不适用□	

表 B.2　机房管理审计底稿（续）

序号	审计项	审计程序	审计结论	备注
10.	**物理位置**			
10.1.	机房或机房所在建筑物是否符合当地抗震要求的相关证明。	a)访谈物理安全负责人，询问机房所在建筑物是否具有防震能力； b)检查机房的设计、验收文档或相关证据，查看机房所在建筑的防震能力说明。	是□ 否□ 不适用□	
10.2.	机房外墙壁是否没有对外的窗户。否则是否采用双层固定窗，并作密封、防水处理。	如果机房外墙壁有对外的窗户，检查是否采用了双层固定窗，并做了密封、防水处理。	是□ 否□ 不适用□	
10.3.	机房场地不宜设在建筑物顶层，如果不可避免，是否采取有效的防水措施。机房场地设在建筑物地下室的，是否采取有效的防水措施。	a)访谈物理安全负责人，询问机房所在建筑物是否具有防水能力； b)检查机房的设计、验收文档或相关证据，查看机房采取的防水措施。	是□ 否□ 不适用□	
10.4.	机房场地设在建筑物高层的，是否对设备采取有效固定措施。	a)访谈物理安全负责人，询问是否对设备采取有效固定措施； b)检查机房的设计、验收文档或相关证据，查看对设备采取的固定措施； c)检查设计、验收文档是否与机房实际情况相符合。	是□ 否□ 不适用□	
10.5.	如果机房周围有用水设备，是否有防渗水和疏导措施。	a)访谈物理安全负责人，询问是否有防渗水和疏导措施； b)检查机房的设计、验收文档或相关证据，查看机房采取的防渗水和疏导措施。	是□ 否□ 不适用□	
11.	**用电安全**			
11.1.	机房管理员是否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。	检查机房用电管理规定，查看是否具有重点保障核心交易业务系统用电安全的措施。	是□ 否□ 不适用□	
11.2.	机房管理员是否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。	a)检查机房管理员安全用电培训记录，查看机房管理员是否获得培训合格证明； b)检查机房用电应急处理、应急演练操作记录，查看应急处理是否正确完成； c)审阅机房管理员相关技能证明材料（可选）； d)审阅机房管理员相关信息，了解是否配备专业电工（可选）； e)审阅与相关电力机构或物业机构签署的服务协议（如有）。	是□ 否□ 不适用□	

表 B.2　机房管理审计底稿（续）

序号	审计项	审计程序	审计结论	备注
11.3.	是否在危险性高的位置张贴相应的用电安全警示或操作指引。	现场检查是否在危险性高的位置张贴相应的用电安全警示或操作指引。	是□ 否□ 不适用□	
11.4.	是否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。	a)检查机房维护记录，是否至少每季度一次对机房供配电、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； b)检查机房维护记录，是否具有定期测试备用供电系统，确保持续供电设施的有效性的记录。	是□ 否□ 不适用□	
11.5.	未经审批是否禁止接入其他用电设备。	审阅其它用电设备接入申请记录，检查是否接入其他用电设备都有相应的审批。	是□ 否□ 不适用□	

附 录 C
（规范性附录）
网络管理审计底稿

表C.1至表C.2给出了网络管理审计的程序、内容及相关记录要求。

表C.1 网络管理审计底稿

被审计部门：	索引号：WLGL
审计主题：网络管理	审计年度：
审计结论、意见及建议： 编制人： 年 月 日 （部门盖章）	
复核意见： 复核人： 年 月 日 （部门盖章）	
被审计部门意见： 年 月 日 （部门盖章）	

表 C.1　网络管理审计底稿（续）

审计证据列表：

表C.2　网络管理审计底稿

序号	审计项	审计程序	审计结论	备注
1.	结构安全			
1.1.	是否保证主要网络设备的业务处理能力具备冗余空间，满足业务高峰期需要；关键网络设备近一年的CPU负载峰值应小于30%。	a)访谈网络管理员，主要网络设备的业务处理能力是否具备冗余空间，能否满足业务高峰期需要，近一年关键网络设备CPU负载峰值； b)检查网络设计和验收文档，查看是否有满足主要路由器、交换机、网关、防火墙、入侵检测设备业务处理能力需要的设计或描述； c)检查网络运行报告、网络监控日志，查看主要路由器、交换机、网关、防火墙、入侵检测设备近一年的CPU负载峰值是否小于30%。	是□ 否□ 不适用□	
1.2.	是否保证网络各个部分的带宽满足业务高峰期需要。	a)访谈网络管理员，是否保证网络各个部分的带宽满足业务高峰期需要； b)检查网络设计和验收文档、业务设计文档，查看是否有满足网络各个部分主要路由器、交换机、网关业务高峰期带宽需要的设计或描述； c)检查网络监控日志，查看网络各个部分主要路由器、交换机、网关的带宽使用率峰值是否满足业务高峰期需要。	是□ 否□ 不适用□	
1.3.	是否在业务终端与业务服务器之间进行路由控制建立安全的访问路径；业务终端和业务服务器应放置在不同的子网内，并建立安全的访问路径。	a)检查网络设计和验收文档，查看是否有业务终端和业务服务器放置在不同的子网内的设计或描述； b)检查边界和主要路由器、交换机、防火墙、网关的路由控制策略，查看是否建立安全的访问路径。	是□ 否□ 不适用□	
1.4.	是否提供主要网络设备、通信线路和数据处理系统的硬件冗余，保证系统的高可用性。	a)询问网络管理员，是否提供主要网络设备、通信线路和数据处理系统的硬件冗余； b)检查主要路由器、交换机、网关等是否提供硬件冗余； c)检查主要数据处理系统（如终端设备、数据库服务器、中间件服务器、应用服务器等）是否提供硬件冗余。	是□ 否□ 不适用□	

表 C.2　网络管理审计底稿（续）

序号	审计项	审计程序	审计结论	备注
1.5.	是否避免将重要网段部署在网络边界处且直接连接外部信息系统。	a)检查网络设计文档或网络验收文档及网络拓扑图，查看重要网段的部署方式； b)检查边界和主要网络设备，查看重要网段是否采取了技术隔离手段与其他网段隔离。	是□ 否□ 不适用□	
1.6.	重要网段与其他网段之间是否采取可靠的技术隔离手段。	a)检查“表 0.3-网络边界防护情况”、网络设计文档或网络验收文档及网络拓扑图，查看重要网段的部署方式； b)检查边界和主要网络设备，查看重要网段是否采取了技术隔离手段与其他网段隔离。	是□ 否□ 不适用□	
1.7.	是否采用冗余技术设计网络拓扑结构，避免关键节点存在单点故障。	a)询问网络管理员，是否采用冗余技术设计网络拓扑结构； b)检查网络设计文档、网络拓扑结构关键节点是否有冗余。	是□ 否□ 不适用□	
1.8.	主通信线路的带宽是否考虑充分的冗余，本地局域网的网络时延应小于 50ms。中介服务机构与其他参与方之间的通信线路，是否根据承载的通信量保证足够的带宽。	a)检查网络设计文档或验收文档，主通信线路的带宽是否考虑充分的冗余； b)现场查看本地局域网的网络时延是否小于 50ms。	是□ 否□ 不适用□	
2.	**网络运维**			
2.1.	是否绘制与当前运行情况相符的网络拓扑结构图；是否绘制完整的网络拓扑结构图，有相应的网络配置表，包含设备 IP 地址等主要信息，与当前运行情况相符，并及时更新。	a)检查网络设计和验收文档，查看网络拓扑结构图，是否有相应的网络配置表，包含设备 IP 地址等主要信息，并及时更新； b)抽查部分终端设备、服务器、路由器、防火墙等，验证网络拓扑结构图与当前运行情况是否相符。	是□ 否□ 不适用□	

表 C.2 网络管理审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.2.	是否根据各部门的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的子网或网段，并按照方便管理和控制的原则为各子网、网段分配地址段。	a)访谈网络管理员，是否根据各部门的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的子网或网段； b)检查网络设计和验收文档，查看是否有根据各部门的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的子网或网段，并按照方便管理和控制的原则为各子网和网段分配地址段的设计或描述； c)抽查部分终端设备和服务器，验证 IP 地址符合设计和验收文档。	是□ 否□ 不适用□	
2.3.	是否根据厂家提供的软件升级版本对网络设备进行更新，并在更新前对现有的重要文件进行备份。	a)访谈网络管理员，是否根据厂家提供的软件升级版本对网络设备进行更新； b)查看软件升级变更操作记录； c)抽查升级操作记录是否有对应的备份数据或者备份记录。	是□ 否□ 不适用□	
2.4.	是否持续跟踪厂商提供的网络设备的软件升级更新情况，在经过充分的测试评估后对必要的补丁进行更新，并在更新前对现有的重要文件进行备份。	a)访谈网络管理员是否持续跟进厂商提供的网络设备的软件升级更新情况； b)查看补丁升级变更操作记录； c)查看变更操作变更评估会议纪要或评审流程； d)查看升级操作记录日期是否有对应的备份数据。	是□ 否□ 不适用□	
2.5.	是否保证所有与外部系统的连接均得到授权和批准。	a)访谈网络管理员，了解网络外联原则和外联审批程序； b)检查网络外联审批文档记录； c)查看网络访问控制列表。	是□ 否□ 不适用□	
2.6.	是否实现设备的最小服务配置，并对配置文件进行定期离线备份；是否在配置变更前、变更后分别对网络设备的配置文件进行备份。	a)访谈网络管理员，了解三级保护系统服务开放策略、网络设备配置文件备份策略； b)检查网络设备的配置文件，抽查关键网络设备的参数配置； c)检查是否具有网络设备配置文件的备份文件，是否离线备份； d)检查在设备配置变更前后，是否对网络设备的配置文件进行了备份。	是□ 否□ 不适用□	

表 C.2　网络管理审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.7.	是否配置、调优网络系统的参数。	a)访谈网络管理员网络参数配置、调优机制； b)对照网络配置文件，抽查关键路由器、交换机、防火墙、网关等网络设备的参数配置，询问网络管理员调优的配置。	是□ 否□ 不适用□	
2.8.	是否禁止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。	a)查看机房管理制度或变更管理制度，是否规定了原则上禁止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； b)抽查变更记录，是否做到原则上不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。	是□ 否□ 不适用□	
2.9.	是否禁止通过无线网络对交易业务网进行网络管理。	a)询问网络管理员，能否通过无线网络对交易业务网进行网络管理； b)查看网络安全管理制度，检查是否有不允许通过无线网进行接入管理的规定； c)查看交易业务网管理策略，检查是否有不允许通过无线网进行接入的限制； d)审阅网络拓扑图，确认网络管理系统未通过无线网接入的方式管理交易业务网。	是□ 否□ 不适用□	
2.10.	计算机网络跳线是否整齐干净，跳线标识清晰。	a)检查机房管理制度是否对标识有要求； b)现场观察公司网络跳线情况，计算机网络跳线是否应整齐干净，跳线标识清晰。	是□ 否□ 不适用□	
2.11.	是否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。	a)检查网络信息点使用表，检查是否对网络信息点进行管理和编制； b)检查对信息点是否进行了及时维护和更新，确保与实际情况一致。	是□ 否□ 不适用□	
2.12.	是否保持网络设备的可用性，及时维修、更换故障设备。	检查网络设备事件记录，结合网络设备故障、维修、更换记录档案，判断时间点上的及时性。	是□ 否□ 不适用□	

表 C.2 网络管理审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.13.	是否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。	a)询问是否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； b)随机抽查一个交换机端口，检查是否处于受控状态。	是□ 否□ 不适用□	
3.	**访问控制**			
3.1.	网络边界是否部署访问控制设备并启用访问控制功能。	a)询问网络管理员，网络边界是否部署访问控制设备并启用访问控制功能； b)检查网络拓扑图，网络边界是否部署访问控制设备； c)检查访问控制设备的访问控制策略，查看其是否根据会话状态信息对数据流进行控制。	是□ 否□ 不适用□	
3.2.	是否能根据会话状态信息为数据流提供明确的允许/拒绝访问的能力，控制粒度为端口级。	a)询问网络管理员，是否为数据流提供明确的允许/拒绝访问的能力，控制粒度为端口级； b)检查边界网络设备的访问控制策略，是否为数据流提供明确的允许/拒绝访问的能力，控制粒度为端口级。	是□ 否□ 不适用□	
3.3.	是否按用户和系统之间的允许访问规则，决定允许或拒绝用户对受控系统进行资源访问，控制粒度为单个用户。	a)询问网络管理员，是否按用户和系统之间的允许访问规则，对受控系统进行资源访问，控制粒度为单个用户； b)检查边界网络设备的访问控制策略，查看是否按用户和系统之间的允许访问规则，对受控系统进行资源访问，控制粒度为单个用户。	是□ 否□ 不适用□	
3.4.	是否限制具有拨号访问权限的用户数量。原则上不应通过互联网对重要信息系统进行远程维护和管理。	a)检查边界网络设备的拨号用户列表，查看其是否对具有拨号访问权限的用户数量进行限制； b)访谈网络管理员，检查是否禁止了通过互联网对重要信息系统进行远程维护和管理； c)现场检查是否存在拨号接入网络的方式；如果存在拨号接入，检查边界网络设备(如路由器，防火墙，认证网关)，查看是否正确的配置了拨号访问控制列表（对系统资源实现允许或拒绝访问）。	是□ 否□ 不适用□	

表 C.2　网络管理审计底稿（续）

序号	审计项	审计程序	审计结论	备注
3.5.	是否在会话处于非活跃一定时间或会话结束后终止网络连接。	访谈网络管理员，现场检查边界网络设备，查看是否有会话处于非活跃的时间或会话结束后自动终止网络连接的配置。	是□ 否□ 不适用□	
3.6.	是否限制网络最大流量数及网络连接数。	访谈网络管理员，现场检查边界网络设备，是否限制网络最大流量数及网络连接数。	是□ 否□ 不适用□	
3.7.	重要网段是否采取技术手段防止地址欺骗。	a)询问网络管理员重要网段是否采取技术手段防止地址欺骗； b)审核防地址欺骗策略。	是□ 否□ 不适用□	
3.8.	是否制定网络访问控制策略，是否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。	a)查看网络拓扑图结构，检查网络边界重要设备是否按照访问控制策略，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； b)获取访问控制策略变更记录，检查变更是否经过合理有效审批。	是□ 否□ 不适用□	
3.9.	系统管理员、安全管理员、安全审计员等设备特权用户的权限是否分离。	a)审阅信息技术部门的组织架构和岗位职责说明，确认系统管理员、安全管理员、安全审计员的职责有明确划分； b)检查主要网络设备的用户权限清单，确认对系统管理员、安全管理员、安全审计员等设备特权用户的权限进行了分离。	是□ 否□ 不适用□	
3.10.	是否采取限制 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。	a)询问网络管理员，是否采取限制 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； b)检查重要服务器、安全设备、主干交换机、路由器及防火墙的访问控制策略，查看是否开启身份认证，是否根据 IP 地址设置安全策略，控制资源访问。	是□ 否□ 不适用□	
4.	**安全审计**			
4.1.	是否对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录。	a)检查边界和主要网络设备的安全审计策略，查看是否包含网络系统中的网络设备运行状况、网络流量、用户行为等； b)检查边界和关键网络设备的安全审计记录。	是□ 否□ 不适用□	

表 C.2 网络管理审计底稿（续）

序号	审计项	审计程序	审计结论	备注
4.2.	审计记录是否包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。	检查边界和主要网络设备的安全审计记录，查看是否包括：事件的日期和时间、用户、事件类型、事件成功情况，及其他与审计相关的信息。	是□ 否□ 不适用□	
4.3.	是否能够根据网络系统中的网络设备运行状况、网络流量、用户行为等日志记录进行分析，并生成审计报表。	检查边界和主要网络设备，查看是否为授权用户浏览和分析审计数据提供专门的审计工具，并能根据需要生成审计报表。	是□ 否□ 不适用□	
4.4.	是否对审计记录进行保护，避免受到未预期的删除、修改或覆盖等。	a)询问网络管理员审计记录保护机制； b)查看审计保护机制设计文档； c)测试边界和主要网络设备，通过以某个非审计用户登录系统，试图删除、修改或覆盖审计记录，验证安全审计的保护情况与要求是否一致。	是□ 否□ 不适用□	
4.5.	是否定期检查网络设备的用户、口令及权限设置的正确性。	审阅网络设备安全检查记录或第三方网络安全检查记录，查看是否定期检查网络设备的用户、口令及权限设置的正确性，删除网络设备上的默认用户或修改默认用户的口令，没有使用缺省口令、空口令、弱口令。	是□ 否□ 不适用□	
4.6.	网络管理是否定期对系统容量进行检查和评估，形成评估报告。	a)访谈网络管理员是否定期对系统容量进行检查和评估； b)检查容量评估报告。	是□ 否□ 不适用□	
5.	**安全管理**			
5.1.	是否能够检查内部网络用户采用双网卡跨接外部网络，或采用电话拨号、ADSL 拨号、手机、无线上网卡等无线拨号方式连接其他外部网络。	a)检查边界完整性检查设备的非法外联策略，查看是否设置了对非法连接到外网的行为进行监控并有效的阻断的配置； b)测试边界完整性检查设备，测试是否能够确定出非法外联设备的位置，并对其进行有效阻断。	是□ 否□ 不适用□	
5.2.	是否能够对非授权设备私自联到内部网络的行为进行检查，准确定出位置，并对其进行有效阻断。	a)检查边界完整性检查设备的非授权接入策略，查看是否设置了对非法连接到内网的行为进行监控并有效的阻断的配置； b)测试边界完整性检查设备，测试是否能够对非授权设备私自接入内部网络的行为进行检查，并准确定出位置，对其进行有效阻断。	是□ 否□ 不适用□	

表 C.2　网络管理审计底稿（续）

序号	审计项	审计程序	审计结论	备注
5.3.	是否定期检查安全隔离情况，确保各安全域之间有效隔离。	a)查看包括自建和托管机房的网络拓扑图、安全域划分情况，检查各安全域之间是否采用了防火墙或安全网关等有效隔离方式和隔离手段； b)审阅最近的网络运行情况报告，判断是否定期对上述事项进行了检查。	是□ 否□ 不适用□	
5.4.	是否在网络边界处监视以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击和网络蠕虫攻击等。	a)检查“表 0.3-该机房的网络安全检查情况”、网络入侵防范设备，查看是否能检测以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击、网络蠕虫攻击等； b)检查入侵防范设备是否根据系统应用要求进行了规则配置。	是□ 否□ 不适用□	
5.5.	当检测到攻击行为时，是否记录攻击源 IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时是否提供报警。	检查网络入侵防范设备的入侵报警记录，查看记录中是否包括入侵的源 IP、攻击的类型、攻击的目的、攻击的时间等。	是□ 否□ 不适用□	
5.6.	是否在网络边界处对恶意代码进行检测和清除。	查看网络安全规划文档和访谈网络安全管理员，检查网络边界恶意代码防护策略，检查在网络边界及核心业务网段处是否有相应的防恶意代码措施，如果部署了主机恶意代码检测系统，网络边界恶意代码检测系统可选择安装部署。	是□ 否□ 不适用□	
5.7.	是否维护恶意代码库的升级和检测系统的更新。	a)检查防恶意代码产品，查看其运行是否正常，恶意代码库是否及时更新； b)可对不同安全域区别对待，在确保系统安全运行的前提下，更新恶意代码库。	是□ 否□ 不适用□	
5.8.	是否定期对网络系统进行漏洞扫描，对发现的网络系统安全漏洞进行及时的修补。	a)查看网络安全规划文档，检查网络系统是否配置漏洞扫描策略； b)查看漏洞扫描记录，检查是否定期对网络系统进行漏洞扫描； c)查看修补漏洞记录，检查是否根据漏洞扫描结果，及时进行漏洞修补。	是□ 否□ 不适用□	

表 C.2 网络管理审计底稿（续）

序号	审计项	审计程序	审计结论	备注
5.9.	是否每季度至少进行一次漏洞扫描，对漏洞风险持续跟踪，在经过充分的验证测试后对必要的漏洞开展修补工作。	a)访谈网络管理员，询问是否每季度对网络进行漏洞扫描，发现漏洞如何处理； b)检查漏洞扫描报告，确认每季度对网络系统进行了漏洞扫描； c)检查漏洞修补（变更）报告，确认对发现的网络系统安全漏洞进行了风险评估并及时修补，完成修补工作后进行了验证测试。	是□ 否□ 不适用□	
5.10.	是否实施漏洞扫描或漏洞修补前，对可能的风险进行评估和充分准备，如选择恰当时间，并做好数据备份和回退方案。	a)访谈网络管理员，询问是否实施漏洞扫描或漏洞修补前，对可能的风险进行评估和充分准备； b)检查漏洞修补（变更）记录，是否对可能的风险进行评估，是否有评估审批记录或者会议纪要，是否进行充分准备，如选择恰当时间，是否根据情况进行数据备份、制定回退方案。	是□ 否□ 不适用□	
5.11.	是否在漏洞扫描或漏洞修补后进行验证测试，以保证网络系统的正常运行。	a)访谈网络管理员，询问是否在漏洞扫描或漏洞修补后应进行验证测试； b)查看漏洞修补（变更）记录，是否有验证测试记录。	是□ 否□ 不适用□	
5.12.	是否依据安全策略允许或者拒绝便携式和移动式设备的网络接入。	a)访谈网络管理员，了解便携式和移动式设备的网络接入控制策略； b)检查网络访问控制列表或网络访问控制策略，查看是否有允许或者拒绝便携式和移动式设备接入网络的措施。	是□ 否□ 不适用□	
5.13.	是否定期检查违反规定拨号上网或其他违反网络安全策略的行为。	a)访谈网络管理员，了解是否有检查网络违规行为（如拨号上网等）的检查手段和工具； b)查看网络监控日志，是否有违反规定拨号上网或其他违反网络安全策略的行为。	是□ 否□ 不适用□	
5.14.	是否合理设置安全域，绘制网络拓扑图，并保持更新。	a)访谈网络管理员，是否设置安全域和绘制网络拓扑图，以及更新机制； b)查看网络拓扑图结构，核实网络管理员描述的安全域； c)检查网络边界是否部署了访问控制设备并启用了访问控制功能，是否有更新记录。	是□ 否□ 不适用□	

表 C.2　网络管理审计底稿（续）

序号	审计项	审计程序	审计结论	备注
5.15.	是否综合运用防火墙、入侵检测等安全设备，保护网络与系统；是否正确设置安全设备的接口参数和过滤规则。	a)访谈网络管理员安全访问控制策略； b)审阅网络拓扑图，查看防火墙、入侵检测等安全设备的配备情况； c)查看安全设备的接口参数、过滤规则等相关文档资料； d)查看安全测试记录或第三方安全测试报告。	是□ 否□ 不适用□	
5.16.	是否定期检查防病毒网关和邮件防病毒网关的恶意代码库的升级情况并进行记录，对截获的危险病毒或恶意代码进行及时分析处理，并形成书面的报表和总结汇报。	a)询问安全管理员，防病毒网关和邮件防病毒网关的恶意代码库的升级机制； b)检查恶意代码库的升级记录，判断是否定期； c)检查恶意代码分析报告，确认对防病毒网关和邮件防病毒网关上截获的危险病毒或恶意代码进行了及时分析处理。	是□ 否□ 不适用□	
6.	**身份鉴别**			
6.1.	是否删除默认用户或修改默认用户的口令，根据管理需要开设用户，不得使用缺省口令、空口令、弱口令。	检查是否已经删除默认用户或修改默认用户的口令，根据管理需要开设用户，不得使用缺省口令、空口令、弱口令。	是□ 否□ 不适用□	
6.2.	是否对网络设备的管理员登录地址进行限制。	a)查阅安全管理相关制度，查看对管理员登录地址的限制策略，评估其合理性； b)现场抽查关键网络设备，检验管理员登录地址限制策略是否被严格执行。	是□ 否□ 不适用□	
6.3.	网络设备用户的标识是否唯一。	检查网络设备用户列表，标识是否唯一。	是□ 否□ 不适用□	
6.4.	口令是否符合以下条件：数字、字母、符号混排，无规律的方式。	检查口令管理制度，是否规定口令符合以下条件：数字、字母、符号混排，无规律的方式。	是□ 否□ 不适用□	
6.5.	管理员用户口令的长度至少为 12 位。	检查口令管理制度，是否规定管理员用户口令的长度至少为 12 位。	是□ 否□ 不适用□	
6.6.	管理员用户口令至少每季度更换 1 次，更新的口令至少 5 次内不能重复。	检查口令管理制度，是否规定管理员用户口令至少每季度更换 1 次，更新的口令至少 5 次内不能重复。	是□ 否□ 不适用□	

表 C.2　网络管理审计底稿（续）

序号	审计项	审计程序	审计结论	备注
6.7.	如果设备口令长度不支持 12 位或其他复杂度要求，口令是否使用所支持的最长长度并适当缩小更换周期；也可以使用动态密码卡等一次性口令认证方式。	检查口令管理制度，是否规定口令应使用所支持的最长长度并适当缩小更换周期，也可以使用动态密码卡等一次性口令认证方式。	是□ 否□ 不适用□	
6.8.	是否具有登录失败处理功能，采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施。	检查边界和主要网络设备的设备防护策略，查看是否配置了鉴别失败处理功能，包括结束会话、限制非法登录次数、登录连接超时自动退出等。	是□ 否□ 不适用□	
6.9.	当对网络设备进行远程管理时，是否采取必要措施防止鉴别信息在网络传输过程中被窃听。	a)询问网络管理员，当对网络设备进行远程管理时采取的措施； b)检查边界和主要网络设备的设备防护策略，查看是否采取相应措施防止鉴别信息在网络传输过程中被窃听。	是□ 否□ 不适用□	
6.10.	通过本地控制台管理主要网络设备时，是否采用一种或一种以上身份鉴别技术。	检查本地控制台管理网络设备是否采用一种或一种以上身份鉴别技术。	是□ 否□ 不适用□	
6.11.	以远程方式登录主要网络设备，是否采用两种或两种以上组合的鉴别技术进行身份鉴别。	a)询问网络管理员，以远程方式登录主要网络设备，是否采用两种或两种以上组合的鉴别技术进行身份鉴别； b)检查远程方式登录网络设备是否采用两种或两种以上组合的鉴别技术进行身份鉴别。	是□ 否□ 不适用□	
6.12.	是否禁止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，特殊紧急情况下是否采取限制登录 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。	a)询问网络管理员，是否禁止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，特殊紧急情况下的访问策略； b)对防火墙、网络设备、服务器进行远程管理和维护，而特殊紧急情况下是否采取限制登录 IP、使用数字证书或动态口令认证、全程监控等措施确保远程维护的安全性，并要求在操作完成后及时关闭相关端口； c)查看操作记录，判断是否按照规定进行紧急维护。	是□ 否□ 不适用□	

附 录 D
（规范性附录）
运维管理审计底稿

表D.1至表D.2 给出了运维管理审计的程序、内容及相关记录要求。

表D.1 运维管理审计底稿

被审计部门：	索引号：YWGL
审计主题：运维管理	审计年度：
审计结论、意见及建议： 编制人： 年 月 日 （部门盖章）	
复核意见： 复核人： 年 月 日 （部门盖章）	
被审计部门意见： 年 月 日 （部门盖章）	

表 D.1　运维管理审计底稿（续）

审计证据列表：

表D.2　运维管理审计底稿

序号	审计项	审计程序	审计结论	备注
1.	**日常操作**			
1.1.	是否加强对办公环境的保密性管理，规范办公环境人员行为，包括工作人员调离办公室应立即交还该办公室钥匙、不在办公区接待来访人员、工作人员离开座位应确保终端计算机退出登录状态和桌面上没有包含敏感信息的纸档文件等。	a)访谈系统运维负责人，询问为保证办公环境的保密性采取了哪些控制措施，在哪个区域接待来访人员，工作人员调离时是否收回办公室钥匙等； b)检查工作人员调离办公室交接记录是否有办公室钥匙交接内容； c)检查办公环境，查看工作人员离开座位时是否退出登录状态； d)观察工作人员桌面是否无包含敏感信息的纸档文件。	是□ 否□ 不适用□	
1.2.	是否制定值班安排表，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。	a)检查值班安排表； b)检查值班记录，确定值班期间值班人员在岗。	是□ 否□ 不适用□	
1.3.	是否制定交接班流程，并严格执行，留存记录。	a)检查交接班流程； b)检查交接班记录，判断是否严格执行。	是□ 否□ 不适用□	
1.4.	是否设置运维值班电话，并保持畅通。	a)检查运维操作手册，是否有运维值班电话； b)检查电话是否通畅。	是□ 否□ 不适用□	
1.5.	是否对信息系统相关的各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理；每季度至少进行一次维护管理。	a)访谈系统运维负责人，询问是否有专门的部门或人员对各种设备、线路进行定期维护，由何部门/何人负责，维护周期多长； b)检查设备、线路维护记录，确定配套设施、软硬件维护是否至少每季度进行一次。	是□ 否□ 不适用□	
1.6.	是否对终端计算机、工作站、便携机、系统和网络等设备的操作和使用进行规范化管理，按操作规程实现关键设备（包括备份和冗余设备）的启动/停止、加电/断电等操作。	a)检查设备安全管理制度中是否有对终端计算机、便携机和网络设备等使用方式、操作原则、注意事项等方面的规定； b)检查是否有关键设备的操作规程。	是□ 否□ 不适用□	
1.7.	信息处理设备是否经过审批才能带离机房或办公地点。	检查设备安全管理制度中是否有信息处理设备必须经过审批才能带离机房或办公地点的要求。	是□ 否□ 不适用□	

表 D.2　运维管理审计底稿（续）

序号	审计项	审计程序	审计结论	备注
1.8.	是否制定操作手册。操作手册的内容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。	检查操作手册，是否针对各个操作环节制定了操作规程。	是□ 否□ 不适用□	
1.9.	注册邮箱账号是否经过审批。	检查一年内全部注册邮箱账号的审批情况。	是□ 否□ 不适用□	
1.10.	是否按照技术规范对客户的主要开户资料进行电子化，并妥善保存在信息系统中。是否按照技术规范在 18 个月内对新增账户实施开户资料电子化，存量的正常交易类账户应在 36 个月内完成开户资料电子化。	a)访谈运维管理人员，了解客户主要开户资料电子化情况； b)抽查客户资料是否完成电子化。	是□ 否□ 不适用□	
1.11.	是否妥善保存客户交易终端信息和开户资料电子化信息，保存期限不得少于 20 年。	访谈运维管理人员，了解客户交易终端信息和开户资料电子化信息的保存期限是否不少于 20 年。	是□ 否□ 不适用□	
1.12.	是否妥善保存交易时段客户交易区的监控录像资料，保存期限不得少于 6 个月。	抽查近 6 个月内的交易区监控录像是否可用。	是□ 否□ 不适用□	
1.13.	是否采取可靠的措施，采集、记录、存储、报送与客户身份识别有关的信息，不得以任何理由拒绝承担相应职责。公司及其工作人员应当对客户交易终端信息予以保密，不得泄露。	a)检查应用系统设计和验收文档，查看是否采取可靠措施，采集、记录、存储、报送与客户身份识别有关的信息； b)检查经营机构承诺保密的相关材料，是否明确说明对客户交易终端信息予以保密的内容； c)检查经营机构工作人员签署的保密协议，是否明确要求工作人员对客户交易终端信息予以保密、不得泄露。	是□ 否□ 不适用□	
1.14.	是否严格限制对客户交易终端信息的人工操作权限，明确查询权限和操作流程，建立日志文档并指定专人妥善保管。禁止任何人对客户交易终端信息进行隐匿、伪造、篡改或毁损。	a)检查权限管理制度，是否严格限制对客户交易终端信息的人工操作权限； b)检查对客户交易终端信息的人工操作日志记录，是否不存在对客户交易终端信息进行隐匿、伪造、篡改或毁损的情况或记录。	是□ 否□ 不适用□	

表 D.2　运维管理审计底稿（续）

序号	审计项	审计程序	审计结论	备注
1.15.	发生影响采集、记录、存储、报送客户交易终端信息安全的重大事件时，是否及时向公司住所地和事件发生地证监局报告，不得隐瞒。	检查是否建立了信息安全事件报告制度和流程，查看是否明确规定，当发生影响采集、记录、存储、报送客户交易终端信息安全的重大事件时，应及时向公司住所地和事件发生地证监局报告，不得隐瞒。	是□ 否□ 不适用□	
1.16.	是否通过多种技术手段加强对投资者账户异动情况的监控，如委托的方式、品种、价格、数量异常等，并及时提醒客户，以保护客户资产安全。	a)查看账户异动监控软件相关文档，判断是否监控委托方式、品种、价格、数量异常等； b)检查账户异动监控软件监控日志和操作记录； c)抽查账户异动提醒记录，判断是否及时提醒客户。	是□ 否□ 不适用□	
2.	**应急演练**			
2.1.	是否定期进行消防设施的使用培训和演习。	a)检查“表 0.10-本年度应急演练情况-针对消防等开展的应急演练的次数（次）”，审阅机房管理制度，是否规定定期进行消防设施的使用培训和演习； b)检查消防设施的使用培训和演习记录，确定是否定期进行培训和演习。	是□ 否□ 不适用□	
3.	**产品采购**			
3.1.	是否采用经过国家密码管理部门批准使用或者准于销售的密码产品进行安全保护，不得采用国外引进或者擅自研制的密码产品；未经批准不得采用含有加密功能的进口信息技术产品。	a)查看“表 0.12-公司所有信息系统的密码设备数量统计”，访谈系统建设负责人，询问系统是否采用了密码产品，密码产品的采购和使用是否符合国家密码主管部门的要求； b)抽样检查密码产品的相关凭证，如销售许可等，查看是否使用了符合国家有关规定产品。	是□ 否□ 不适用□	
3.2.	是否指定或授权专门的部门负责产品的采购。	访谈系统建设负责人，询问是否有专门的部门负责产品的采购，由何部门负责。	是□ 否□ 不适用□	
3.3.	是否对产品进行选型测试，根据选型测试确定产品候选范围，并定期审核更新候选产品名单。	a)访谈系统建设负责人，询问采购产品前是否预先对产品进行选型测试确定产品的候选范围，是否有产品采购清单指导产品采购，是否定期审定和更新候选产品采购清单，审定周期多长； b)检查是否具有产品选型测试结果文档、候选产品采购清单及审定或更新的记录。	是□ 否□ 不适用□	

表 D.2　运维管理审计底稿（续）

序号	审计项	审计程序	审计结论	备注
4.	**自行软件开发**			
4.1.	自行软件开发是否提供软件设计文档和使用指南，并由专人保管。	检查是否具有软件使用指南或操作手册等。	是□ 否□ 不适用□	
4.2.	开发人员和测试人员是否分离，测试数据和测试结果受到控制。是否保证同一组件或子系统的开发人员和测试人员分离。	a)访谈系统建设负责人，询问是否要求开发人员不能做测试人员（即二者分离），自主开发软件是否在独立的模拟环境中完成编码和调试，如相对独立的网络区域； b)检查软件开发管理制度，查看文件是否明确软件设计、开发、测试、验收过程的控制方法和人员行为准则，是否明确哪些开发活动应经过授权、审批； c)检查网络拓扑图和实际开发环境，查看是否实际运行环境和开发环境有效隔离； d)检查同一组件或子系统的开发人员和测试人员是否人员分离； e)检查是否具有软件开发相关文档(源代码、测试数据、测试结果等）的使用控制记录。	是□ 否□ 不适用□	
4.3.	是否制定代码编写安全规范，要求开发人员参照规范编写代码。	a)访谈软件开发人员，询问其是否了解软件开发管理制度，是否了解代码编写安全规范，是否按照代码编写安全规范进行软件开发； b)检查代码编写安全规范，查看规范中是否明确代码编写规则，应抽样部分源代码，检查是否按照代码编写安全规范开发。	是□ 否□ 不适用□	
4.4.	是否对程序资源库的修改、更新、发布进行授权和批准。	检查对程序资源库的修改、更新、发布进行授权和审批的文档或记录，查看是否有批准人的签字	是□ 否□ 不适用□	
5.	**外包软件开发**			
5.1.	是否根据开发要求测试软件质量。	a)访谈系统建设负责人，询问软件交付前是否依据开发要求的技术指标对软件功能和性能等进行验收测试； b)检查软件测试文档。	是□ 否□ 不适用□	

表 D.2　运维管理审计底稿（续）

序号	审计项	审计程序	审计结论	备注
5.2.	是否确保提供软件设计的相关文档和使用指南。	检查是否具有软件开发的相关文档，如需求分析说明书、软件设计说明书等，是否具有软件操作手册或使用指南。	是□ 否□ 不适用□	
5.3.	是否在软件安装之前检测软件包中可能存在的恶意代码。	访谈系统建设负责人，询问软件安装之前是否检测软件中的恶意代码；	是□ 否□ 不适用□	
6.	**资产管理**			
6.1.	是否编制与信息系统相关的资产清单，包括资产责任部门、重要程度和所处位置等内容。	检查是否有资产清单，查看其内容是否覆盖资产责任部门、责任人、所处位置和重要程度等方面。	是□ 否□ 不适用□	
6.2.	是否根据资产重要程度分类标识管理资产，根据资产的价值选择相应的管理措施。	检查是否有资产安全管理方面的制度，查看是否明确了依据资产的重要程度对资产进行分类和标识管理的方法，是否说明了不同类别的资产采取的不同管理措施。	是□ 否□ 不适用□	
6.3.	是否对信息分类与标识方法作出规定，并对信息的使用、传输和存储等进行规范化管理。	检查是否有资产安全管理方面的制度，查看是否明确了信息分类标识的原则和方法，对信息的使用、传输和存储等进行规范化管理。	是□ 否□ 不适用□	
6.4.	检查信息系统设备清单，是否包括设备名称、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。	a)检查信息系统设备清单，是否包括设备名称、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； b)检查设备启用、转移、维修、报废等过程的维护记录。	是□ 否□ 不适用□	
6.5.	是否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。	a)检查资产管理制度中是否对设备和软件的使用年限作出规定； b)检查一年内的盘点记录、设备状态评估更新记录。	是□ 否□ 不适用□	
7.	**数据和介质管理**			
7.1.	是否确保介质存放在介质库或档案室等安全的环境中，并实行存储环境专人管理，实现对各类介质和备份数据的控制和保护。	a)访谈资产管理员，询问介质的存放环境是否采取保护措施防止介质被盗、被毁等； b)访谈资产管理员，询问是否将介质保管在一个特定环境里，有专人负责。	是□ 否□ 不适用□	

表 D.2　运维管理审计底稿（续）

序号	审计项	审计程序	审计结论	备注
7.2.	是否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。	a)访谈资产管理员，询问是否根据重要性对介质进行分类和标识； b)检查介质存储环境，查看是否对其进行了分类，并具有不同标识。	是□ 否□ 不适用□	
7.3.	是否对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，对介质归档和查询等进行登记记录，并根据存档介质的目录清单定期盘点。	a)访谈资产管理员，询问对介质的物理传输过程是否要求选择可靠传输人员、严格介质的打包、选择安全的物理传输途径、双方在场交付等环节的控制； b)检查介质使用管理记录，查看其是否记录介质归档和使用等情况； c)访谈资产管理员，询问是否根据介质的目录清单对介质的使用现状进行定期检查。	是□ 否□ 不适用□	
7.4.	是否对存储介质的使用过程、送出维修以及销毁等进行严格的管理，对带出工作环境的存储介质进行内容加密和监控管理，对送出维修或销毁的介质应首先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，是否按国家相关规定另行处理。	访谈资产管理员，询问对送出维修或销毁的介质在送出之前是否对介质内存储数据进行净化处理，对介质带出工作环境和重要介质中的数据和软件是否进行保密性处理；对保密性较高的介质销毁前是否有领导批准。	是□ 否□ 不适用□	
7.5.	是否对重要介质中的数据和软件采取加密存储，并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。	访谈资产管理员，询问是否定期对存储介质的完整性（数据是否损坏或丢失）和可用性(介质是否受到物理破坏)进行检查，是否对重要数据进行加密存储。	是□ 否□ 不适用□	
7.6.	是否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。	a)检查数据备份及验证策略，是否明确备份范围、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； b)检查数据备份及验证记录，确认按照数据备份及验证策略，对数据进行了备份和验证。	是□ 否□ 不适用□	

表 D.2　运维管理审计底稿（续）

序号	审计项	审计程序	审计结论	备注
7.7.	交易业务系统数据是否至少每交易日备份一次。	查看“表 0.4-客户信息及交易数据备份情况”、“表 0.5-转账日志备份情况”、“表 0.7 附表-该机房的网上信息系统数据备份情况”、“表 0.8-数据备份情况”，检查在线数据备份记录，确认交易业务系统数据至少每交易日备份一次。	是□ 否□ 不适用□	
7.8.	交易业务系统历史数据至少保留一年。	检查在线数据备份记录，确认交易业务系统历史数据至少保留一年。	是□ 否□ 不适用□	
7.9.	在线数据未经授权不得访问、复制。	检查在线数据访问、复制记录，查看是否有授权审批记录。	是□ 否□ 不适用□	
7.10.	对数据的修改是否通过审批，双岗操作并记录操作日志。	检查在线数据的修改记录，查看是否有授权审批记录、双岗操作记录。	是□ 否□ 不适用□	
7.11.	离线数据不得更改。	检查离线数据维护记录，查看是否有更改记录。	是□ 否□ 不适用□	
7.12.	是否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，如发现问题是否采取措施修复备份数据，并查明原因。	检查“表 0.4-客户信息及交易数据备份情况”、“表 0.5-转账日志备份情况”、“表 0.7 附表-该机房的网上信息系统数据备份情况”、“表 0.8-数据备份情况”，查看是否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，如发现问题是否采取措施修复备份数据，并查明原因。	是□ 否□ 不适用□	
7.13.	离线数据的调阅、复制、传输、查询，是否按照拟定的流程办理审批手续，并进行登记。	检查离线数据维护记录，查看对离线数据的调阅、复制、传输、查询的授权审批记录。	是□ 否□ 不适用□	
7.14.	备份数据带离存储环境时是否采取必要的安全措施。	a)访谈安全管理员，了解备份数据带离存储环境时，应采取哪些安全措施； b)检查离线数据维护记录，确认采取了必要的安全措施。	是□ 否□ 不适用□	
7.15.	在线数据和离线数据用于非生产环境时，是否进行脱敏处理；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。	访谈安全管理员，在线数据和离线数据用于非生产环境时，是否进行脱敏处理；用于模拟测试时如无法进行脱敏处理，测试环境的与生产环境安全措施是否相当。	是□ 否□ 不适用□	

表 D.2　运维管理审计底稿（续）

序号	审计项	审计程序	审计结论	备注
7.16.	离线备份介质是否在本地机房、同城、异地安全可靠存放。	检查“表 0.4-客户信息及交易数据备份情况”、“表 0.5-转账日志备份情况”、“表 0.7 附表-该机房的网上信息系统数据备份情况”、“表 0.8-数据备份情况”，确认对离线备份介质采取了本地机房、同城、异地安全可靠存放。	是□ 否□ 不适用□	
7.17.	涉及敏感信息的介质送修时是否由专人全程陪同，并保证修复过程可控。	访谈安全管理员，涉及敏感信息的介质送修时是否由专人全程陪同，并保证修复过程可控。	是□ 否□ 不适用□	
7.18.	在交易业务网使用的移动介质是否专网专用，不得接入可以访问互联网的主机。	访谈安全管理员，采取了何种措施，保证交易业务网使用的移动介质专网专用，不得接入可以访问互联网的主机。	是□ 否□ 不适用□	
7.19.	是否对外送设备的维修进行严格管理，防止数据泄露。	访谈安全管理员，了解采取了哪些措施，防止外送维修设备的数据泄露。	是□ 否□ 不适用□	
7.20.	是否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。设备和软件报废符合资产管理规定。	a)检查信息清除记录，是否按照规定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； b)检查系统下线记录，是否按照规定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。	是□ 否□ 不适用□	
8.	**配置管理**			
8.1.	是否制定配置管理流程，明确配置管理负责人。	访谈配置管理负责人，检查配置管理流程。	是□ 否□ 不适用□	
8.2.	是否建立配置库，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。	检查配置库文档，是否包括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、数据库等配置清单。	是□ 否□ 不适用□	
8.3.	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。	检查配置库文档，配置项属性是否至少包括编号、名称、描述、维护责任人、运行状态、关联关系等。	是□ 否□ 不适用□	
8.4.	配置项编号是否唯一。	检查配置库文档，配置项编号应唯一。	是□ 否□ 不适用□	

表 D.2　运维管理审计底稿（续）

序号	审计项	审计程序	审计结论	备注
8.5.	配置项的添加、修改、替换、删除是否有变更记录。	检查配置库维护记录，配置项的添加、修改、替换、删除是否有变更记录。	是□ 否□ 不适用□	
8.6.	是否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。	检查配置库文档，查看配置项历史记录，是否确保与事件管理、问题管理、变更管理等流程记录的关联性。	是□ 否□ 不适用□	
8.7.	是否定期对配置库进行备份。	检查配置库维护记录，判断是否定期对配置库进行备份。	是□ 否□ 不适用□	
8.8.	是否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。	检查配置库维护记录，判断是否定期审计数据库，对发现的不一致情况及时纠正。	是□ 否□ 不适用□	
9.	**安全管理**			
9.1.	是否建立安全管理中心，对设备状态、恶意代码、补丁升级、安全审计等安全相关事项进行集中管理。	访谈系统运维负责人，询问是否对通信线路、主机、网络设备和应用软件的运行状况，对设备状态、恶意代码、网络流量、补丁升级、安全审计等安全相关事项进行集中管理，是否形成监测记录文档，是否组织人员对监测记录进行整理并保管。	是□ 否□ 不适用□	
9.2.	是否对防恶意代码软件的授权使用、恶意代码库升级、定期汇报等作出明确规定。	检查是否有恶意代码防范方面的管理制度，查看其内容是否覆盖防恶意代码软件的授权使用、恶意代码库升级、定期汇报等方面。	是□ 否□ 不适用□	
10.	**事件与问题管理**			
10.1.	是否对安全检查情况进行评估，形成评估报告。	审阅评估报告，检查是否对安全检查情况进行评估。	是□ 否□ 不适用□	
10.2.	是否建立事件管理流程，对信息系统运维事件的处理进行规范。	检查事件管理流程，是否对信息系统运维事件的处理进行规范。	是□ 否□ 不适用□	
10.3.	是否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。	是否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。	是□ 否□ 不适用□	
10.4.	是否对所有事件响应、处理、结束等过程进行跟踪、督促及检查。	查看运维事件处理记录，是否对所有事件响应、处理、结束等过程进行跟踪、督促及检查。	是□ 否□ 不适用□	

表 D.2　运维管理审计底稿（续）

序号	审计项	审计程序	审计结论	备注
10.5.	是否每月回顾、分析事件处理记录，完成事件分析报告。	查看月度事件分析报告，判断是否每月回顾、分析事件处理记录，完成事件分析报告。	是□ 否□ 不适用□	
10.6.	是否将运维过程中重复发生的事件、重大事件纳入问题管理。	查看问题库，是否将运维过程中重复发生的事件、重大事件纳入问题管理。	是□ 否□ 不适用□	
10.7.	是否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。	查看问题处理记录，是否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。	是□ 否□ 不适用□	
10.8.	是否将监控、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。	查看问题库，是否将监控、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。	是□ 否□ 不适用□	
10.9.	是否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。	查看问题库，是否对问题进行分析、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。	是□ 否□ 不适用□	
11.	**应急准备**			
11.1.	是否在统一的应急预案框架下制定不同事件的应急预案，应急预案框架应包括启动应急预案的条件、应急处理流程、系统恢复流程、事后教育和培训等内容。	a)检查应急预案框架，查看其内容是否覆盖启动应急预案的条件、应急处理流程、系统恢复流程、事后教育和培训等方面； b)检查是否具有根据应急预案框架制定的不同事件的应急预案。	是□ 否□ 不适用□	
11.2.	是否对系统相关的人员进行应急预案培训，应急预案的培训是否至少每年举办一次。	a)访谈系统运维负责人，询问是否对系统相关人员进行应急预案培训，多长时间举办一次； b)检查应急培训记录，判断系统相关人员是否参加、是否每年至少一次。	是□ 否□ 不适用□	
11.3.	是否从人力、设备、技术和财务等方面确保应急预案的执行有足够的资源保障。	访谈系统运维负责人，询问应急预案执行所需人力、设备、技术和财务等方面是否有足够的资源。	是□ 否□ 不适用□	
11.4.	是否至少每年对电力故障、消防、空调故障等应急预案进行演练。	检查“表 0.10-本年度应急演练情况”和演练记录，查看是否至少每年对应急预案进行演练。	是□ 否□ 不适用□	

表 D.2　运维管理审计底稿（续）

序号	审计项	审计程序	审计结论	备注
11.5.	是否规定每年审查应急预案，根据实际情况更新应急预案的内容，并按照执行。	检查应急预案审查记录，是否每年审查应急预案，并根据实际情况更新应急预案的内容。	是□ 否□ 不适用□	
11.6.	是否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。	检查应急预案，是否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。	是□ 否□ 不适用□	
11.7.	网络与信息安全事件应急处置指挥决策机构是否由主要领导负责，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。	检查应急预案应急指挥决策机构设置情况及人员名单，是否明确了应急处置指挥决策机构由主要领导负责，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。	是□ 否□ 不适用□	
11.8.	是否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。	检查“表 0.9-公司信息安全应急联络人”和应急预案， 是否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。	是□ 否□ 不适用□	
11.9.	网络与信息安全事件应急预案内容是否包括应急预案编制的目的和依据。	检查应急预案，判断是否包括应急预案编制目的和依据。	是□ 否□ 不适用□	
11.10.	网络与信息安全事件应急预案内容是否包括应急预案的适用范围。	检查应急预案，判断是否包括应急预案的适用范围。	是□ 否□ 不适用□	
11.11.	网络与信息安全事件应急预案内容是否包括应急处置的组织体系及职责。	检查应急预案，判断是否包括应急处置的组织体系及职责。	是□ 否□ 不适用□	
11.12.	网络与信息安全事件应急预案内容是否包括预防措施、保障措施与应急准备。	检查应急预案，判断是否包括预防措施、保障措施与应急准备。	是□ 否□ 不适用□	
11.13.	网络与信息安全事件应急预案内容是否包括预警监测、处置和信息报送。	检查应急预案，判断是否包括预警监测、处置和信息报送。	是□ 否□ 不适用□	
11.14.	网络与信息安全事件应急预案内容是否包括网络与信息安全事件的分级分类。	检查应急预案，判断是否包括网络与信息安全事件的分级分类。	是□ 否□ 不适用□	

表 D.2　运维管理审计底稿（续）

序号	审计项	审计程序	审计结论	备注
11.15.	网络与信息安全事件应急预案内容是否包括网络与信息安全事件的报告流程。	检查应急预案，判断是否包括网络与信息安全事件的报告流程。	是□ 否□ 不适用□	
11.16.	网络与信息安全事件应急预案内容是否包括网络与信息安全事件处置的一般原则。	检查应急预案，判断是否包括网络与信息安全事件处置的一般原则。	是□ 否□ 不适用□	
11.17.	网络与信息安全事件应急预案内容是否包括网络与信息安全事件处置的具体方案。	检查应急预案，判断是否包括网络与信息安全事件处置的具体方案。	是□ 否□ 不适用□	
11.18.	网络与信息安全事件应急预案内容是否包括网络与信息安全事件内部调查处理以及分析总结的要求。	检查应急预案，判断是否包括网络与信息安全事件内部调查处理以及分析总结的要求。	是□ 否□ 不适用□	
11.19.	网络与信息安全事件处置的具体方案是否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。	检查应急预案，判断网络与信息安全事件处置的具体方案是否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。	是□ 否□ 不适用□	
11.20.	应急预案内容是否针对各种技术故障拟定统一的解释口径和通知公告模板。	检查应急预案，判断是否针对各种技术故障拟定统一的解释口径和通知公告模板。	是□ 否□ 不适用□	
11.21.	应急预案是否每年至少进行一次评估，并及时修订	检查应急预案评估报告，判断是否每年至少进行一次评估。	是□ 否□ 不适用□	
11.22.	应急预案内容是否根据应急演练的情况进行评估和更新。	检查应急预案评估报告，判断是否根据应急演练的情况进行评估和更新。	是□ 否□ 不适用□	
11.23.	应急预案是否向住所地证监局报备。	检查应急预案报备记录，判断经营机构是否向住所地证监局报备。	是□ 否□ 不适用□	
11.24.	在应急预案发生重大变化时，应急预案是否及时重新报备。	检查应急预案报备记录，判断是否在应急预案发生重大变化时，及时重新报备。	是□ 否□ 不适用□	
11.25.	值班负责人和信息技术负责人是否负责信息安全应急值守。	检查值班管理制度，是否明确值班负责人和信息技术负责人负责信息安全应急值守。	是□ 否□ 不适用□	

表 D.2　运维管理审计底稿（续）

序号	审计项	审计程序	审计结论	备注
11.26.	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是否熟练掌握应急预案，能有效处置网络与信息安全事件。	查看应急预案，访谈相关系统管理员、网络管理员、数据库管理员、安全管理员等关键岗位，询问是否知悉其应急处置职责范围。	是□ 否□ 不适用□	
11.27.	在自身力量不足以满足应急要求的情况下，是否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。是否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。	a)检查应急响应服务协议是否包括通信、消防、电力设备、空调设备、软硬件产品、安全服务等相关单位； b)检查应急响应及服务保障协议内容是否包括双方联系人、联系方式、服务内容及范围、应急处理方式等； c)检查应急响应服务协议评估报告，判断是否定期检查和评估协议。	是□ 否□ 不适用□	
11.28.	是否建立有效的应急通讯联络系统，确保信息畅通。	a)查看应急预案中是否要求建立应急通讯联络系统； b)抽查应急通讯联络系统中的相关信息是否真实、有效、可用。	是□ 否□ 不适用□	
11.29.	是否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。应急处置联络手册是否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。	a)审阅应急处置联络手册，是否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，且联络方式必须明确详细； b)抽查应急处置联络手册中的相关信息是否真实、有效、可用。	是□ 否□ 不适用□	
11.30.	是否实行 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。	a)查看应急预案，是否明确要求 7×24 小时联络制度； b)检查通报联络人应急值守电话是否能够及时接通。	是□ 否□ 不适用□	
11.31.	是否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。	检查抽查领导和员工的应急工作卡片，是否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。	是□ 否□ 不适用□	

表 D.2　运维管理审计底稿（续）

序号	审计项	审计程序	审计结论	备注
11.32.	是否准备了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。	检查信息系统技术资料和软件备份，是否包括网络拓扑图、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。	是□ 否□ 不适用□	
11.33.	是否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。	a)访谈运维管理负责人，询问是否准备充足的重要设备备品配件，哪些设备有备品配件； b)检查重要设备备品配件的维护记录，判断是否期评估、检测和维护。	是□ 否□ 不适用□	
11.34.	是否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。	检查通讯、消防、应急照明等应急设备或物资的盘点记录，判断对于有时效性的应急物资是否做到及时更新。	是□ 否□ 不适用□	
11.35.	是否准备应急保障资金，确保应急处置中能及时采购应急设备或物资。	检查应急保障资金的预算记录、使用流程。	是□ 否□ 不适用□	
11.36.	是否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。	检查应急演练计划，是否至少包括目的、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。	是□ 否□ 不适用□	
11.37.	是否每半年至少组织一次网络与信息安全应急演练。	a)查看“表 0.10 度应急演练情况”和应急演练计划，是否每半年至少组织一次网络与信息安全应急演练； b)检查应急演练记录。	是□ 否□ 不适用□	
11.38.	是否记录演练情况，演练记录至少保存两年。	检查两年内的演练记录。	是□ 否□ 不适用□	
11.39.	是否对演练中发现的问题进行改进。	检查演练整改报告，是否对演练中发现的问题进行改进。	是□ 否□ 不适用□	
11.40.	是否每年向住所地证监局报告年度应急演练情况。	检查应急演练情况报告记录，核心机构是否每年向中国证监会报告年度应急演练情况；经营机构是否每年向住所地证监局报告年度应急演练情况。	是□ 否□ 不适用□	

表 D.2　运维管理审计底稿（续）

序号	审计项	审计程序	审计结论	备注
11.42.	是否定期组织灾难备份应急预案和应急计划的演练，至少每年二次，并根据演练的结果和发现的问题进行总结，对系统和应急方案进行优化及完善。	检查“表 0.10-本年度应急演练情况-对灾备系统切换进行应急演练的次数（次）”，检查集中交易系统应急演练记录，是否每年至少进行二次演练，是否根据演练的结果和发现的问题进行总结，对系统和应急方案进行优化及完善。	是□ 否□ 不适用□	
11.43.	是否对集中交易系统实行年度例行安全评估，并将评估结果报备相关交易所。	检查集中交易系统评估报告和报备记录，确认进行了年度例行安全评估，并将评估报告报备相关交易所。	是□ 否□ 不适用□	
11.44.	是否制定了针对第三方存管系统完整的应急预案及应急协调预案，并定期组织演练及联合演练。	检查“表 0.10-本年度应急演练情况-针对第三方存管系统与银行开展联合演练的次数（次）”，查看第三方存管系统的应急预案和应急演练记录，确认定期进行演练及联合演练。	是□ 否□ 不适用□	
11.45.	网上信息系统应急预案是否针对电力、通信等基础设施故障、计算机硬件或网络设备故障、操作系统或应用系统故障、操作系统或应用系统漏洞、病毒入侵、恶意攻击、误操作、不可抗力等可能的故障原因制定对应的应急恢复操作流程或步骤。	审阅网上信息系统应急预案，确认针对电力、通信等基础设施故障、计算机硬件或网络设备故障、操作系统或应用系统故障、操作系统或应用系统漏洞、病毒入侵、恶意攻击、误操作、不可抗力等可能的故障原因制定对应的应急恢复操作流程或步骤。	是□ 否□ 不适用□	
12.	**应急处置**			
12.1.	是否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。	访谈系统运维负责人，询问是否告知用户在发现安全弱点和可疑事件时应及时报告。	是□ 否□ 不适用□	
12.2.	是否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。	a)审阅应急预案，是否规定在网络与信息安全事件发生后，报告要素有哪些，如何报告事件情况，并保持持续报告，直至系统恢复正常运行； b)检查事件报告记录，判断要素是否完备、及时、准确，没有迟报、漏报、谎报或瞒报。	是□ 否□ 不适用□	

表 D.2　运维管理审计底稿（续）

序号	审计项	审计程序	审计结论	备注
12.3.	是否根据国家相关管理部门对计算机安全事件等级划分方法和安全事件对本系统产生的影响，对本系统计算机安全事件进行等级划分。	检查是否有安全事件报告和处置管理制度，查看其是否明确安全事件的级别，明确不同级别安全事件的报告和处置方式等内容。	是□ 否□ 不适用□	
12.4.	是否制定安全事件报告和响应处理程序，确定事件的报告流程，响应和处置的范围、程度，以及处理方法等。	检查是否有安全事件报告和处置管理制度，查看其是否细化了不同安全事件的处理和报告程序，是否明确具体报告方式、报告内容、报告人等方面内容，造成系统中断和造成信息泄密的重大安全事件是否采用了不同于其他的处理程序和报告程序。	是□ 否□ 不适用□	
12.5.	是否在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训，制定防止再次发生的补救措施。	检查安全事件处理记录，查看其是否记录引发安全事件的原因，是否记录事件处理过程，是否与管理规定的处理要求一致等。	是□ 否□ 不适用□	
12.6.	是否做好应急处置的相关记录，保留有关证据。	检查安全事件处理记录，是否保留有关证据。	是□ 否□ 不适用□	
12.7.	是否对造成系统中断和造成信息泄密的安全事件采用不同的处理程序和报告程序。	检查是否有安全事件报告和处置管理制度，查看其是否细化了不同安全事件的处理和报告程序，是否明确具体报告方式、报告内容、报告人等方面内容，造成系统中断和造成信息泄密的重大安全事件是否采用了不同于其他的处理程序和报告程序。	是□ 否□ 不适用□	
12.8.	是否对证券期货行业内通报的重大安全隐患立即进行专项安全检查。	检查行业通报和行业通报专项检查记录，对证券期货行业内通报的重大安全隐患，是否立即进行专项安全检查。	是□ 否□ 不适用□	
12.9.	是否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。	检查事件处置报告，判断发生网络与信息安全事件后，是否立即启动应急预案，迅速采取应急措施，尽快恢复信息系统正常运行。	是□ 否□ 不适用□	
12.10.	是否在应急处置中注意保证工作人员的人身安全。	检查应急预案，是否有保证工作人员的人身安全的措施。	是□ 否□ 不适用□	

表 D.2　运维管理审计底稿（续）

序号	审计项	审计程序	审计结论	备注
12.11.	是否在应急处置结束前，保证专人 24 小时值班。	检查应急预案，是否规定在应急处置结束前，保证专人 24 小时值班。	是□ 否□ 不适用□	
12.12.	应急处置人员是否保持联系方式畅通，及时向有关方面通报事件处置进展情况。	检查应急预案，是否规定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。	是□ 否□ 不适用□	
12.13.	是否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。	检查应急预案，是否规定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。	是□ 否□ 不适用□	
12.14.	是否针对集中交易制定规范化的故障处理流程，建立详细的故障日志（包括故障发生的时间、范围、现象、处理结果和处理人员等内容）。	a)访谈运维管理负责人，询问是否有集中交易系统故障处理，并检查该流程； b)检查集中交易系统故障日志，是否包括故障发生的时间、范围、现象、处理结果和处理人员等内容。	是□ 否□ 不适用□	
13.	**调查处理**			
13.1.	是否在信息安全事件应急处置结束、系统恢复正常运行后 5 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。	检查事件总结报告，判断是否在信息安全事件应急处置结束、系统恢复正常运行后 5 个工作日内，组织了内部调查，查明了事件性质，认定了事件责任，提出了整改措施。	是□ 否□ 不适用□	
13.2.	事件总结报告中事件基本情况，是否包括事件发生时间、地点、经过、影响范围、影响程度、损失情况等。	检查事件总结报告，事件基本情况是否包括事件发生时间、地点、经过、影响范围、影响程度、损失情况等。	是□ 否□ 不适用□	
13.3.	事件总结报告是否说明应急处置情况，包括事件报告的情况、采取的措施及效果。	检查事件总结报告，应急处置情况是否包括事件报告的情况、采取的措施及效果。	是□ 否□ 不适用□	
13.4.	事件总结报告中事件调查情况，是否包括事件原因、事件级别、责任认定和结论。	检查事件总结报告，事件调查情况是否包括事件原因、事件级别、责任认定和结论。	是□ 否□ 不适用□	
13.5.	事件总结报告中事件处理情况，是否包括事件暴露出的问题及采取的整改措施，责任追究情况。	检查事件总结报告，事件处理情况是否包括事件暴露出的问题及采取的整改措施，责任追究情况。	是□ 否□ 不适用□	

表 D.2　运维管理审计底稿（续）

序号	审计项	审计程序	审计结论	备注
13.6.	是否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。	查看事故调查处理办法，是否明确要求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。	是□ 否□ 不适用□	
13.7.	对于暂时无法确定事件原因、责任和结论的，是否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。	检查事件总结报告，对于暂时无法确定事件原因、责任和结论的事件，是否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。	是□ 否□ 不适用□	
13.8.	接到中国证监会及其派出机构关于系统漏洞、安全隐患、产品缺陷的信息安全通报书后，是否立即核实情况，采取必要的处置措施，并根据要求进行事件总结报告。事件总结报告内容应当包括：事件基本情况，可能或者已经造成的影响范围和后果，已采取的防范措施及相关建议。	a)检查监管部门信息安全通报记录，对系统漏洞、安全隐患、产品缺陷等，是否立即核实情况，采取必要的处置措施； b)检查信息安全通报事件总结报告，内容是否包括：事件基本情况，可能或者已经造成的影响范围和后果，已采取的防范措施及相关建议。	是□ 否□ 不适用□	
13.9.	是否向住所地中国证监会派出机构进行预警报告、应急报告和事件总结报告，分支机构应当向所在地中国证监会派出机构进行预警报告、应急报告和事件总结报告。事件总结报告同时抄送中国证券业协会。	检查应急报告记录，总部是否向住所地中国证监会派出机构进行应急报告，分支机构是否向所在地中国证监会派出机构进行应急报告。事件总结报告同时抄送中国证券业协会。	是□ 否□ 不适用□	

表 D.2　运维管理审计底稿（续）

序号	审计项	审计程序	审计结论	备注
13.10.	发生信息安全事件影响到证券期货交易业务时，是否同时向相关证券期货交易所进行应急报告和事件总结报告；影响到证券登记结算业务时，是否同时向中国证券登记结算公司进行应急报告和事件总结报告；影响到转融通业务时，是否同时向中国证券金融公司进行应急报告和事件总结报告；影响到其他机构的，是否及时向有关机构进行应急通报。	a)审阅应急管理制度，是否要求发生信息安全事件影响到证券期货交易业务时，向相关证券期货交易所提交应急报告和事件总结报告；发生信息安全事件影响到证券登记结算业务时，向中国证券登记结算公司提交应急报告和事件总结报告；发生信息安全事件影响到转融通业务时，向中国证券金融公司提交应急报告和事件总结报告；发生信息安全事件影响到其他机构的，向有关机构提交应急通报； b)检查应急报告记录，是否遵循以上流程。	是□ 否□ 不适用□	
13.11.	发生涉及计算机犯罪的事件，是否向公安机关进行应急报告。	a)审阅应急管理制度，是否要求发生涉及计算机犯罪的事件时，向公安机关进行应急报告； b)检查应急报告记录，是否遵循以上流程。	是□ 否□ 不适用□	

附 录 E
（规范性附录）
信息系统安全等级保护相关工作审计底稿

表E.1至表E.2给出了信息系统安全等级保护相关工作审计的程序、内容及相关记录要求。

表E.1 信息系统安全等级保护相关工作审计底稿

被审计部门：	索引号：DJBH
审计主题：信息系统安全等级保护相关工作	审计年度：
审计结论、意见及建议： 编制人： 年 月 日 （部门盖章）	
复核意见： 复核人： 年 月 日 （部门盖章）	
被审计部门意见： 年 月 日 （部门盖章）	

表 E.1　信息系统安全等级保护相关工作审计底稿（续）

审计证据列表：

表E.2　信息系统安全等级保护相关工作审计底稿

序号	审计项	审计程序	审计结论	备注
1.	**等级测评**			
1.1.	三级系统是否至少每年对系统进行一次等级测评，发现不符合相应等级保护标准要求的及时整改。	a)检查等级测评报告，检查是否每年对三级系统进行测评； b)检查测评报告是否覆盖所有三级系统； c)检查整改报告，对发现的问题是否及时整改。	是□ 否□ 不适用□	
1.2.	是否在系统发生变更时及时对系统进行等级测评，发现级别发生变化的及时调整级别并进行安全改造，发现不符合相应等级保护标准要求的及时整改。	a)检查系统变更记录，了解系统是否发生重大变更； b)检查系统评测记录，如果系统发生重大变更是否及时对系统进行登记测评； c)检查安全整改报告，发现级别发生变化的，是否及时调整级别并进行安全改造，发现不符合相应等级保护标准要求的，是否及时整改。	是□ 否□ 不适用□	
1.3.	三级信息系统是否选择了由省级（含）以上信息安全等级保护工作协调小组办公室（不限本省市）推荐的技术实力强、测评工作规范、熟悉行业信息系统的测评机构进行等级测评。	查看“表0.9-本年度开展安全建设整改的信息系统情况-信息安全等级保护等级测评机构名称（全称）”，对照省级（含）以上信息安全等级保护工作协调小组办公室（不限本省市）推荐评测机构清单，检查三级信息系统测评机构是否由省级（含）以上信息安全等级保护工作协调小组办公室（不限本省市）推荐。	是□ 否□ 不适用□	
1.4.	第二级信息系统是否每年开展一次自查，对于不符合证券期货业信息安全等级保护基本要求（试行）的内容，是否及时整改。	a)查看“表0.9-本年度开展安全建设整改的信息系统情况-是否组织开展信息系统安全自查工作”，二级信息系统本年度是否开展自查工作； b)检查二级信息系统的自查报告，是否每年开展一次自查； c)检查二级信息系统的整改报告，对于不符合证券期货业信息安全等级保护基本要求（试行）的内容，是否及时整改。	是□ 否□ 不适用□	
2.	**方案设计**			
2.1.	是否根据系统的安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施。	a)访谈信息技术负责人，询问是否根据系统的安全保护等级选择基本安全措施，并依据风险分析的结果补充和调整安全措施； b)检查基本安全措施相关文档和修订、完善安全策略的记录。	是□ 否□ 不适用□	

表 E.2　信息系统安全等级保护相关工作审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.2.	是否根据等级划分情况，统一规划总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等配套文件。	a)访谈信息技术负责人，是否根据当前等级划分情况，统一规划总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等配套文件； b)检查是否具有总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件。	是□ 否□ 不适用□	
2.3.	是否组织相关部门和有关安全技术专家对总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件的合理性和正确性进行论证和审定，并且经过批准后，才能正式实施。	a)访谈信息技术负责人，询问总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件的论证、审定及审批的机制； b)检查相关论证审定报告及记录； c)检查相关审批实施流程记录。	是□ 否□ 不适用□	
2.4.	是否根据等级测评、安全评估的结果定期调整和修订总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件。	a)访谈信息技术负责人，询问是否根据等级测评、安全评估的结果定期调整和修订总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件； b)检查相关配套文档； c)检查调整修改记录及审批实施记录。	是□ 否□ 不适用□	
3.	**系统备案**			
3.1.	各信息系统备案单位在取得公安机关颁发的备案证明后，是否将备案证明复印件报送住所地证监局。	a)检查备案证明发文记录； b)检查在取得公安机关颁发的备案证明后是否将等级保护备案证明等相关材料报送至住所地证监局。	是□ 否□ 不适用□	
3.2.	是否将系统等级及其他要求的备案材料报相应公安机关备案。	a)查看“表0.9-信息系统备案情况-信息系统备案情况-备案受理公安机关”，信息系统是否在公安机关备案； b)检查发文记录，是否将系统等级及其他要求的备案材料报相应公安机关备案。	是□ 否□ 不适用□	

表 E.2　信息系统安全等级保护相关工作审计底稿（续）

序号	审计项	审计程序	审计结论	备注
4.	**系统定级**			
4.1.	是否明确信息系统的边界和安全保护等级。	a)查看“表0.9-信息系统备案情况-信息系统备案情况-定级级别”，信息系统是否评定了安全保护等级； b)访谈信息技术负责人，询问是否明确信息系统的边界和安全保护等级； c)审阅信息系统安全等级评定资料，确定是否明确了信息系统边界和对应的安全等级划分。	是□ 否□ 不适用□	
4.2.	是否以书面的形式说明信息系统确定为某个安全保护等级的方法和理由。	检查系统定级文档，查看文档是否说明定级的方法和理由，是否有相关部门或主管领导的盖章或签名。	是□ 否□ 不适用□	
4.3.	是否组织相关部门和有关安全技术专家对信息系统定级结果的合理性和正确性进行论证和审定。	检查会议纪要或者论证报告等文档，是否组织有关部门及技术专家对信息系统定级结果的合理性和正确性进行论证和审定。	是□ 否□ 不适用□	
4.4.	定级结果是否经过相关部门批准，由住所地证监局出具定级审核意见。	检查是否将定级结果向相关部门报批，并由住所地证监局出具了定级审核意见书。	是□ 否□ 不适用□	

附 录 F
（规范性附录）
软件正版化审计底稿

表F.1至表F.2给出了软件正版化审计的程序、内容及相关记录要求。

表F.1 软件正版化审计底稿

被审计部门：	索引号：RJZBH
审计主题：软件正版化	审计年度：
审计结论、意见及建议： 编制人： 年 月 日 （部门盖章）	
复核意见： 复核人： 年 月 日 （部门盖章）	
被审计部门意见： 年 月 日 （部门盖章）	

表 F.1　软件正版化审计底稿（续）

审计证据列表：

表F.2　软件正版化审计底稿

序号	审计项	审计程序	审计结论	备注
1.	是否使用正版软件并保存软件授权证书和许可协议，是否编制软件清单，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。	a)检查软件授权证书和许可协议； b)检查软件清单，是否包括软件名称、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。	是□ 否□ 不适用□	
2.	是否对达到固定资产价值和使用年限的软件进行登记入库、建账管理、定期盘点。	a)访谈固定资产管理人员，是否对采购软件进行登记入库，并纳入管理； b)检查固定资产盘点表，是否包含软件。	是□ 否□ 不适用□	
3.	是否妥善保存购置合同、软件授权证书或许可协议等核心资料。	a)访谈文档管理员，是否对软件采购合同、授权书等资料进行管理； b)检查文档清单，是否包含软件购置合同及授权许可。	是□ 否□ 不适用□	
4.	是否每年对软件正版化情况开展自查。	a)访谈软件正版化人员，是否对公司使用的软件正版化情况每年进行自查，并出具自查报告； b)检查软件正版化自查报告。	是□ 否□ 不适用□	
5.	操作系统软件是否有授权（服务器）。	检查“表0.11-软件正版化情况-操作系统”，查看服务器使用的各操作系统版本，并检查使用的操作系统是否有授权文件。	是□ 否□ 不适用□	
6.	操作系统是否有授权（办公计算机）。	检查“表0.11-软件正版化情况-操作系统”，查看办公计算机使用的各操作系统版本，并检查在使用的操作系统是否有授权文件。	是□ 否□ 不适用□	
7.	数据库软件是否有授权。	检查“表0.11-软件正版化情况-数据库软件”，查看系统使用的数据库版本，并检查在使用的数据库系统是否有授权文件。	是□ 否□ 不适用□	
8.	杀毒软件是否有授权。	检查“表0.11-软件正版化情况-杀毒软件”，查看使用的杀毒软件版本，并检查在使用杀毒软件是否有授权文件。	是□ 否□ 不适用□	
9.	办公文字处理软件是否有授权。	检查“表0.11-软件正版化情况-办公文字处理软件”，查看使用的办公文字处理软件版本，并检查在使用办公文字处理软件是否有授权文件。	是□ 否□ 不适用□	

表 F.2　软件正版化审计底稿（续）

序号	审计项	审计程序	审计结论	备注
10.	办公专业处理软件是否有授权。	检查“表0.11-软件正版化情况-办公专业处理软件”，查看使用的办公专业处理软件版本，并检查在使用办公专业处理软件是否有授权文件。	是□ 否□ 不适用□	
11.	应用服务器软件是否有授权。	检查“表0.11-软件正版化情况-应用服务器软件”，查看使用的应用服务器软件版本，并检查在使用应用服务器软件是否有授权文件。	是□ 否□ 不适用□	
12.	专用业务软件是否有授权。	检查“表0.11-软件正版化情况-专用业务软件”，查看使用的专用业务软件版本，并检查在使用专用业务软件是否有授权文件。	是□ 否□ 不适用□	
13.	是否制定了软件正版化计划。	a)访谈软件正版化人员，是否制定了软件正版化计划； b)检查软件正版化计划，是否对通用软件和专业软件制定正版化计划。	是□ 否□ 不适用□	

附 录 G
（规范性附录）
集中交易系统审计底稿

表G.1至表G.2给出了集中交易系统审计的程序、内容及相关记录要求。

表G.1 集中交易系统审计底稿

被审计部门：	索引号：JZJYXT
审计主题：集中交易系统	审计年度：
审计结论、意见及建议： 编制人： 年 月 日 （部门盖章）	
复核意见： 复核人： 年 月 日 （部门盖章）	
被审计部门意见： 年 月 日 （部门盖章）	

表 G.1　集中交易系统审计底稿（续）

审计证据列表：

表G.2　集中交易系统审计底稿

序号	审计项	审计程序	审计结论	备注
1	主机管理			
1.1.	身份鉴别			
1.1.1.	操作系统管理员口令是否符合以下条件：数字、字母、符号混排，无规律的方式。	检查口令管理制度，是否规定口令符合以下条件：数字、字母、符号混排，无规律的方式。	是□ 否□ 不适用□	
1.1.2.	操作系统管理员口令的长度是否为12位。	检查口令管理制度，是否规定管理员用户口令的长度至少为12位。	是□ 否□ 不适用□	
1.1.3.	操作系统管理员口令是否每季度更换1次，更新的口令至少5次内不能重复。	检查口令管理制度，是否规定管理员用户口令至少每季度更换1次，更新的口令至少5次内不能重复。	是□ 否□ 不适用□	
1.1.4.	如果受限于操作系统，使得管理员口令长度不支持12位或其他复杂度要求，口令是否使用所支持的最长长度并适当缩小更换周期；也可以使用动态密码卡等一次性口令认证方式。	检查口令管理制度，是否规定如果设备口令长度不支持12位或其他复杂度要求，口令应使用所支持的最长长度并适当缩小更换周期，也可以使用动态密码卡等一次性口令认证方式。	是□ 否□ 不适用□	
1.1.5.	是否启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施。	a)检查重要服务器操作系统的身份鉴别策略，查看是否配置了登录失败处理功能、设置了非法登录次数的限制值； b)查看是否设置网络登录连接超时，并自动退出。	是□ 否□ 不适用□	
1.1.6.	当对服务器进行远程管理时，是否采取必要措施，防止鉴别信息在网络传输过程中被窃听。	查看“表0.13附表一-信息系统名称”、“表0.13附表一-本系统中密码机使用情况”，访谈系统管理员，询问是否对操作系统采用了远程管理方式，如果采用远程管理方式，查看是否具有防止鉴别信息在网络传输过程中被窃听的措施。	是□ 否□ 不适用□	
1.1.7.	是否为操作系统的不同用户分配不同的用户名，确保用户名具有唯一性。	检查操作系统的用户列表，标识是否唯一，或采取堡垒机等措施。	是□ 否□ 不适用□	
1.1.8.	通过本地控制台管理主机设备时，是否采用一种或一种以上身份鉴别技术。	查看安全策略文档，检查本地控制台管理主机设备是否采用一种或一种以上身份鉴别技术。	是□ 否□ 不适用□	
1.1.9.	以远程方式登录主机设备，是否采用两种或两种以上组合的鉴别技术进行身份鉴别。	查看安全策略文档，检查远程方式登录主机设备是否采用两种或两种以上组合的鉴别技术进行身份鉴别。	是□ 否□ 不适用□	

表 G.2　集中交易系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
1.2.	**访问控制**			
1.2.1.	是否启用访问控制功能，依据安全策略控制用户对资源的访问。	检查重要服务器操作系统的访问控制策略，查看是否对重要文件的访问权限进行了限制，对系统不需要的服务、共享路径等进行了禁用或删除。	是□ 否□ 不适用□	
1.2.2.	是否实现操作系统和数据库系统特权用户的权限分离；HP Tandem、IBM OS400系列、运行DB2数据库的IBM AIX等专用系统的特权用户除外。	如果系统支持操作系统和数据库系统特权用户的权限分离，应检查重要数据库管理系统的特权用户和重要操作系统的特权用户，查看不同管理员的系统账户权限是否不同，且不应由同一人担任。	是□ 否□ 不适用□	
1.2.3.	是否严格限制默认账户的访问权限，重命名系统默认账户，修改这些账户的默认口令。a)系统无法修改访问权限的特殊默认账户，可不修改访问权限；b)系统无法重命名的特殊默认账户，可不重命名。	检查重要服务器操作系统的访问控制策略，查看是否已禁用或者限制匿名/默认帐户的访问权限，是否重命名系统默认帐户、修改这些帐户的默认口令。	是□ 否□ 不适用□	
1.2.4.	是否及时删除多余的、过期的账户，避免共享账户的存在。	a)检查系统中的账号是否为用户工作必须的； b)检查是否及时删除了多余的、过期的账户	是□ 否□ 不适用□	
1.2.5.	是否根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限。	如果系统支持操作系统和数据库系统特权用户的权限分离，应检查主要服务器操作系统和主要数据库管理系统的访问控制策略，查看特权用户的权限是否进行分离，如可分为系统管理员、安全管理员、安全审计员等；查看是否采用最小授权原则。	是□ 否□ 不适用□	
1.3.	**安全审计**			
1.3.1.	服务器主机的审计内容是否包括：用户的添加和删除、审计功能的启动和关闭、审计策略的调整、权限变更、系统资源的异常使用、重要的系统操作（如用户登录、退出）等。	检查审计内容是否至少包括：用户的添加和删除、审计功能的启动和关闭、审计策略的调整、权限的变更、系统资源的异常使用、重要的系统操作（如用户登录、退出）等。	是□ 否□ 不适用□	

表 G.2　集中交易系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
1.3.2.	服务器主机的审计记录是否包括事件的日期、时间、类型、主体标识、客体标识和结果等。	检查主要服务器操作系统、重要终端操作系统的安全审计策略，查看审计记录信息是否包括事件发生的日期与时间、触发事件的主体与客体、事件的类型、事件成功或失败、事件的结果等内容。	是□ 否□ 不适用□	
1.3.3.	是否保护审计记录，避免受到未预期的删除、修改或覆盖等。审计记录是否至少保存6个月。	a)检查主要服务器操作系统、重要终端操作系统的安全审计策略，查看是否通过日志覆盖周期、存储方式、日志文件/空间大小、日志文件操作权限等设置，实现了对审计记录的保护，使其避免受到未预期的删除、修改或覆盖等； b)检查审计记录是否至少保存6个月。	是□ 否□ 不适用□	
1.3.4.	服务器主机的审计范围是否覆盖到服务器和重要客户端上的每个操作系统用户；应在保证系统运行安全和效率的前提下，启用系统审计或采用第三方安全审计产品实现审计要求。	a)检查主要服务器操作系统、重要终端操作系统和主要数据库管理系统的安全审计策略，查看安全审计配置是否包括系统内重要用户行为、系统资源的异常和重要系统命令的使用等重要的安全相关事件； b)检查是否在确保系统运行安全和效率的前提下，启用系统审计或采用第三方安全审计产品实现审计要求。	是□ 否□ 不适用□	
1.3.5.	是否能够根据记录数据进行分析，并生成审计报表。	检查主要服务器操作系统、重要终端操作系统和主要数据库管理系统的安全审计策略，查看是否为授权用户提供浏览和分析审计记录的功能，是否可以根据需要自动生成不同格式的审计报表。	是□ 否□ 不适用□	
1.4.	**安全管理**			
1.4.1.	操作系统是否遵循最小安装的原则，仅安装需要的组件和应用程序，并通过设置升级服务器等方式保持系统补丁及时得到更新。持续跟踪厂商提供的系统升级更新情况，是否在经过充分的测试评估后对必要的系统补丁进行及时更新。	a)检查主要服务器操作系统中所安装的系统组件和应用程序是否都是必须的； b)检查是否设置了专门的升级服务器实现对主要服务器操作系统补丁的升级，主要服务器操作系统是否具有操作系统补丁更新策略； c)检查是否持续跟踪厂商提供的系统升级更新情况，对关键性补丁是否进行充分的评估测试，并记录了相关评估情况和升级过程。	是□ 否□ 不适用□	

表 G.2　集中交易系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
1.4.2.	是否能够检测到对重要服务器进行入侵的行为，能够记录入侵的源IP、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警；针对重要服务器的入侵行为检测是否通过网络级或主机级入侵检测系统等方式实现。	a)查看“表0.3-该机房的攻击防护措施”，检查入侵防范系统的入侵防范策略，查看是否能够记录对主要服务器攻击的源IP、攻击类型、攻击目标、攻击时间等，在发生严重入侵事件时是否提供报警（如声音、短信和EMAIL等）；应当同时检查入侵防范系统的特征库是否保持最新状态； b)渗透测试主要服务器操作系统和主要数据库管理系统，查看入侵防范系统是否及时正确记录了本次攻击行为，并自动报警。	是□ 否□ 不适用□	
1.4.3.	是否能够对重要程序的完整性进行检测，并在检测到完整性受到破坏后具有恢复的措施。如不能正常恢复，是否停止有关服务，并提供报警。	检查主要服务器完整性保护情况说明，确认提供对重要程序的完整性进行检测，并在检测到完整性受到破坏后具有恢复的措施的功能。	是□ 否□ 不适用□	
1.4.4.	是否对所有服务器和终端设备安装防木马、病毒等防恶意代码软件，定期进行全面检查，并及时更新防恶意代码软件版本和恶意代码库。a)原则上所有主机应安装防恶意代码软件，系统不支持该要求的除外；b) 未安装防恶意代码软件的主机，应采取有效措施进行恶意代码防范。	查看“表0.3-该机房的病毒木马防护软件情况”，检查关键服务器的恶意代码防范策略，对支持安装防恶意代码软件的主机操作系统，查看是否安装了实时检测与查杀恶意代码的软件产品，并且及时更新了软件版本和恶意代码库。	是□ 否□ 不适用□	
1.4.5.	是否支持防恶意代码软件的统一管理。	a)访谈安全管理员，询问防恶意代码软件是否由专人负责进行管理和维护； b)检查主机防恶意代码软件维护记录，确认防恶意代码软件由专人统一管理。	是□ 否□ 不适用□	
1.4.6.	主机防恶意代码产品是否具有与网络防恶意代码产品不同的恶意代码库。	检查主机防恶意代码软件或硬件，查看其厂家名称、产品版本号和恶意代码库名称等，查看其是否与网络防恶意代码软件有不同的恶意代码库。	是□ 否□ 不适用□	

表 G.2　集中交易系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
1.4.7.	是否提高所有用户的防病毒意识，告知及时升级防病毒软件，在读取移动存储设备上的数据以及网络上接收文件或邮件之前，先进行病毒检查，对外来计算机或存储设备接入网络系统之前也应进行病毒检查。	访谈系统运维负责人，询问是否对员工进行基本恶意代码防范意识的教育，是否告知应及时升级软件版本，使用外来设备、网络上接收文件和外来计算机或存储设备接入网络系统之前进行病毒检查等。	是□ 否□ 不适用□	
1.4.8.	是否定期检查主机防病毒产品的恶意代码库的升级情况并进行记录，对截获的危险病毒或恶意代码进行及时分析处理，并形成书面的报表和总结汇报。	a)询问安全管理员，主机防病毒产品的恶意代码库的升级机制； b)检查恶意代码库的升级记录，判断是否定期； c)检查恶意代码分析报告，确认对主机防病毒产品上截获的危险病毒或恶意代码进行了及时分析处理。	是□ 否□ 不适用□	
1.4.9.	是否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。	a)查看病毒扫描记录，判断是否定期对服务器进行全面病毒扫描； b)检查病毒扫描时间，确认未在交易时段内进行。	是□ 否□ 不适用□	
1.5.	**资源控制**			
1.5.1.	是否通过设定终端接入方式、网络地址范围等条件限制终端登录。	检查主要服务器操作系统的资源控制策略，查看是否设定了终端接入方式、网络地址范围等条件限制终端登录。	是□ 否□ 不适用□	
1.5.2.	是否根据安全策略设置登录终端的操作超时锁定。	a)访谈运维负责人，询问是否存在登录终端的操作超时锁定的安全策略； b)现场测试安全策略的有效性。	是□ 否□ 不适用□	
1.5.3.	是否限制单个用户对系统资源的最大或最小使用限度。	检查主要服务器操作系统和主要数据库管理系统的资源控制策略，查看是否设置了单个用户或应用对系统资源的最大或最小使用限度。	是□ 否□ 不适用□	
1.6.	**主机运维**			
1.6.1.	是否对重要服务器进行监视，包括监视服务器的CPU、硬盘、内存、网络等资源的使用情况。	查看“表0.4附表-该机房的网上信息系统监控情况”，检查主要服务器操作系统的资源控制策略，查看是否对CPU、硬盘、内存和网络等资源的使用情况进行监控。	是□ 否□ 不适用□	
1.6.2.	重要服务器的CPU利用率、内存、磁盘存储空间等指标超过预先规定的阈值后是否实时进行报警。	检查重要服务器监控系统的日志记录，CPU利用率、内存、磁盘存储空间等指标超过预先规定的阈值后是否实时进行报警。	是□ 否□ 不适用□	

表 G.2　集中交易系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
1.6.3.	是否对操作系统的参数配置、调优，编制文档并保持更新。	a)访谈系统管理员，询问是否知悉其职责范围； b)检查维护记录，确认及时维修、更换故障设备和更新软件，关闭了与业务无关的服务，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； c)检查参数配置文档，确认及时对应用系统、操作系统的参数进行了配置、调优； d)检查系统容量评估报告，确认定期对系统容量进行了检查和评估。	是□ 否□ 不适用□	
2.	**系统管理**			
2.1.	**系统架构**			
2.1.1.	是否为证券交易所或登记结算机构采集客户交易终端信息提供相应的数据接口，并符合国家信息安全标准。	检查客户交易终端信息数据采集接口功能设计和验收文档，确认为证券交易所或登记结算机构采集客户交易终端信息提供相应的数据接口。	是□ 否□ 不适用□	
2.1.2.	是否提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的数据格式或长度符合系统设定要求。	a)检查设计或验收文档，查看是否有对人机接口输入或通信接口输入的数据进行有效性检验； b)测试主要应用系统，查看应用系统是否能明确拒绝不符合格式要求数据。	是□ 否□ 不适用□	
2.1.3.	是否提供自动保护功能，当故障发生时自动保护当前所有状态，保证系统能够进行恢复。	a)检查设计或验收文档，查看是否在故障发生时自动保护当前所有状态保证系统能够进行恢复的描述； b)测试主要应用系统，验证是否提供自动保护功能，当故障发生时自动保护当前所有状态，保证系统能够进行恢复。	是□ 否□ 不适用□	
2.2.	**系统建设**			
2.2.1.	在开展信息系统新建、升级、变更、换代等建设项目时，是否进行充分论证和测试，论证材料包括需求分析、立项报告等。	a)访谈信息技术负责人，询问是否在开展信息系统新建、升级、变更、换代等建设项目时，进行充分论证和测试，以及确保落实的机制； b)检查是否具有相关测试报告、论证材料（包括需求分析、立项报告等）。	是□ 否□ 不适用□	

表 G.2　集中交易系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.2.2.	是否制定详细的工程实施方案控制实施过程，并要求工程实施单位能正式地执行安全工程过程。	a)检查系统建设方面的管理制度，查看其是否包括工程实施过程的控制方法、实施参与人员的行为准则等方面内容； b)检查工程实施方案，查看其是否包括工程时间限制、进度控制和质量控制等方面内容，是否按照工程实施方面的管理制度进行各类控制、产生阶段性文档等。	是□ 否□ 不适用□	
2.2.3.	是否向用户提供系统建设文档和运行维护所需文档。	检查系统交付提交的文档，查看是否有指导用户进行系统运维的文档等，提交的文档是否符合管理规定的要求。	是□ 否□ 不适用□	
2.2.4.	是否书面规定系统交付的控制方法和人员行为准则。	检查系统建设方面的管理制度，查看其是否包括系统交付的控制方法和人员行为准则的规定。	是□ 否□ 不适用□	
2.2.5.	是否指定专门部门管理系统交付，并按照要求完成交付工作。	访谈系统建设负责人，询问是否有专门的部门负责系统交接工作，系统交接工作是否根据交付清单对所交接的设备、文档、软件等进行清点。	是□ 否□ 不适用□	
2.2.6.	是否建立交付流程，对建成的信息系统交付运行维护的活动进行规范。	检查交付管理制度，查看交付流程是否对建成的信息系统交付运行维护的活动进行规范。	是□ 否□ 不适用□	
2.2.7.	是否制定交付工作清单，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。	检查是否具有系统交付清单，查看交付清单是否说明系统交付的各类设备、软件、文档等。	是□ 否□ 不适用□	
2.2.8.	是否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。	a)访谈系统建设负责人，询问系统正式运行前是否对运行维护人员进行过培训，针对哪些方面进行过培训； b)检查是否有系统交付技术培训记录，查看是否包括培训内容、培训时间和参与人员等。	是□ 否□ 不适用□	
2.2.9.	是否制定交付实施计划，划定交付双方的职责，交付的步骤，并对交付过程留存记录。	检查是否具有交付实施计划，查看交付实施计划是否划定交付双方的职责，交付的步骤，并对交付过程留存记录。	是□ 否□ 不适用□	
2.2.10.	是否制定信息系统备份能力建设工作计划。	检查信息技术部门是否编制了信息系统备份能力建设工作计划。	是□ 否□ 不适用□	

表 G.2　集中交易系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.3.	**测试验收**			
2.3.1.	是否建立完整、规范的系统测试操作流程，对测试工作的计划、实施及总结做出详细的规定。对于在生产系统上进行的测试工作，必须制定详细的系统及数据备份、测试环境搭建、测试后系统及数据恢复、生产系统审核等计划，确保生产系统的安全。	检查系统测试操作流程，是否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。	是□ 否□ 不适用□	
2.3.2.	测试验收前是否根据设计方案或合同要求等制订测试验收方案，在测试验收过程中详细记录测试验收结果，并形成测试验收报告。	a)访谈系统建设负责人，询问是否根据设计方案或合同要求组织相关部门和人员制定工程测试验收方案，并对系统测试验收报告进行审定； b)检查是否具有工程测试验收方案，查看其是否明确说明参与测试的部门、人员、测试验收内容、现场操作过程等内容，过程控制是否符合管理规定的要求.	是□ 否□ 不适用□	
2.3.3.	是否组织相关部门和相关人员对系统测试验收报告进行审定，并签字确认。	检查是否具有系统测试验收报告，是否有相关部门和人员对系统测试验收报告进行审定的意见。	是□ 否□ 不适用□	
2.3.4.	是否委托第三方测试单位测试系统安全性，并出具安全性测试报告。	检查是否具有系统测试验收报告，是否有第三方测试机构的签字或盖章。	是□ 否□ 不适用□	
2.3.5.	是否书面规定系统测试验收的控制方法和人员行为准则。	检查系统建设方面的管理制度，查看其是否包括对系统测试验收的控制方法和人员行为准则规定。	是□ 否□ 不适用□	
2.3.6.	是否指定或授权专门的部门负责系统测试验收的管理，并按照管理规定的要求完成系统测试验收工作。	访谈系统建设负责人，询问是否有专门的部门负责测试验收工作，由何部门负责；是否委托第三方测试机构对信息系统进行独立的安全性测试。	是□ 否□ 不适用□	
2.3.7.	是否为系统测试配备必要的人员和设备资源，需要时协调关联单位配合测试。	访谈开发负责人，询问是否为系统测试配备必要的人员和设备资源，需要时协调关联单位配合测试。	是□ 否□ 不适用□	
2.3.8.	是否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覆盖功能、性能、容量、安全性、稳定性等方面。测试完成后对测试结果进行分析评估，并给出测试报告。	a)访谈开发负责人，询问是否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； b)检查是否具有测试方案，是否包括覆盖功能、性能、容量、安全性、稳定性等方面； c)检查近期上线系统的测试报告。	是□ 否□ 不适用□	

表 G.2　集中交易系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.3.9.	是否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。模拟环境是否与生产环境进行有效隔离，不得对生产环境进行干扰。	检查“表 0.3-网络边界防护情况-交易业务网与模拟环境测试网络”，检查系统模拟环境逻辑架构，查看系统模拟环境在逻辑架构上是否与生产环境一致，是否与生产环境有效隔离。	是□ 否□ 不适用□	
2.3.10.	是否根据测试方案的设计，合理配置模拟环境测试所需的设备，识别设备不同可能带来的测试结果正确性风险。	a)访谈开发负责人，询问是否根据测试方案的设计，合理配置模拟环境测试所需的设备，识别设备不同可能带来的测试结果正确性风险； b)检查系统测试方案、测试报告，查看是否有设备不同可能带来的测试结果正确性风险的说明。	是□ 否□ 不适用□	
2.3.11.	是否根据需要，要求生产系统运维人员和业务部门组织业务人员参与模拟环境测试。	a)访谈开发负责人，询问是否根据需要，要求生产系统运维人员和业务部门组织业务人员参与模拟环境测试； b)查看测试通知或记录，是否有生产系统运维人员和业务部门组织业务人员参与。	是□ 否□ 不适用□	
2.3.12.	模拟环境使用的密码是否与生产系统严格区分，系统管理员宜由不同的人员担任。	访谈开发负责人，询问模拟环境使用的密码是否与生产系统严格区分，系统管理员由不同的人员担任。	是□ 否□ 不适用□	
2.3.13.	生产环境测试前是否备份当前系统的数据和配置。	a)检查系统测试管理制度和操作流程，查看数据和配置备份要求； b)抽查在生产系统上进行测试的工作记录，检查是否做好数据备份。	是□ 否□ 不适用□	
2.3.14.	是否提前发布生产环境测试的系统测试公告。	a)访谈开发负责人，询问是否提前发布生产环境测试系统测试公告； b)查看一次使用生产环境测试的测试公告。	是□ 否□ 不适用□	
2.3.15.	是否由生产系统运维人员在生产环境下组织完成生产环境测试。	a)访谈开发负责人，询问是否由生产系统运维人员在生产环境下组织完成生产环境测试； b)查看一次生产环境测试的测试方案、测试记录，是否由生产系统运维人员在生产环境下组织完成生产环境测试。	是□ 否□ 不适用□	

表 G.2　集中交易系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.3.16.	是否根据需要，要求业务部门组织业务人员参与生产环境测试。	a)访谈开发负责人，询问是否根据需要，要求业务部门组织业务人员参与生产环境测试； b)查看一次生产环境测试的测试方案、测试记录，是否根据需要，要求业务部门组织业务人员参与生产环境测试。	是□ 否□ 不适用□	
2.3.17.	是否根据生产环境测试的结果设计系统升级过程及应急预案。	a)访谈开发负责人，询问是否根据生产环境测试的结果设计系统升级过程及应急预案； b)抽查一次生产环境测试报告和系统变更方案。	是□ 否□ 不适用□	
2.3.18.	如果生产环境测试内容涉及其他相关系统，是否协调其他系统用户参与测试。	a)访谈开发负责人，询问如果生产环境测试内容涉及其他相关系统，是否协调其他系统用户参与测试； b)抽查测试方案、测试记录，是否体现其他系统用户。	是□ 否□ 不适用□	
2.3.19.	涉及核心交易业务系统的上线测试，是否组织全市场或全公司各相关部门测试。	a)访谈开发负责人，询问涉及核心交易业务系统的上线测试，是否组织全市场或全公司各相关部门测试； b)抽查核心系统上线测试方案、测试记录，是否体现参测机构及部门。	是□ 否□ 不适用□	
2.3.20.	测试后是否恢复生产环境并验证恢复的有效性。	a)访谈开发负责人，询问测试后是否恢复生产环境并验证恢复的有效性； b)抽查测试方案、恢复验证记录。	是□ 否□ 不适用□	
2.3.21.	是否禁止交易时段使用生产环境进行测试。	a)访谈开发负责人，询问是否交易时段不得使用生产环境进行测试； b)抽查测试方案、测试记录、测试报告，查看是否在交易时段测试。	是□ 否□ 不适用□	
2.3.22.	是否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。	查看测试记录，是否在设备和软件投入使用前进行必要的验证性测试。	是□ 否□ 不适用□	

表 G.2　集中交易系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.4.	**系统运维**			
2.4.1.	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。	a)检查运维管理制度，是否包括机房管理、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； b)检查运维操作流程，是否包括日常操作、事件处理、问题处理、系统变更、应急处置等。	是□ 否□ 不适用□	
2.4.2.	交易业务系统的操作规程是否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。	检查交易业务系统的操作规程，是否包括操作的对象、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。	是□ 否□ 不适用□	
2.4.3.	是否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进行记录留痕，记录的保存时间不少于一年。	检查一年内对交易业务系统的操作记录，是否严格按照操作手册执行运维操作。	是□ 否□ 不适用□	
2.4.4.	特殊操作、临时操作是否经批准后方可双岗执行。操作过程是否进行记录留痕，记录的保存时间是否不少于一年。	抽查公司一年内特殊操作和临时操作的记录，检查相关操作是否经过审批，是否有操作人员和复核人员签名确认。	是□ 否□ 不适用□	
2.4.5.	是否依据业务、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。	抽查修订记录，确认业务或信息系统发生重大变更时，是否对相关系统操作手册及规程进行修订并经过审批。	是□ 否□ 不适用□	
2.4.6.	是否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，是否开启自动监控系统和自动报警系统。	a)访谈运维负责人，询问是否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； b)检查巡检记录，是否包括报单数、成交数、委托数、CPU 使用率、内存使用率等指标。	是□ 否□ 不适用□	
2.4.7.	是否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。	a)访谈运维负责人，询问是否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； b)检查定期检查、评估的记录或报告，确定是否设定了预警阈值。	是□ 否□ 不适用□	

表 G.2　集中交易系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.4.8.	主机监控指标是否包括：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。	a)检查“表 0.4-系统监控情况”，检查系统设计和验收文档，服务器监控指标是否包括设备运行状态、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； b)现场检查主机监控情况。	是□ 否□ 不适用□	
2.4.9.	存储监控指标是否包括：设备运行状态、数据交换延时、存储电池状态等。	a)检查“表 0.4-系统监控情况”，检查系统设计和验收文档，存储监控指标是否包括设备运行状态、数据交换延时、存储电池状态等； b)现场检查存储监控情况。	是□ 否□ 不适用□	
2.4.10.	数据库监控指标是否包括日志信息、表空间使用率、连接数等。	a)检查“表 0.4-系统监控情况”，检查系统设计和验收文档，数据库监控指标是否包括日志信息、表空间使用率、连接数等； b)现场检查数据库监控情况。	是□ 否□ 不适用□	
2.4.11.	核心交易业务相关的应用系统监控指标是否包括进程的活动状态、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。	a)检查“表 0.4-系统监控情况”，检查系统设计和验收文档，检查相关的应用系统监控指标，是否包括进程的活动状态、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； b)现场检查应用系统监控情况。	是□ 否□ 不适用□	
2.4.12.	是否针对不同系统设置合理的监测频度。	a)访谈运维负责人，询问是否针对不同系统设置合理的监测频度； b)查阅相关系统设置文档，是否有监测频度的说明； c)根据监测频度说明，检查相关参数设置情况。	是□ 否□ 不适用□	
2.4.13.	持续跟踪厂商提供的系统升级更新情况，是否在经过充分的测试评估后对必要的补丁进行及时更新，并在安装系统补丁前对现有的重要文件进行备份。	a)访谈系统管理员，了解系统补丁更新程序和评估方法； b)查看系统补丁更新记录，确认持续跟踪厂商提供的系统升级更新情况，确认在对重要文件进行备份后，才实施系统补丁程序的安装。	是□ 否□ 不适用□	

表 G.2　集中交易系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.4.14.	是否依据操作手册对系统进行维护，详细记录操作日志，包括重要的日常操作、运行维护记录、参数的设置和修改等内容，严禁进行未经授权的操作。	a)访谈信息技术部门负责人和操作人员，了解对系统进行维护审批和操作步骤； b)检查运维操作手册和操作日志，确认是否包括重要的日常操作、运行维护记录、参数的设置和修改等内容，确认按照授权进行操作。	是□ 否□ 不适用□	
2.4.15.	是否保持系统的可用性，及时维修、更换故障设备和更新软件。	检查运维操作手册,是否包括保持系统的可用性，及时维修、更换故障设备和更新软件。	是□ 否□ 不适用□	
2.4.16.	是否负责应用系统的参数配置、调优，编制文档并保持更新。	检查运维操作手册,是否包括对应用系统、操作系统的参数进行配置、调优，编制文档并保持更新。	是□ 否□ 不适用□	
2.4.17.	是否定期对系统容量进行检查和评估，形成评估报告。	检查系统容量评估报告，是否定期对系统容量进行检查和评估。	是□ 否□ 不适用□	
2.4.18.	是否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。	检查运维操作手册,是否包括管理系统和应用程序服务进程，并关闭与业务无关的服务。	是□ 否□ 不适用□	
2.4.19.	是否对新上线的设备在接入运行网络前进行全面的安全检查。	a)访谈安全管理员，了解设备上线前的安全检查流程； b)查看设备上线前的漏洞扫描、渗透测试、病毒扫描、木马检测等扫描报告。	是□ 否□ 不适用□	
2.5.	**变更管理**			
2.5.1.	是否确认系统中要发生的变更，并制定相应的变更方案；重要系统变更前是否制定详细的变更方案、失败恢复方案、专项应急预案。	a)访谈系统运维负责人，询问系统变更机制或流程，是否针对系统的重大变更制定变更方案、失败恢复方案、专项应急预案； b)现场检查变更方案，抽查重要系统变更是否制定详细的变更方案、失败恢复方案、专项应急预案。	是□ 否□ 不适用□	
2.5.2.	是否建立变更控制的申报和审批文件化程序，对变更影响进行分析并文档化，记录变更实施过程，并妥善保存所有文档和记录。	检查是否有变更管理制度，查看其是否覆盖变更前审批、变更过程记录、变更后通报等方面内容，是否包括变更申报、审批程序，是否规定需要申报的变更类型、申报流程、审批部门、批准人等方面内容。	是□ 否□ 不适用□	

表 G.2　集中交易系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.5.3.	是否建立中止变更并从失败变更中恢复的文件化程序，明确过程控制方法和人员职责，必要时对恢复过程进行演练。	检查系统变更方案，查看其是否覆盖变更类型、变更原因、变更过程、变更前评估、变更失败恢复程序等方面内容，查看其是否有主管领导的批准签字。	是□ 否□ 不适用□	
2.5.4.	是否建立系统变更流程，对信息系统的变更活动进行规范。	检查变更管理流程。	是□ 否□ 不适用□	
2.5.5.	是否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。	检查系统变更记录，系统变更中的角色是否包括申请人、审批人、实施人、复核人。	是□ 否□ 不适用□	
2.5.6.	变更申请人是否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。	检查系统变更申请，申请中是否有明确的变更方案，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。	是□ 否□ 不适用□	
2.5.7.	变更审批人是否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。	a)检查变更风险评估报告，判断变更审批人是否充分评估变更的技术风险和业务风险； b)检查变更审批记录，是否审批记录留痕并满足审计需要。	是□ 否□ 不适用□	
2.5.8.	变更审批人是否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。	检查变更审批记录，变更审批人是否确定了变更实施时间窗口，做到了除紧急变更外，不得在交易时段进行变更实施。	是□ 否□ 不适用□	
2.5.9.	是否按照测试方案，组织变更前后的测试，测试后是否提交测试记录或报告。	检查变更测试记录或报告，是否按照测试方案，组织变更前后的测试。	是□ 否□ 不适用□	
2.5.10.	变更实施人是否按照变更实施方案进行变更，并及时更新配置库。	a)检查系统变更记录，变更实施人是否按照变更实施方案进行变更； b)检查系统配置库，是否变更后及时更新配置库。	是□ 否□ 不适用□	
2.5.11.	变更复核人是否对变更记录和变更结果进行评估，评估内容是否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。	检查变更复核记录，变更复核人是否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。	是□ 否□ 不适用□	

表 G.2　集中交易系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.6.	**安全管理**			
2.6.1.	是否建立至少每季度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。	a)访谈系统管理员，询问是否定期对系统进行漏洞扫描，扫描周期多长，发现漏洞是否及时修补，在安装系统补丁前是否对重要文件进行备份，是否先在测试环境中测试通过再安装； b)检查是否至少每季进行一次漏洞扫描，并对漏洞风险持续跟踪，在经过充分的验证测试后，对必要的漏洞开展修补工作。	是□ 否□ 不适用□	
2.7.	**身份鉴别**			
2.7.1.	是否提供专用的登录控制模块对登录用户进行身份标识和鉴别。	检查主要应用系统设计和验收文档，查看是否提供身份标识和鉴别功能。	是□ 否□ 不适用□	
2.7.2.	是否提供用户身份标识唯一和鉴别信息复杂度检查功能，保证应用系统中不存在重复用户身份标识，身份鉴别信息不易被冒用。	检查主要应用系统设计和验收文档，查看是否采用了措施保证身份标识具有唯一性，是否对登录用户的口令最小长度、复杂度和更换周期等进行了要求和限制，保证身份鉴别信息不易被冒用。	是□ 否□ 不适用□	
2.7.3.	是否提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施。	检查主要应用系统设计和验收文档，查看是否提供登录失败处理功能，是否根据安全策略设置了登录失败次数等参数。	是□ 否□ 不适用□	
2.7.4.	是否启用身份鉴别、用户身份标识唯一性检查、用户身份鉴别信息复杂度检查以及登录失败处理功能，并根据安全策略配置相关参数。	a)测试主要应用系统，可通过试图以合法和非法用户分别登录系统，验证身份标识和鉴别功能是否有效； b)测试主要应用系统，可通过多次输入错误的密码，验证登录失败处理功能是否有效； c)渗透测试主要应用系统，如多次猜测用户口令，验证应用系统身份标识和鉴别功能是否不存在明显的弱点。应当从互联网向被测试对象进行渗透测试。	是□ 否□ 不适用□	
2.7.5.	管理用户通过受控本地控制台管理应用系统时，是否采用一种或一种以上身份鉴别技术。	检查应用系统设计和验收文档，当管理用户通过受控本地控制台管理应用系统时，是否采用了一种或一种以上身份鉴别技术。	是□ 否□ 不适用□	

表 G.2　集中交易系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.7.6.	管理用户以远程方式登录应用系统，是否采用两种或两种以上组合的鉴别技术进行身份鉴别。	检查应用系统设计和验收文档，当管理用户以远程方式登录应用系统，是否采用了两种或两种以上组合的鉴别技术进行身份鉴别。	是□ 否□ 不适用□	
2.7.7.	面向互联网服务的系统是否提供两种或两种以上组合的鉴别技术供用户选择。	检查应用系统设计和验收文档，面向互联网服务的系统是否向用户提供两种或两种以上组合的鉴别技术供用户选择。	是□ 否□ 不适用□	
2.7.8.	是否禁止设置弱口令，若系统条件允许，口令是否采用数字、字母、符号混排且无规律的方式。	检查口令管理制度，是否规定口令应采用数字、字母、符号混排且无规律的方式。	是□ 否□ 不适用□	
2.7.9.	是否禁止设置弱口令，若系统条件允许，管理员口令长度原则上不少于 12 位。	检查口令管理制度，是否规定管理员用户口令的长度至少为 12 位。	是□ 否□ 不适用□	
2.7.10.	核心交易业务系统是否提示并阻止用户使用弱口令登录。	检查核心交易业务系统设计和验收文档，确定核心交易业务系统是否提示并阻止用户使用弱口令登录。	是□ 否□ 不适用□	
2.7.11.	是否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。	检查口令管理制度，是否规定管理员用户口令至少每季度更换 1 次，更新的口令至少 5 次内不能重复。	是□ 否□ 不适用□	
2.7.12.	应用系统的账户及口令是否采用加密方式存储、传输，加密产品的使用是否符合国家有关规定。	检查口令管理制度，是否规定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。	是□ 否□ 不适用□	
2.7.13.	是否重点加强对匿名/默认用户的管理，防止被非法使用。	a)检查账户列表，是否没有匿名/默认用户； b)若有匿名/默认用户，测试是否不能被非法使用。	是□ 否□ 不适用□	
2.7.14.	是否及时注销不再使用的账户。	检查在岗人员名单和账户列表，确定没有未注销的不再使用的账户。	是□ 否□ 不适用□	
2.7.15.	是否设置抵御连续猜测等对客户账户恶意攻击行为的策略。	a)检查连续猜测等对客户账户恶意攻击行为的策略； b)现场测试系统抵御连续猜测客户账户的攻击行为。	是□ 否□ 不适用□	

表 G.2　集中交易系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.8.	**访问控制**			
2.8.1.	是否提供访问控制和权限管理机制，依据安全策略控制用户对文件等客体的访问，防止客户的授权被恶意提升或转授，防止客户使用未经授权的功能，防止客户进行访问未经授权的数据等非法访问活动。	a)检查应用系统设计和验收文档，查看是否依据安全策略控制用户对文件等客体的访问； b)测试主要应用系统，可通过以不同权限的用户登录系统，查看其拥有的权限是否与系统赋予的权限一致，验证应用系统访问控制功能是否有效。	是□ 否□ 不适用□	
2.8.2.	访问控制的覆盖范围是否包括与资源访问相关的主体、客体及它们之间的操作。	检查应用系统设计和验收文档，查看其访问控制的覆盖范围是否包括与信息安全直接相关的主体、客体及它们之间的操作。	是□ 否□ 不适用□	
2.8.3.	是否由授权主体配置访问控制策略，并严格限制默认账户的访问权限。	a)检查应用系统设计和验收文档，查看其访问控制的覆盖范围是否包括与信息安全直接相关的主体、客体及它们之间的操作； b)测试主要应用系统，可通过以默认用户登录系统，并进行一些合法和非法操作，验证系统是否严格限制了默认帐户的访问权限。	是□ 否□ 不适用□	
2.8.4.	是否授予不同账户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系。	a)检查应用系统的用户角色或权限的分配情况，查看是否仅授予不同帐户为完成各自承担任务所需的最小权限，特权用户的权限是否分离，权限之间是否相互制约，如系统管理员不能进行审计操作、审计员不能进行系统管理操作等； b)渗透测试主要应用系统，进行试图绕过访问控制的操作，验证应用系统的访问控制功能是否不存在明显的弱点。	是□ 否□ 不适用□	
2.8.5.	是否根据业务需求和系统安全分析确定系统的访问控制策略。	a)访谈系统运维负责人，询问是否指定专门的部门或人员负责系统管理，如根据业务需求和系统安全分析制定系统的访问控制策略，控制分配文件及服务的访问权限； b)查看访问控制策略文档，判断是否根据业务需求和系统安全分析制定了系统的访问控制策略。	是□ 否□ 不适用□	

表 G.2　集中交易系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.8.6.	是否指定专人对系统进行管理，划分系统管理员角色，明确各个角色的权限、责任和风险，权限设定是否遵循最小授权原则。	访谈系统运维负责人，询问是否对系统管理员用户进行分类，明确各个角色的权限、责任和风险，权限设定是否遵循最小授权原则。	是□ 否□ 不适用□	
2.9.	**资源控制**			
2.9.1.	用户登录应用系统后在规定的时间内未执行任何操作，是否自动退出系统。	测试主要应用系统，当应用系统的通信双方中的一方在一段时间内未作任何响应，查看另一方是否能够自动结束会话。	是□ 否□ 不适用□	
2.9.2.	是否能够对系统的最大并发会话连接数进行限制。	检查主要应用系统的配置参数，查看是否提供对最大并发会话连接数进行限制。	是□ 否□ 不适用□	
2.9.3.	是否能够对单个账户的多重并发会话进行限制。	测试主要应用系统，可通过对系统进行超过规定的单个帐户的多重并发会话数进行连接，验证系统是否能够正确地限制单个帐户的多重并发会话数。	是□ 否□ 不适用□	
2.9.4.	是否能够对一个时间段内可能的并发会话连接数进行限制。	检查主要应用系统的配置参数，查看是否提供对最大并发会话连接数进行限制。	是□ 否□ 不适用□	
2.9.5.	是否能够对一个访问账户或一个请求进程占用的资源分配最大限额和最小限额。	检查主要应用系统设计和验收文档，查看是否对一个访问帐户或一个请求进程占用的资源分配最大限额和最小限额。	是□ 否□ 不适用□	
2.9.6.	是否能够对系统服务水平降低到预先规定的最小值进行检测和报警。	a)检查主要应用系统设计和验收文档，查看是否有服务水平最小值的设定，当系统的服务水平降低到预先设定的最小值时，系统报警； b)测试主要应用系统，可试图使服务水平降低到预先规定的最小值，验证系统是否能够正确检测并报警。	是□ 否□ 不适用□	
2.9.7.	是否提供服务优先级设定功能，并在安装后根据安全策略设定访问账户或请求进程的优先级，根据优先级分配系统资源。	检查主要应用系统设计和验收文档，查看是否能根据安全策略设定主体的服务优先级，根据优先级分配系统资源。	是□ 否□ 不适用□	

表 G.2　集中交易系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.10.	**数据安全**			
2.10.1.	通过互联网、卫星网进行通信时，是否采用密码技术保证通信过程中数据的完整性。	a)检查设计、验收文档或源代码，查看其是否有关于保护通信完整性的说明，如果有则查看是否有根据校验码判断对方数据有效性，以及散列（Hash）密码计算报文校验码的描述； b)对于通过互联网、卫星网进行通信的系统，通过截包分析，检查通信报文是否经过加密保护。	是□ 否□ 不适用□	
2.10.2.	是否能够检测到系统管理数据、鉴别信息和重要业务数据在传输过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施。	如果主要主机操作系统能够进行远程管理，则应查看应用系统的设计、验收文档或源代码，查看是否有关于能检测系统管理数据、鉴别信息和重要业务数据传输过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施的描述。	是□ 否□ 不适用□	
2.10.3.	是否采用加密或其他保护措施实现系统管理数据、鉴别信息和重要业务数据存储保密性。	检查主要应用系统设计文档，查看鉴别信息是否采用加密或其他有效措施实现存储保密性。	是□ 否□ 不适用□	
2.11.	**备份能力**			
2.11.1.	灾难应对能力是否达到《证券期货经营机构信息系统备份能力标准》第五级或重大灾难应对能力达到第六级要求。	检查“表0.8-系统备份能力”、“表0.8-数据备份情况”，查看灾难应对能力达标证明材料（包括：灾备系统建设情况、备份策略、应急演练记录等），确认灾难应对能力达到《证券期货经营机构信息系统备份能力标准》第五级或重大灾难应对能力达到第六级要求。	是□ 否□ 不适用□	
2.11.2.	重大灾难应对能力是否达到《证券期货经营机构信息系统备份能力标准》第六级要求。	检查“表0.8-系统备份能力”、“表0.8-数据备份情况”，查看灾难应对能力达标证明材料（包括：灾备系统建设情况、备份策略、应急演练记录等），确认重大灾难应对能力达到《证券期货经营机构信息系统备份能力标准》第六级要求。	是□ 否□ 不适用□	
2.11.3.	实时信息系统是否达到《证券期货经营机构信息系统备份能力标准》中故障应对能力的第四级要求。	检查“表0.8-系统备份能力”、“表0.8-数据备份情况”，检查公司实时信息系统故障应对能力达标证明材料（包括：备份系统建设情况、备份策略、应急演练记录等），确认故障应对能力达到《证券期货经营机构信息系统备份能力标准》中第四级要求。	是□ 否□ 不适用□	

表 G.2　集中交易系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.11.4.	法人清算系统、门户网站系统等非实时信息系统是否满足《证券期货经营机构信息系统备份能力标准》中故障应对能力的第二级要求。	检查“表0.8-系统备份能力”、“表0.8-数据备份情况”，检查公司非实时信息系统故障应对能力达标证明材料（包括：备份系统建设情况、备份策略、应急演练记录等），确认法人清算系统、门户网站系统等非实时信息系统的故障应对能力达到《证券期货经营机构信息系统备份能力标准》中故障应对能力的第二级要求。	是□ 否□ 不适用□	
2.12.	**安全审计**			
2.12.1.	应用系统是否能够对每个业务用户的关键操作进行记录，例如用户登录、用户退出、增加用户、修改用户权限等操作。	a)检查主要应用系统，查看审计范围是否覆盖到每个用户，审计策略是否覆盖系统内重要的安全相关事件，例如，用户标识与鉴别、访问控制的所有操作记录、重要用户行为、系统资源的异常使用、重要系统命令的使用等； b)测试主要应用系统，在应用系统上试图产生一些重要的安全相关事件（如进行用户登录、修改用户权限等操作），查看应用系统是否对其进行了审计，验证应用系统安全审计的覆盖情况是否覆盖到每个用户；如果进行了审计则查看审计记录内容是否包含事件的日期、时间、发起者信息、类型、描述和结果等。	是□ 否□ 不适用□	
2.12.2.	审计记录的内容是否包括事件日期、时间、发起者信息、类型、描述和结果等。审计记录是否至少保存6个月。	检查主要应用系统的审计记录，查看是否包括事件发生的日期与时间、触发事件的主体与客体、事件的类型、事件成功或失败、身份鉴别事件中请求的来源、事件的结果等内容；检查是否保存了6个月以上的审计记录。	是□ 否□ 不适用□	
2.12.3.	是否采取有效措施防止单独中断审计进程；审计进程应作为应用系统整体进程中的一部分，并且不能单独中断。	测试主要应用系统，试图非授权终止审计进程或审计功能，删除、修改或覆盖审计记录，查看安全审计进程和记录的保护情况。	是□ 否□ 不适用□	
2.12.4.	是否提供对审计记录数据进行统计、查询、分析及生成审计报表的功能。	检查主要应用系统，查看是否为授权用户浏览和分析审计数据提供专门的审计分析功能，并能根据需要生成审计报表。	是□ 否□ 不适用□	

表 G.2　集中交易系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.12.5.	是否保证信息系统日志的完备性，确保所有重大修改被完整地记录，确保开启审计留痕功能。证券公司信息系统日志是否至少保存 15 年。	a)检查运维管理制度，是否规定保证信息系统日志的完备性，确保所有重大修改被完整地记录，信息系统日志是否至少保存 15 年； b)检查系统设计和验收文档，是否开启审计留痕功能。	是□ 否□ 不适用□	
2.12.6.	是否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。	查看每日检查记录，是否指定人员按照运维管理制度和操作流程，对日常操作执行情况进行每日检查。	是□ 否□ 不适用□	
2.12.7.	是否每季组织开展内部检查，形成检查报告。	审阅内部检查报告，检查是否每季度一次。	是□ 否□ 不适用□	
2.12.8.	是否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。	a)审阅公司年度审计计划，是否包含信息系统运维管理工作审计项目； b)检查公司年度审计报告，是否包含信息系统运维管理工作审计项目。	是□ 否□ 不适用□	
2.12.9.	检查和审计范围是否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。	检查信息系统运维管理工作审计报告，确定信息系统运维管理工作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。	是□ 否□ 不适用□	
2.12.10.	是否对检查和审计的结果采取纠正性和预防性的措施。	审阅信息系统运维管理工作审计整改报告，确定是否对检查和审计的结果采取纠正性和预防性的措施。	是□ 否□ 不适用□	
2.12.11.	是否定期检查安全隔离情况，确保各安全域之间有效隔离。	a)查看包括自建和托管机房的网络拓扑图、安全域划分情况，检查各安全域之间是否采用了防火墙或安全网关等有效隔离方式和隔离手段； b)审阅最近的网络隔离情况检查报告，判断是否定期对上述事项进行了检查。	是□ 否□ 不适用□	

表 G.2　集中交易系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.12.12.	是否组织相关人员定期对监测和报警记录进行分析、评审，发现可疑行为，形成分析报告，并采取必要的应对措施。	a)访谈系统运维负责人，询问其是否组织人员定期对监测记录进行分析、评审，是否发现可疑行为并对其采取必要的措施，是否形成分析报告； b)检查监测记录，查看是否记录监控对象、监控内容、监控的异常现象处理等方面，查看是否对异常现象及处理措施形成分析报告。	是□ 否□ 不适用□	
2.12.13.	是否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。	检查是否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，以满足审计的需要。	是□ 否□ 不适用□	
2.12.14.	是否保存监控产生的日志，保存时间不少于一年。	检查监控日志，保存时间是否不少于一年。	是□ 否□ 不适用□	
2.12.15.	是否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。	查看评估记录，是否每日分析核心交易业务系统监控日志及巡检记录，并跟踪处理日志分析中发现的异常事件。	是□ 否□ 不适用□	
2.12.16.	是否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。	查看评估报告，是否至少每季度全面评估监控日志和操作记录，分析异常情况。	是□ 否□ 不适用□	
2.12.17.	是否至少每月对运行日志和审计数据进行分析。	检查是否每月对运行日志和审计数据进行分析。	是□ 否□ 不适用□	
3.	**数据库管理**			
3.1.	**安全审计**			
3.1.1.	审计内容是否至少包括：用户的添加和删除、审计功能的启动和关闭、审计策略的调整、权限变更、系统资源的异常使用、重要的系统操作（如用户登录、退出）等。	审阅主机审计记录，检查审计内容是否包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件；审计内容至少包括：用户的添加和删除、审计功能的启动和关闭、审计策略的调整、权限变更、系统资源的异常使用、重要的系统操作（如用户登录、退出）等。	是□ 否□ 不适用□	
3.1.2.	审计记录是否包括事件的日期、时间、类型、主体标识、客体标识和结果等。	审阅主机运行日志，检查审计记录是否包括事件的日期、时间、类型、主体标识、客体标识和结果等。	是□ 否□ 不适用□	

表 G.2　集中交易系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
3.1.3.	是否保护审计记录，避免受到未预期的删除、修改或覆盖等。审计记录是否至少保存 6 个月。	检查审计记录是否至少保存 6 个月。	是□ 否□ 不适用□	
3.1.4.	审计范围是否覆盖到服务器和重要客户端上的每个数据库用户；应在保证系统运行安全和效率的前提下，启用系统审计或采用第三方安全审计产品实现审计要求。	a)通过访谈，了解是否在保证系统运行安全和效率的前提下，启用了系统审计或采用第三方安全审计产品实现审计要求，保证产生、有效记录和存储了审计日志； b)通过访谈，审阅主机和客户端审计记录，判断是否覆盖到服务器和重要客户端上的每个操作系统用户和数据库用户。	是□ 否□ 不适用□	
3.1.5.	是否能够根据记录数据进行分析，并生成审计报表。	检查主要服务器操作系统、重要终端操作系统和主要数据库管理系统的安全审计策略，查看是否为授权用户提供浏览和分析审计记录的功能，是否可以根据需要自动生成不同格式的审计报表。	是□ 否□ 不适用□	
3.1.6.	是否保护审计进程，避免受到未预期的中断。	测试主要服务器操作系统、重要终端操作系统和主要数据库管理系统，可通过非审计员的其他帐户试图中断审计进程，验证审计进程是否受到保护。	是□ 否□ 不适用□	
3.2.	**访问控制**			
3.2.1.	是否严格限制人工对数据库操作的账户权限，并分别使用不同权限的账户执行查询、插入、更新、删除等操作。	a)查看数据库账户权限管理制度，是否规定分别使用不同权限的账户执行查询、插入、更新、删除等操作； b)检查对数据库进行人工操作的记录，确认使用不同权限的账户执行查询、插入、更新、删除等操作。	是□ 否□ 不适用□	
3.3.	**身份鉴别**			
3.3.1.	口令是否符合以下条件：数字、字母、符号混排，无规律的方式。	检查口令管理制度，是否规定口令符合以下条件：数字、字母、符号混排，无规律的方式。	是□ 否□ 不适用□	
3.3.2.	口令的长度是否至少为 12 位。	检查口令管理制度，是否规定管理员用户口令的长度至少为 12 位。	是□ 否□ 不适用□	
3.3.3.	口令是否至少每季度更换 1 次，更新的口令至少 5 次内不能重复。	检查口令管理制度，是否规定管理员用户口令至少每季度更换 1 次，更新的口令至少 5 次内不能重复。	是□ 否□ 不适用□	

表 G.2　集中交易系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
3.3.4.	如果设备口令长度不支持 12 位或其他复杂度要求，口令是否使用所支持的最长长度并适当缩小更换周期；也可以使用动态密码卡等一次性口令认证方式。	检查口令管理制度，是否规定口令应使用所支持的最长长度并适当缩小更换周期，也可以使用动态密码卡等一次性口令认证方式。	是□ 否□ 不适用□	
3.3.5.	是否为数据库系统的不同用户分配不同的用户名，确保用户名具有唯一性。	检查数据库系统的用户列表，标识是否唯一。	是□ 否□ 不适用□	
3.4.	**数据库运维**			
3.4.1.	是否保持数据库的可用性，及时维护、更新软件。	a)查看数据库软件、数据库监控软件的采购合同，以及维护、更新记录； b)查看数据库监控日志，判断表空间使用率、连接数等是否保持在合理范围。	是□ 否□ 不适用□	
3.4.2.	是否对数据库的参数进行配置、调优，编制文档并保持更新。	a)访谈数据库管理员,询问是否依照数据库配置文档进行安装、配置及调优； b)查看数据库配置文档和维护记录，确认对数据库系统进行了配置、调优。	是□ 否□ 不适用□	
3.4.3.	是否定期对数据库容量进行检查和评估，形成评估报告。	a)查看公司数据库容量管理制度，是否明确要求定期对数据库系统容量进行检查和评估，并形成评估报告； b)访谈数据库管理员，查看数据库容量评估报告，确认定期对数据库容量进行了检查和评估。	是□ 否□ 不适用□	
3.4.4.	是否管理数据库、表、索引、存储过程，数据库的升级、优化、扩容、迁移。	a)查看公司数据库容量管理制度，是否明确数据库管理员应负责管理数据库、表、索引、存储过程，数据库的升级、优化、扩容、迁移； b)访谈数据库管理员，查看数据库维护记录，确认数据库管理员按照要求管理数据库、表、索引、存储过程，对数据库进行了升级、优化、扩容、迁移等维护工作。	是□ 否□ 不适用□	
3.4.5.	是否定期检查数据库的用户、口令及权限设置的正确性。	访谈数据库管理员，查看数据库维护记录，确认是否定期检查数据库的用户、口令及权限设置的正确性。	是□ 否□ 不适用□	

表 G.2　集中交易系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
4.	**集中交易系统**			
4.1.	**系统架构**			
4.1.1.	集中交易系统是否在系统构架上支持前台操作与后台数据的分离。	a)访谈技术部门负责人交易系统的软件来源、版本情况、软件架构说明； b)检查软件架构说明，不应存在客户终端直接使用数据库接口，访问核心数据的情况； c)检查软件架构说明，不应存在为客户终端或者管理员终端提供通用的直接修改核心数据的方法。	是□ 否□ 不适用□	
4.1.2.	集中交易系统是否提供数据接口，满足稽核、审计及技术监控等的要求。	审阅系统设计文档，确定集中交易系统提供的数据接口满足稽核、审计及技术监控的需要。	是□ 否□ 不适用□	
4.1.3.	集中交易系统的功能设计与技术实现是否禁止对违规业务功能的设计与实现。	a)访谈集中交易系统业务管理部门，确认所支持的全部业务合规，新开发的业务模块均经过业务部门和内部控制部门的审批流程，已过时的业务模块也经内部审批后进行了及时清理； b)在技术人员协助下，对当前系统的所有功能模块进行审查。	是□ 否□ 不适用□	
4.1.4.	是否逐笔存储交易委托、银证转账等操作的客户交易终端信息。	a)检查设计文档或验收文档，查看是否采取适当技术，确保网上交易、语音交易、自助交易等外围信息系统、集中交易系统能够逐笔记录客户交易终端 IP 地址、IMEI、WIFI MAC 地址、电话号码等信息； b)检查网上交易、语音交易、自助交易等外围信息系统交易记录，以及集中交易系统交易记录，是否包含包括客户交易终端 IP 地址、IMEI、WIFI MAC 地址、电话号码等信息。	是□ 否□ 不适用□	
4.2.	**结构安全**			
4.2.1.	集中交易系统的重要环节是否采取冗余备份措施，如报盘系统、重要的数据库服务器和中间件服务器等。	检查集中交易系统设计文档和验收文档，并现场检查，确认报盘系统、重要的数据库服务器和中间件服务器等重要环节均有冗余备份措施。	是□ 否□ 不适用□	

表 G.2　集中交易系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
4.2.2.	集中交易系统是否保证系统的可扩展性与可维护性。	a)检查“表 0.4-系统处理能力-扩展系统处理能力所需时间（自然日）”，审阅系统架构图，确认集中交易系统具有平行扩展能力，并可在较短工作日内完成处理能力的扩展； b)检查系统扩展方案，评价系统的可扩展性和可维护性。	是□ 否□ 不适用□	
4.2.3.	是否按照99.99%可用性和7×24 小时连续性指标对集中交易系统进行整体设计。	a)检查“表 0.4-系统处理能力-本年度交易中断、严重缓慢的总时长（分钟）”，审阅系统设计方案并访谈技术开发人员，是否按照99.99%可用性和 7×24 小时连续性指标对集中交易系统进行整体设计； b)检查最近一年集中交易系统故障记录，确认系统最近一年的可用率是否达到99.99%。	是□ 否□ 不适用□	
4.2.4.	系统最大处理能力是否达到日常实际处理量的 5 倍以上	检查“表 0.4-系统处理能力”，测算压力测试峰值每秒最大委托处理笔数与历史峰值交易日峰值每秒处理笔数的比值，确定结果大于 5。	是□ 否□ 不适用□	
4.3.	**外包软件开发**			
4.3.1.	由证券公司组织定制开发的集中交易系统，是否要求开发商提供源代码或对源代码实行第三方托管。	a)检查“表 0.4-集中交易软件情况-源代码保存机制”、源代码所有权、开发方式相关文件（如供应商服务合同），查看由证券公司组织定制开发的集中交易系统，是否要求开发商提供源代码或对源代码实行第三方托管； b)访谈系统建设负责人，是否要求开发单位提供源代码，或对源代码实行第三方托管。	是□ 否□ 不适用□	
4.4.	**测试验收**			
4.4.1.	是否配备独立的测试系统，并与交易所测试系统联网，实现完整的交易测试环境。	a)检查集中交易系统测试环境系统架构图和网络拓扑图，确认在测试环境下部署了集中交易系统并与交易所测试环境联网； b)现场检查测试系统与交易所测试系统联网，能实现完整的交易测试。	是□ 否□ 不适用□	
4.4.2.	测试验收	检查集中交易系统测试环境系统架构图和网络拓扑图，确认测试系统与主用系统的技术架构相同，与主用系统在通讯、主机及操控系统方面物理隔离。	是□ 否□ 不适用□	

表 G.2　集中交易系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
4.5.	**系统监控**			
4.5.1.	集中交易系统是否提供系统运行状态监控模块。	a)检查“表 0.4-系统监控情况”和系统设计文档，确认系统具有运行状态监控模块； b)现场观察监控模块运行正常，并能对业务处理量、CPU 利用率、内存使用率等关键指标进行监控。	是□ 否□ 不适用□	
4.6.	**岗位管理**			
4.6.1.	对各重要岗位的人员上岗是否有相应的资质要求和必要的上岗培训，对重要岗位人员建立轮岗制度和定期培训制度。	a)检查录用管理文档，是否具有人员录用时对录用人身份、背景和专业资格等进行审查的相关文档或记录，查看是否记录审查内容和审查结果等； b)检查岗位培训记录，查看考核人员是否包括各个重要岗位的人员，考核内容是否包含岗位知识和技能等；检查相关重要岗位的岗位知识和技能培训是否定期进行； c)检查岗位轮岗制度及轮岗记录，是否建立了重要岗位的轮岗制度。	是□ 否□ 不适用□	
4.7.	**身份鉴别**			
4.7.1.	集中交易系统是否能防止强力试探口令，并具有超时自动锁定功能。	a)检查对多个连续号码账户使用同一口令、一个账户试探不同口令登录采取了防护措施； b)检查账户登陆后具有超时锁定功能。	是□ 否□ 不适用□	
4.8.	**访问控制**			
4.8.1.	是否在权限体系中支持前台业务操作、中台业务管理与后台业务支持的分离。	访谈系统管理员，检查权限分配表，是否实现前台业务操作、中台业务管理与后台业务支持的分离。	是□ 否□ 不适用□	
4.9.	**备份能力**			
4.9.1.	本地集中交易系统的备份系统是否有足够的处理能力，确保届时能完全承担交易、清算及交收业务。	检查“表0.4-备份系统处理能力”，审阅灾备演练时的系统日志记录，确认本地集中交易系统的备份系统是否有足够的处理能力，确保届时能完全承担交易、清算及交收业务。	是□ 否□ 不适用□	
4.9.2.	同城灾难备份中心的交易系统是否有足够的处理能力，确保届时能完全承担交易、清算及交收业务。	a)检查“表0.4-备份系统处理能力”，审阅资源数据中灾难应对能力的系统备份能力等级，确认灾备交易系统的处理能力； b)审阅灾备演练时的系统日志记录，确认灾备系统具有足够的处理能力。	是□ 否□ 不适用□	

表 G.2　集中交易系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
4.9.3.	异地灾难备份中心的交易系统是否有足够的处理能力，确保届时能完全承担交易、清算及交收业务。	a)检查“表 0.4-备份系统处理能力”，审阅资源数据中灾难应对能力的系统备份能力等级，确认灾备交易系统的处理能力； b)审阅灾备演练时的系统日志记录，确认灾备系统具有足够的处理能力。	是□ 否□ 不适用□	
4.10.	**网络通信**			
4.10.1.	集中交易系统与上海证券交易所的通信连接是否做到地面线路和卫星通信相互备份。	a)检查“表 0.4-卫星通信情况”、“表 0.4-地面通信情况-与上交所和上证通地面专线连接情况通信情况”，检查网络设计或验收文档，查看是否具有备份线路； b)查看网络拓扑图，检查与上海证券交易所的通信连接情况。	是□ 否□ 不适用□	
4.10.2.	集中交易系统与深圳证券交易所的通信连接是否做到地面线路和卫星通信相互备份。	a)检查“表 0.4-卫星通信情况”、“表 0.4-地面通信情况-与深交所和深证通的地面专线连接情况”，检查网络设计或验收文档，查看是否具有备份线路； b)查看网络拓扑图，检查与深圳证券交易所的通信连接情况。	是□ 否□ 不适用□	
4.10.3.	集中交易系统与中国证券登记结算公司的通信连接是否有备份线路。	a)检查网络设计或验收文档，查看是否具有备份线路； b)查看网络拓扑图，检查与中国证券登记结算公司的通信连接情况。	是□ 否□ 不适用□	
4.10.4.	同城灾难备份中心与中心机房之间的通信连接除主用线路外、是否有备用线路；	检查“表 0.4-地面通信情况-内部通信情况-总部主备机房之间地面专线连接情况”、网络设计或验收文档，判断同城灾难备份中心与中心机房之间的通信连接除主用线路外、是否有备用线路。	是□ 否□ 不适用□	
4.11.	**系统托管**			
4.11.1	二级系统托管是否满足《证券期货业信息系统托管基本要求》（JR/T 0133-2015)的相关要求。	检查托管服务合同和相关文档，确认按照信息安全等级保护二级要求进行定级的系统选购了二级系统托管服务。	是□ 否□ 不适用□	
4.11.2	三级系统托管是否满足《证券期货业信息系统托管基本要求》（JR/T 0133-2015)的相关要求。	检查托管服务合同和相关文档，确认按照信息安全等级保护三级要求进行定级的系统选购了三级系统托管服务。	是□ 否□ 不适用□	
4.11.3	未定级系统托管是否满足《证券期货业信息系统托管基本要求》（JR/T 0133-2015)的相关要求。	检查托管服务合同和相关文档，确认未进行信息安全等级保护定级备案的信息系统选购了二级系统托管服务。	是□ 否□ 不适用□	

附 录 H
（规范性附录）
网上信息系统审计底稿

表H.1至表H.2给出了网上信息系统审计的程序、内容及相关记录要求。

表H.1 网上信息系统审计底稿

被审计部门：	索引号：WSXXXT
审计主题：网上信息系统	审计年度：
审计结论、意见及建议： 编制人： 年 月 日 （部门盖章）	
复核意见： 复核人： 年 月 日 （部门盖章）	
被审计部门意见： 年 月 日 （部门盖章）	

表 H.1　网上信息系统审计底稿（续）

审计证据列表：

表H.2　网上信息系统审计底稿

序号	审计项	审计程序	审计结论	备注
1	主机管理			
1.1.	身份鉴别			
1.1.1.	操作系统管理员口令是否符合以下条件：数字、字母、符号混排，无规律的方式。	检查口令管理制度，是否规定口令符合以下条件：数字、字母、符号混排，无规律的方式。	是□ 否□ 不适用□	
1.1.2.	操作系统管理员口令的长度是否为12位。	检查口令管理制度，是否规定管理员用户口令的长度至少为12位。	是□ 否□ 不适用□	
1.1.3.	操作系统管理员口令是否每季度更换1次，更新的口令至少5次内不能重复。	检查口令管理制度，是否规定管理员用户口令至少每季度更换1次，更新的口令至少5次内不能重复。	是□ 否□ 不适用□	
1.1.4.	如果受限于操作系统，使得管理员口令长度不支持12位或其他复杂度要求，口令是否使用所支持的最长长度并适当缩小更换周期；也可以使用动态密码卡等一次性口令认证方式。	检查口令管理制度，是否规定如果设备口令长度不支持12位或其他复杂度要求，口令应使用所支持的最长长度并适当缩小更换周期，也可以使用动态密码卡等一次性口令认证方式。	是□ 否□ 不适用□	
1.1.5.	是否启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施。	a)检查重要服务器操作系统的身份鉴别策略，查看是否配置了登录失败处理功能、设置了非法登录次数的限制值； b)查看是否设置网络登录连接超时，并自动退出。	是□ 否□ 不适用□	
1.1.6.	当对服务器进行远程管理时，是否采取必要措施，防止鉴别信息在网络传输过程中被窃听。	查看“表0.13附表一-信息系统名称”、“表0.13附表一-本系统中密码机使用情况”，访谈系统管理员，询问是否对操作系统采用了远程管理方式，如果采用远程管理方式，查看是否具有防止鉴别信息在网络传输过程中被窃听的措施。	是□ 否□ 不适用□	
1.1.7.	是否为操作系统的不同用户分配不同的用户名，确保用户名具有唯一性。	检查操作系统的用户列表，标识是否唯一，或采取堡垒机等措施。	是□ 否□ 不适用□	
1.1.8.	通过本地控制台管理主机设备时，是否采用一种或一种以上身份鉴别技术。	查看安全策略文档，检查本地控制台管理主机设备是否采用一种或一种以上身份鉴别技术。	是□ 否□ 不适用□	
1.1.9.	以远程方式登录主机设备，是否采用两种或两种以上组合的鉴别技术进行身份鉴别。	查看安全策略文档，检查远程方式登录主机设备是否采用两种或两种以上组合的鉴别技术进行身份鉴别。	是□ 否□ 不适用□	

表 H.2　网上信息系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
1.2.	**访问控制**			
1.2.1.	是否启用访问控制功能，依据安全策略控制用户对资源的访问。	检查重要服务器操作系统的访问控制策略，查看是否对重要文件的访问权限进行了限制，对系统不需要的服务、共享路径等进行了禁用或删除。	是□ 否□ 不适用□	
1.2.2.	是否实现操作系统和数据库系统特权用户的权限分离；HP Tandem、IBM OS400系列、运行DB2数据库的IBM AIX等专用系统的特权用户除外。	如果系统支持操作系统和数据库系统特权用户的权限分离，应检查重要数据库管理系统的特权用户和重要操作系统的特权用户，查看不同管理员的系统账户权限是否不同，且不应由同一人担任。	是□ 否□ 不适用□	
1.2.3.	是否严格限制默认账户的访问权限，重命名系统默认账户，修改这些账户的默认口令。a)系统无法修改访问权限的特殊默认账户，可不修改访问权限；b)系统无法重命名的特殊默认账户，可不重命名。	检查重要服务器操作系统的访问控制策略，查看是否已禁用或者限制匿名/默认帐户的访问权限，是否重命名系统默认帐户、修改这些帐户的默认口令。	是□ 否□ 不适用□	
1.2.4.	是否及时删除多余的、过期的账户，避免共享账户的存在。	a)检查系统中的账号是否为用户工作必须的； b)检查是否及时删除了多余的、过期的账户	是□ 否□ 不适用□	
1.2.5.	是否根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限。	如果系统支持操作系统和数据库系统特权用户的权限分离，应检查主要服务器操作系统和主要数据库管理系统的访问控制策略，查看特权用户的权限是否进行分离，如可分为系统管理员、安全管理员、安全审计员等；查看是否采用最小授权原则。	是□ 否□ 不适用□	
1.3.	**安全审计**			
1.3.1.	服务器主机的审计内容是否包括：用户的添加和删除、审计功能的启动和关闭、审计策略的调整、权限变更、系统资源的异常使用、重要的系统操作（如用户登录、退出）等。	检查审计内容是否至少包括：用户的添加和删除、审计功能的启动和关闭、审计策略的调整、权限的变更、系统资源的异常使用、重要的系统操作（如用户登录、退出）等。	是□ 否□ 不适用□	

表 H.2　网上信息系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
1.3.2.	服务器主机的审计记录是否包括事件的日期、时间、类型、主体标识、客体标识和结果等。	检查主要服务器操作系统、重要终端操作系统的安全审计策略，查看审计记录信息是否包括事件发生的日期与时间、触发事件的主体与客体、事件的类型、事件成功或失败、事件的结果等内容。	是□ 否□ 不适用□	
1.3.3.	是否保护审计记录，避免受到未预期的删除、修改或覆盖等。审计记录是否至少保存6个月。	a)检查主要服务器操作系统、重要终端操作系统的安全审计策略，查看是否通过日志覆盖周期、存储方式、日志文件/空间大小、日志文件操作权限等设置，实现了对审计记录的保护，使其避免受到未预期的删除、修改或覆盖等； b)检查审计记录是否至少保存6个月。	是□ 否□ 不适用□	
1.3.4.	服务器主机的审计范围是否覆盖到服务器和重要客户端上的每个操作系统用户；应在保证系统运行安全和效率的前提下，启用系统审计或采用第三方安全审计产品实现审计要求。	a)检查主要服务器操作系统、重要终端操作系统和主要数据库管理系统的安全审计策略，查看安全审计配置是否包括系统内重要用户行为、系统资源的异常和重要系统命令的使用等重要的安全相关事件； b)检查是否在确保系统运行安全和效率的前提下，启用系统审计或采用第三方安全审计产品实现审计要求。	是□ 否□ 不适用□	
1.3.5.	是否能够根据记录数据进行分析，并生成审计报表。	检查主要服务器操作系统、重要终端操作系统和主要数据库管理系统的安全审计策略，查看是否为授权用户提供浏览和分析审计记录的功能，是否可以根据需要自动生成不同格式的审计报表。	是□ 否□ 不适用□	
1.4.	**安全管理**			
1.4.1.	操作系统是否遵循最小安装的原则，仅安装需要的组件和应用程序，并通过设置升级服务器等方式保持系统补丁及时得到更新。持续跟踪厂商提供的系统升级更新情况，是否在经过充分的测试评估后对必要的系统补丁进行及时更新。	a)检查主要服务器操作系统中所安装的系统组件和应用程序是否都是必须的； b)检查是否设置了专门的升级服务器实现对主要服务器操作系统补丁的升级，主要服务器操作系统是否具有操作系统补丁更新策略； c)检查是否持续跟踪厂商提供的系统升级更新情况，对关键性补丁是否进行充分的评估测试，并记录了相关评估情况和升级过程。	是□ 否□ 不适用□	

表 H.2　网上信息系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
1.4.2.	是否能够检测到对重要服务器进行入侵的行为，能够记录入侵的源IP、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警；针对重要服务器的入侵行为检测是否通过网络级或主机级入侵检测系统等方式实现。	a)查看“表0.3-该机房的攻击防护措施”，检查入侵防范系统的入侵防范策略，查看是否能够记录对主要服务器攻击的源IP、攻击类型、攻击目标、攻击时间等，在发生严重入侵事件时是否提供报警（如声音、短信和EMAIL等）；应当同时检查入侵防范系统的特征库是否保持最新状态； b)渗透测试主要服务器操作系统和主要数据库管理系统，查看入侵防范系统是否及时正确记录了本次攻击行为，并自动报警。	是□ 否□ 不适用□	
1.4.3.	是否能够对重要程序的完整性进行检测，并在检测到完整性受到破坏后具有恢复的措施。如不能正常恢复，是否停止有关服务，并提供报警。	检查主要服务器完整性保护情况说明，确认提供对重要程序的完整性进行检测，并在检测到完整性受到破坏后具有恢复的措施的功能。	是□ 否□ 不适用□	
1.4.4.	是否对所有服务器和终端设备安装防木马、病毒等防恶意代码软件，定期进行全面检查，并及时更新防恶意代码软件版本和恶意代码库。a)原则上所有主机应安装防恶意代码软件，系统不支持该要求的除外;b) 未安装防恶意代码软件的主机，应采取有效措施进行恶意代码防范。	查看“表N03-该机房的病毒木马防护软件情况”，检查关键服务器的恶意代码防范策略，对支持安装防恶意代码软件的主机操作系统，查看是否安装了实时检测与查杀恶意代码的软件产品，并且及时更新了软件版本和恶意代码库。	是□ 否□ 不适用□	
1.4.5.	是否支持防恶意代码软件的统一管理。	a)访谈安全管理员，询问防恶意代码软件是否由专人负责进行管理和维护； b)检查主机防恶意代码软件维护记录，确认防恶意代码软件由专人统一管理。	是□ 否□ 不适用□	
1.4.6.	主机防恶意代码产品是否具有与网络防恶意代码产品不同的恶意代码库。	检查主机防恶意代码软件或硬件，查看其厂家名称、产品版本号和恶意代码库名称等，查看其是否与网络防恶意代码软件有不同的恶意代码库。	是□ 否□ 不适用□	

表 H.2　网上信息系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
1.4.7.	是否提高所有用户的防病毒意识，告知及时升级防病毒软件，在读取移动存储设备上的数据以及网络上接收文件或邮件之前，先进行病毒检查，对外来计算机或存储设备接入网络系统之前也应进行病毒检查。	访谈系统运维负责人，询问是否对员工进行基本恶意代码防范意识的教育，是否告知应及时升级软件版本，使用外来设备、网络上接收文件和外来计算机或存储设备接入网络系统之前进行病毒检查等。	是□ 否□ 不适用□	
1.4.8.	是否定期检查主机防病毒产品的恶意代码库的升级情况并进行记录，对截获的危险病毒或恶意代码进行及时分析处理，并形成书面的报表和总结汇报。	a)询问安全管理员，主机防病毒产品的恶意代码库的升级机制； b)检查恶意代码库的升级记录，判断是否定期； c)检查恶意代码分析报告，确认对主机防病毒产品上截获的危险病毒或恶意代码进行了及时分析处理。	是□ 否□ 不适用□	
1.4.9.	是否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。	a)查看病毒扫描记录，判断是否定期对服务器进行全面病毒扫描； b)检查病毒扫描时间，确认未在交易时段内进行。	是□ 否□ 不适用□	
1.5.	**资源控制**			
1.5.1.	是否通过设定终端接入方式、网络地址范围等条件限制终端登录。	检查主要服务器操作系统的资源控制策略，查看是否设定了终端接入方式、网络地址范围等条件限制终端登录。	是□ 否□ 不适用□	
1.5.2.	是否根据安全策略设置登录终端的操作超时锁定。	a)访谈运维负责人，询问是否存在登录终端的操作超时锁定的安全策略； b)现场测试安全策略的有效性。	是□ 否□ 不适用□	
1.5.3.	是否限制单个用户对系统资源的最大或最小使用限度。	检查主要服务器操作系统和主要数据库管理系统的资源控制策略，查看是否设置了单个用户或应用对系统资源的最大或最小使用限度。	是□ 否□ 不适用□	
1.6.	**主机运维**			
1.6.1.	是否对重要服务器进行监视，包括监视服务器的CPU、硬盘、内存、网络等资源的使用情况。	查看“表0.7附表-该机房的网上信息系统监控情况”，检查主要服务器操作系统的资源控制策略，查看是否对CPU、硬盘、内存和网络等资源的使用情况进行监控。	是□ 否□ 不适用□	
1.6.2.	重要服务器的CPU利用率、内存、磁盘存储空间等指标超过预先规定的阈值后是否实时进行报警。	检查重要服务器监控系统的日志记录，CPU利用率、内存、磁盘存储空间等指标超过预先规定的阈值后是否实时进行报警。	是□ 否□ 不适用□	

表 H.2　网上信息系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
1.6.3.	是否对操作系统的参数配置、调优，编制文档并保持更新。	a)访谈系统管理员，询问是否知悉其职责范围； b)检查维护记录，确认及时维修、更换故障设备和更新软件，关闭了与业务无关的服务，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； c)检查参数配置文档，确认及时对应用系统、操作系统的参数进行了配置、调优； d)检查系统容量评估报告，确认定期对系统容量进行了检查和评估。	是□ 否□ 不适用□	
2.	**系统管理**			
2.1.	**系统架构**			
2.1.1.	是否为证券交易所或登记结算机构采集客户交易终端信息提供相应的数据接口，并符合国家信息安全标准。	检查客户交易终端信息数据采集接口功能设计和验收文档，确认为证券交易所或登记结算机构采集客户交易终端信息提供相应的数据接口。	是□ 否□ 不适用□	
2.1.2.	是否提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的数据格式或长度符合系统设定要求。	a)检查设计或验收文档，查看是否有对人机接口输入或通信接口输入的数据进行有效性检验； b)测试主要应用系统，查看应用系统是否能明确拒绝不符合格式要求数据。	是□ 否□ 不适用□	
2.1.3.	是否提供自动保护功能，当故障发生时自动保护当前所有状态，保证系统能够进行恢复。	a)检查设计或验收文档，查看是否在故障发生时自动保护当前所有状态保证系统能够进行恢复的描述； b)测试主要应用系统，验证是否提供自动保护功能，当故障发生时自动保护当前所有状态，保证系统能够进行恢复。	是□ 否□ 不适用□	
2.2.	**系统建设**			
2.2.1.	在开展信息系统新建、升级、变更、换代等建设项目时，是否进行充分论证和测试，论证材料包括需求分析、立项报告等。	a)访谈信息技术负责人，询问是否在开展信息系统新建、升级、变更、换代等建设项目时，进行充分论证和测试，以及确保落实的机制； b)检查是否具有相关测试报告、论证材料（包括需求分析、立项报告等）。	是□ 否□ 不适用□	

表 H.2　网上信息系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.2.2.	是否制定详细的工程实施方案控制实施过程，并要求工程实施单位能正式地执行安全工程过程。	a)检查系统建设方面的管理制度，查看其是否包括工程实施过程的控制方法、实施参与人员的行为准则等方面内容； b)检查工程实施方案，查看其是否包括工程时间限制、进度控制和质量控制等方面内容，是否按照工程实施方面的管理制度进行各类控制、产生阶段性文档等。	是□ 否□ 不适用□	
2.2.3.	是否向用户提供系统建设文档和运行维护所需文档。	检查系统交付提交的文档，查看是否有指导用户进行系统运维的文档等，提交的文档是否符合管理规定的要求。	是□ 否□ 不适用□	
2.2.4.	是否书面规定系统交付的控制方法和人员行为准则。	检查系统建设方面的管理制度，查看其是否包括系统交付的控制方法和人员行为准则的规定。	是□ 否□ 不适用□	
2.2.5.	是否指定专门部门管理系统交付，并按照要求完成交付工作。	访谈系统建设负责人，询问是否有专门的部门负责系统交接工作，系统交接工作是否根据交付清单对所交接的设备、文档、软件等进行清点。	是□ 否□ 不适用□	
2.2.6.	是否建立交付流程，对建成的信息系统交付运行维护的活动进行规范。	检查交付管理制度，查看交付流程是否对建成的信息系统交付运行维护的活动进行规范。	是□ 否□ 不适用□	
2.2.7.	是否制定交付工作清单，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。	检查是否具有系统交付清单，查看交付清单是否说明系统交付的各类设备、软件、文档等。	是□ 否□ 不适用□	
2.2.8.	是否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。	a)访谈系统建设负责人，询问系统正式运行前是否对运行维护人员进行过培训，针对哪些方面进行过培训； b)检查是否有系统交付技术培训记录，查看是否包括培训内容、培训时间和参与人员等。	是□ 否□ 不适用□	
2.2.9.	是否制定交付实施计划，划定交付双方的职责，交付的步骤，并对交付过程留存记录。	检查是否具有交付实施计划，查看交付实施计划是否划定交付双方的职责，交付的步骤，并对交付过程留存记录。	是□ 否□ 不适用□	
2.2.10.	是否制定信息系统备份能力建设工作计划。	检查信息技术部门是否编制了信息系统备份能力建设工作计划。	是□ 否□ 不适用□	

表 H.2　网上信息系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.3.	**测试验收**			
2.3.1.	是否建立完整、规范的系统测试操作流程，对测试工作的计划、实施及总结做出详细的规定。对于在生产系统上进行的测试工作，必须制定详细的系统及数据备份、测试环境搭建、测试后系统及数据恢复、生产系统审核等计划，确保生产系统的安全。	检查系统测试操作流程，是否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。	是□ 否□ 不适用□	
2.3.2.	测试验收前是否根据设计方案或合同要求等制订测试验收方案，在测试验收过程中详细记录测试验收结果，并形成测试验收报告。	a)访谈系统建设负责人，询问是否根据设计方案或合同要求组织相关部门和人员制定工程测试验收方案，并对系统测试验收报告进行审定； b)检查是否具有工程测试验收方案，查看其是否明确说明参与测试的部门、人员、测试验收内容、现场操作过程等内容，过程控制是否符合管理规定的要求.	是□ 否□ 不适用□	
2.3.3.	是否组织相关部门和相关人员对系统测试验收报告进行审定，并签字确认。	检查是否具有系统测试验收报告，是否有相关部门和人员对系统测试验收报告进行审定的意见。	是□ 否□ 不适用□	
2.3.4.	是否委托第三方测试单位测试系统安全性，并出具安全性测试报告。	检查是否具有系统测试验收报告，是否有第三方测试机构的签字或盖章。	是□ 否□ 不适用□	
2.3.5.	是否书面规定系统测试验收的控制方法和人员行为准则。	检查系统建设方面的管理制度，查看其是否包括对系统测试验收的控制方法和人员行为准则规定。	是□ 否□ 不适用□	
2.3.6.	是否指定或授权专门的部门负责系统测试验收的管理，并按照管理规定的要求完成系统测试验收工作。	访谈系统建设负责人，询问是否有专门的部门负责测试验收工作，由何部门负责；是否委托第三方测试机构对信息系统进行独立的安全性测试。	是□ 否□ 不适用□	
2.3.7.	是否为系统测试配备必要的人员和设备资源，需要时协调关联单位配合测试。	访谈开发负责人，询问是否为系统测试配备必要的人员和设备资源，需要时协调关联单位配合测试。	是□ 否□ 不适用□	
2.3.8.	是否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覆盖功能、性能、容量、安全性、稳定性等方面。测试完成后对测试结果进行分析评估，并给出测试报告。	a)访谈开发负责人，询问是否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； b)检查是否具有测试方案，是否包括覆盖功能、性能、容量、安全性、稳定性等方面； c)检查近期上线系统的测试报告。	是□ 否□ 不适用□	

表 H.2　网上信息系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.3.9.	是否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。模拟环境是否与生产环境进行有效隔离，不得对生产环境进行干扰。	检查“表 0.3-网络边界防护情况-交易业务网与模拟环境测试网络”，检查系统模拟环境逻辑架构，查看系统模拟环境在逻辑架构上是否与生产环境一致，是否与生产环境有效隔离。	是□ 否□ 不适用□	
2.3.10.	是否根据测试方案的设计，合理配置模拟环境测试所需的设备，识别设备不同可能带来的测试结果正确性风险。	a)访谈开发负责人，询问是否根据测试方案的设计，合理配置模拟环境测试所需的设备，识别设备不同可能带来的测试结果正确性风险； b)检查系统测试方案、测试报告，查看是否有设备不同可能带来的测试结果正确性风险的说明。	是□ 否□ 不适用□	
2.3.11.	是否根据需要，要求生产系统运维人员和业务部门组织业务人员参与模拟环境测试。	a)访谈开发负责人，询问是否根据需要，要求生产系统运维人员和业务部门组织业务人员参与模拟环境测试； b)查看测试通知或记录，是否有生产系统运维人员和业务部门组织业务人员参与。	是□ 否□ 不适用□	
2.3.12.	模拟环境使用的密码是否与生产系统严格区分，系统管理员宜由不同的人员担任。	访谈开发负责人，询问模拟环境使用的密码是否与生产系统严格区分，系统管理员由不同的人员担任。	是□ 否□ 不适用□	
2.3.13.	生产环境测试前是否备份当前系统的数据和配置。	a)检查系统测试管理制度和操作流程，查看数据和配置备份要求； b)抽查在生产系统上进行测试的工作记录，检查是否做好数据备份。	是□ 否□ 不适用□	
2.3.14.	是否提前发布生产环境测试的系统测试公告。	a)访谈开发负责人，询问是否提前发布生产环境测试系统测试公告； b)查看一次使用生产环境测试的测试公告。	是□ 否□ 不适用□	
2.3.15.	是否由生产系统运维人员在生产环境下组织完成生产环境测试。	a)访谈开发负责人，询问是否由生产系统运维人员在生产环境下组织完成生产环境测试； b)查看一次生产环境测试的测试方案、测试记录，是否由生产系统运维人员在生产环境下组织完成生产环境测试。	是□ 否□ 不适用□	

表 H.2　网上信息系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.3.16.	是否根据需要，要求业务部门组织业务人员参与生产环境测试。	a)访谈开发负责人，询问是否根据需要，要求业务部门组织业务人员参与生产环境测试； b)查看一次生产环境测试的测试方案、测试记录，是否根据需要，要求业务部门组织业务人员参与生产环境测试。	是□ 否□ 不适用□	
2.3.17.	是否根据生产环境测试的结果设计系统升级过程及应急预案。	a)访谈开发负责人，询问是否根据生产环境测试的结果设计系统升级过程及应急预案； b)抽查一次生产环境测试报告和系统变更方案。	是□ 否□ 不适用□	
2.3.18.	如果生产环境测试内容涉及其他相关系统，是否协调其他系统用户参与测试。	a)访谈开发负责人，询问如果生产环境测试内容涉及其他相关系统，是否协调其他系统用户参与测试； b)抽查测试方案、测试记录，是否体现其他系统用户。	是□ 否□ 不适用□	
2.3.19.	涉及核心交易业务系统的上线测试，是否组织全市场或全公司各相关部门测试。	a)访谈开发负责人，询问涉及核心交易业务系统的上线测试，是否组织全市场或全公司各相关部门测试； b)抽查核心系统上线测试方案、测试记录，是否体现参测机构及部门。	是□ 否□ 不适用□	
2.3.20.	测试后是否恢复生产环境并验证恢复的有效性。	a)访谈开发负责人，询问测试后是否恢复生产环境并验证恢复的有效性； b)抽查测试方案、恢复验证记录。	是□ 否□ 不适用□	
2.3.21.	是否禁止交易时段使用生产环境进行测试。	a)访谈开发负责人，询问是否交易时段不得使用生产环境进行测试； b)抽查测试方案、测试记录、测试报告，查看是否在交易时段测试。	是□ 否□ 不适用□	
2.3.22.	是否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。	查看测试记录，是否在设备和软件投入使用前进行必要的验证性测试。	是□ 否□ 不适用□	

表 H.2　网上信息系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.4.	**系统运维**			
2.4.1.	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。	a)检查运维管理制度，是否包括机房管理、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； b)检查运维操作流程，是否包括日常操作、事件处理、问题处理、系统变更、应急处置等。	是□ 否□ 不适用□	
2.4.2.	交易业务系统的操作规程是否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。	检查交易业务系统的操作规程，是否包括操作的对象、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。	是□ 否□ 不适用□	
2.4.3.	是否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进行记录留痕，记录的保存时间不少于一年。	检查一年内对交易业务系统的操作记录，是否严格按照操作手册执行运维操作。	是□ 否□ 不适用□	
2.4.4.	特殊操作、临时操作是否经批准后方可双岗执行。操作过程是否进行记录留痕，记录的保存时间是否不少于一年。	抽查公司一年内特殊操作和临时操作的记录，检查相关操作是否经过审批，是否有操作人员和复核人员签名确认。	是□ 否□ 不适用□	
2.4.5.	是否依据业务、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。	抽查修订记录，确认业务或信息系统发生重大变更时，是否对相关系统操作手册及规程进行修订并经过审批。	是□ 否□ 不适用□	
2.4.6.	是否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，是否开启自动监控系统和自动报警系统。	a)访谈运维负责人，询问是否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； b)检查巡检记录，是否包括报单数、成交数、委托数、CPU 使用率、内存使用率等指标。	是□ 否□ 不适用□	
2.4.7.	是否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。	a)访谈运维负责人，询问是否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； b)检查定期检查、评估的记录或报告，确定是否设定了预警阈值。	是□ 否□ 不适用□	

表 H.2　网上信息系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.4.8.	主机监控指标是否包括：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。	a)检查“表 0.4-系统监控情况”，检查系统设计和验收文档，服务器监控指标是否包括设备运行状态、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； b)现场检查主机监控情况。	是□ 否□ 不适用□	
2.4.9.	存储监控指标是否包括：设备运行状态、数据交换延时、存储电池状态等。	a)检查“表 0.4-系统监控情况”，检查系统设计和验收文档，存储监控指标是否包括设备运行状态、数据交换延时、存储电池状态等； b)现场检查存储监控情况。	是□ 否□ 不适用□	
2.4.10.	数据库监控指标是否包括日志信息、表空间使用率、连接数等。	a)检查“表 0.4-系统监控情况”，检查系统设计和验收文档，数据库监控指标是否包括日志信息、表空间使用率、连接数等； b)现场检查数据库监控情况。	是□ 否□ 不适用□	
2.4.11.	核心交易业务相关的应用系统监控指标是否包括进程的活动状态、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。	a)检查“表 0.4-系统监控情况”，检查系统设计和验收文档，检查相关的应用系统监控指标，是否包括进程的活动状态、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； b)现场检查应用系统监控情况。	是□ 否□ 不适用□	
2.4.12.	是否针对不同系统设置合理的监测频度。	a)访谈运维负责人，询问是否针对不同系统设置合理的监测频度； b)查阅相关系统设置文档，是否有监测频度的说明； c)根据监测频度说明，检查相关参数设置情况。	是□ 否□ 不适用□	
2.4.13.	持续跟踪厂商提供的系统升级更新情况，是否在经过充分的测试评估后对必要的补丁进行及时更新，并在安装系统补丁前对现有的重要文件进行备份。	a)访谈系统管理员，了解系统补丁更新程序和评估方法； b)查看系统补丁更新记录，确认持续跟踪厂商提供的系统升级更新情况，确认在对重要文件进行备份后，才实施系统补丁程序的安装。	是□ 否□ 不适用□	

表 H.2　网上信息系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.4.14.	是否依据操作手册对系统进行维护，详细记录操作日志，包括重要的日常操作、运行维护记录、参数的设置和修改等内容，严禁进行未经授权的操作。	a)访谈信息技术部门负责人和操作人员，了解对系统进行维护审批和操作步骤； b)检查运维操作手册和操作日志，确认是否包括重要的日常操作、运行维护记录、参数的设置和修改等内容，确认按照授权进行操作。	是□ 否□ 不适用□	
2.4.15.	是否保持系统的可用性，及时维修、更换故障设备和更新软件。	检查运维操作手册,是否包括保持系统的可用性，及时维修、更换故障设备和更新软件。	是□ 否□ 不适用□	
2.4.16.	是否负责应用系统的参数配置、调优，编制文档并保持更新。	检查运维操作手册,是否包括对应用系统、操作系统的参数进行配置、调优，编制文档并保持更新。	是□ 否□ 不适用□	
2.4.17.	是否定期对系统容量进行检查和评估，形成评估报告。	检查系统容量评估报告，是否定期对系统容量进行检查和评估。	是□ 否□ 不适用□	
2.4.18.	是否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。	检查运维操作手册,是否包括管理系统和应用程序服务进程，并关闭与业务无关的服务。	是□ 否□ 不适用□	
2.4.19.	是否对新上线的设备在接入运行网络前进行全面的安全检查。	a)访谈安全管理员，了解设备上线前的安全检查流程； b)查看设备上线前的漏洞扫描、渗透测试、病毒扫描、木马检测等扫描报告。	是□ 否□ 不适用□	
2.5.	**变更管理**			
2.5.1.	是否确认系统中要发生的变更，并制定相应的变更方案；重要系统变更前是否制定详细的变更方案、失败恢复方案、专项应急预案。	a)访谈系统运维负责人，询问系统变更机制或流程，是否针对系统的重大变更制定变更方案、失败恢复方案、专项应急预案； b)现场检查变更方案，抽查重要系统变更是否制定详细的变更方案、失败恢复方案、专项应急预案。	是□ 否□ 不适用□	
2.5.2.	是否建立变更控制的申报和审批文件化程序，对变更影响进行分析并文档化,记录变更实施过程，并妥善保存所有文档和记录。	检查是否有变更管理制度，查看其是否覆盖变更前审批、变更过程记录、变更后通报等方面内容，是否包括变更申报、审批程序，是否规定需要申报的变更类型、申报流程、审批部门、批准人等方面内容。	是□ 否□ 不适用□	

表 H.2　网上信息系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.5.3.	是否建立中止变更并从失败变更中恢复的文件化程序，明确过程控制方法和人员职责，必要时对恢复过程进行演练。	检查系统变更方案，查看其是否覆盖变更类型、变更原因、变更过程、变更前评估、变更失败恢复程序等方面内容，查看其是否有主管领导的批准签字。	是□ 否□ 不适用□	
2.5.4.	是否建立系统变更流程，对信息系统的变更活动进行规范。	检查变更管理流程。	是□ 否□ 不适用□	
2.5.5.	是否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。	检查系统变更记录，系统变更中的角色是否包括申请人、审批人、实施人、复核人。	是□ 否□ 不适用□	
2.5.6.	变更申请人是否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。	检查系统变更申请，申请中是否有明确的变更方案，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。	是□ 否□ 不适用□	
2.5.7.	变更审批人是否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。	a)检查变更风险评估报告，判断变更审批人是否充分评估变更的技术风险和业务风险； b)检查变更审批记录，是否审批记录留痕并满足审计需要。	是□ 否□ 不适用□	
2.5.8.	变更审批人是否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。	检查变更审批记录，变更审批人是否确定了变更实施时间窗口，做到了除紧急变更外，不得在交易时段进行变更实施。	是□ 否□ 不适用□	
2.5.9.	是否按照测试方案，组织变更前后的测试，测试后是否提交测试记录或报告。	检查变更测试记录或报告，是否按照测试方案，组织变更前后的测试。	是□ 否□ 不适用□	
2.5.10.	变更实施人是否按照变更实施方案进行变更，并及时更新配置库。	a)检查系统变更记录，变更实施人是否按照变更实施方案进行变更； b)检查系统配置库，是否变更后及时更新配置库。	是□ 否□ 不适用□	
2.5.11.	变更复核人是否对变更记录和变更结果进行评估，评估内容是否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。	检查变更复核记录，变更复核人是否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。	是□ 否□ 不适用□	

表 H.2　网上信息系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.6.	**安全管理**			
2.6.1.	是否建立至少每季度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。	a)访谈系统管理员，询问是否定期对系统进行漏洞扫描，扫描周期多长，发现漏洞是否及时修补，在安装系统补丁前是否对重要文件进行备份，是否先在测试环境中测试通过再安装； b)检查是否至少每季进行一次漏洞扫描，并对漏洞风险持续跟踪，在经过充分的验证测试后，对必要的漏洞开展修补工作。	是□ 否□ 不适用□	
2.7.	**身份鉴别**			
2.7.1.	是否提供专用的登录控制模块对登录用户进行身份标识和鉴别。	检查主要应用系统设计和验收文档，查看是否提供身份标识和鉴别功能。	是□ 否□ 不适用□	
2.7.2.	是否提供用户身份标识唯一和鉴别信息复杂度检查功能，保证应用系统中不存在重复用户身份标识，身份鉴别信息不易被冒用。	检查主要应用系统设计和验收文档，查看是否采用了措施保证身份标识具有唯一性，是否对登录用户的口令最小长度、复杂度和更换周期等进行了要求和限制，保证身份鉴别信息不易被冒用。	是□ 否□ 不适用□	
2.7.3.	是否提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施。	检查主要应用系统设计和验收文档，查看是否提供登录失败处理功能，是否根据安全策略设置了登录失败次数等参数。	是□ 否□ 不适用□	
2.7.4.	是否启用身份鉴别、用户身份标识唯一性检查、用户身份鉴别信息复杂度检查以及登录失败处理功能，并根据安全策略配置相关参数。	a)测试主要应用系统，可通过试图以合法和非法用户分别登录系统，验证身份标识和鉴别功能是否有效； b)测试主要应用系统，可通过多次输入错误的密码，验证登录失败处理功能是否有效； c)渗透测试主要应用系统，如多次猜测用户口令，验证应用系统身份标识和鉴别功能是否不存在明显的弱点。应当从互联网向被测试对象进行渗透测试。	是□ 否□ 不适用□	
2.7.5.	管理用户通过受控本地控制台管理应用系统时，是否采用一种或一种以上身份鉴别技术。	检查应用系统设计和验收文档，当管理用户通过受控本地控制台管理应用系统时，是否采用了一种或一种以上身份鉴别技术。	是□ 否□ 不适用□	

表 H.2　网上信息系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.7.6.	管理用户以远程方式登录应用系统，是否采用两种或两种以上组合的鉴别技术进行身份鉴别。	检查应用系统设计和验收文档，当管理用户以远程方式登录应用系统，是否采用了两种或两种以上组合的鉴别技术进行身份鉴别。	是□ 否□ 不适用□	
2.7.7.	面向互联网服务的系统是否提供两种或两种以上组合的鉴别技术供用户选择。	检查应用系统设计和验收文档，面向互联网服务的系统是否向用户提供两种或两种以上组合的鉴别技术供用户选择。	是□ 否□ 不适用□	
2.7.8.	是否禁止设置弱口令，若系统条件允许，口令是否采用数字、字母、符号混排且无规律的方式。	检查口令管理制度，是否规定口令应采用数字、字母、符号混排且无规律的方式。	是□ 否□ 不适用□	
2.7.9.	是否禁止设置弱口令，若系统条件允许，管理员口令长度原则上不低于 12 位。	检查口令管理制度，是否规定管理员用户口令的长度至少为 12 位。	是□ 否□ 不适用□	
2.7.10.	核心交易业务系统是否提示并阻止用户使用弱口令登录。	检查核心交易业务系统设计和验收文档，确定核心交易业务系统是否提示并阻止用户使用弱口令登录。	是□ 否□ 不适用□	
2.7.11.	是否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。	检查口令管理制度，是否规定管理员用户口令至少每季度更换 1 次，更新的口令至少 5 次内不能重复。	是□ 否□ 不适用□	
2.7.12.	应用系统的账户及口令是否采用加密方式存储、传输，加密产品的使用是否符合国家有关规定。	检查口令管理制度，是否规定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。	是□ 否□ 不适用□	
2.7.13.	是否重点加强对匿名/默认用户的管理，防止被非法使用。	a)检查账户列表，是否没有匿名/默认用户； b)若有匿名/默认用户，测试是否不能被非法使用。	是□ 否□ 不适用□	
2.7.14.	是否及时注销不再使用的账户。	检查在岗人员名单和账户列表，确定没有未注销的不再使用的账户。	是□ 否□ 不适用□	
2.7.15.	是否设置抵御连续猜测等对客户账户恶意攻击行为的策略。	a)检查连续猜测等对客户账户恶意攻击行为的策略； b)现场测试系统抵御连续猜测客户账户的攻击行为。	是□ 否□ 不适用□	

表 H.2　网上信息系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.8.	**访问控制**			
2.8.1.	是否提供访问控制和权限管理机制，依据安全策略控制用户对文件等客体的访问，防止客户的授权被恶意提升或转授，防止客户使用未经授权的功能，防止客户进行访问未经授权的数据等非法访问活动。	a)检查应用系统设计和验收文档，查看是否依据安全策略控制用户对文件等客体的访问； b)测试主要应用系统，可通过以不同权限的用户登录系统，查看其拥有的权限是否与系统赋予的权限一致，验证应用系统访问控制功能是否有效。	是□ 否□ 不适用□	
2.8.2.	访问控制的覆盖范围是否包括与资源访问相关的主体、客体及它们之间的操作。	检查应用系统设计和验收文档，查看其访问控制的覆盖范围是否包括与信息安全直接相关的主体、客体及它们之间的操作。	是□ 否□ 不适用□	
2.8.3.	是否由授权主体配置访问控制策略，并严格限制默认账户的访问权限。	a)检查应用系统设计和验收文档，查看其访问控制的覆盖范围是否包括与信息安全直接相关的主体、客体及它们之间的操作； b)测试主要应用系统，可通过以默认用户登录系统，并进行一些合法和非法操作，验证系统是否严格限制了默认帐户的访问权限。	是□ 否□ 不适用□	
2.8.4.	是否授予不同账户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系。	a)检查应用系统的用户角色或权限的分配情况，查看是否仅授予不同帐户为完成各自承担任务所需的最小权限，特权用户的权限是否分离，权限之间是否相互制约，如系统管理员不能进行审计操作、审计员不能进行系统管理操作等； b)渗透测试主要应用系统，进行试图绕过访问控制的操作，验证应用系统的访问控制功能是否不存在明显的弱点。	是□ 否□ 不适用□	
2.8.5.	是否根据业务需求和系统安全分析确定系统的访问控制策略。	a)访谈系统运维负责人，询问是否指定专门的部门或人员负责系统管理，如根据业务需求和系统安全分析制定系统的访问控制策略，控制分配文件及服务的访问权限； b)查看访问控制策略文档，判断是否根据业务需求和系统安全分析制定了系统的访问控制策略。	是□ 否□ 不适用□	

表 H.2　网上信息系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.8.6.	是否指定专人对系统进行管理，划分系统管理员角色，明确各个角色的权限、责任和风险，权限设定是否遵循最小授权原则。	访谈系统运维负责人，询问是否对系统管理员用户进行分类，明确各个角色的权限、责任和风险，权限设定是否遵循最小授权原则。	是□ 否□ 不适用□	
2.9.	**资源控制**			
2.9.1.	用户登录应用系统后在规定的时间内未执行任何操作，是否自动退出系统。	测试主要应用系统，当应用系统的通信双方中的一方在一段时间内未作任何响应，查看另一方是否能够自动结束会话。	是□ 否□ 不适用□	
2.9.2.	是否能够对系统的最大并发会话连接数进行限制。	检查主要应用系统的配置参数，查看是否提供对最大并发会话连接数进行限制。	是□ 否□ 不适用□	
2.9.3.	是否能够对单个账户的多重并发会话进行限制。	测试主要应用系统，可通过对系统进行超过规定的单个帐户的多重并发会话数进行连接，验证系统是否能够正确地限制单个帐户的多重并发会话数。	是□ 否□ 不适用□	
2.9.4.	是否能够对一个时间段内可能的并发会话连接数进行限制。	检查主要应用系统的配置参数，查看是否提供对最大并发会话连接数进行限制。	是□ 否□ 不适用□	
2.9.5.	是否能够对一个访问账户或一个请求进程占用的资源分配最大限额和最小限额。	检查主要应用系统设计和验收文档，查看是否对一个访问帐户或一个请求进程占用的资源分配最大限额和最小限额。	是□ 否□ 不适用□	
2.9.6.	是否能够对系统服务水平降低到预先规定的最小值进行检测和报警。	a)检查主要应用系统设计和验收文档，查看是否有服务水平最小值的设定，当系统的服务水平降低到预先设定的最小值时，系统报警； b)测试主要应用系统，可试图使服务水平降低到预先规定的最小值，验证系统是否能够正确检测并报警。	是□ 否□ 不适用□	
2.9.7.	是否提供服务优先级设定功能，并在安装后根据安全策略设定访问账户或请求进程的优先级，根据优先级分配系统资源。	检查主要应用系统设计和验收文档，查看是否能根据安全策略设定主体的服务优先级，根据优先级分配系统资源。	是□ 否□ 不适用□	

表 H.2　网上信息系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.10.	**数据安全**			
2.10.1.	通过互联网、卫星网进行通信时，是否采用密码技术保证通信过程中数据的完整性。	a)检查设计、验收文档或源代码，查看其是否有关于保护通信完整性的说明，如果有则查看是否有根据校验码判断对方数据有效性，以及散列（Hash）密码计算报文校验码的描述； b)对于通过互联网、卫星网进行通信的系统，通过截包分析，检查通信报文是否经过加密保护。	是□ 否□ 不适用□	
2.10.2.	是否能够检测到系统管理数据、鉴别信息和重要业务数据在传输过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施。	如果主要主机操作系统能够进行远程管理，则应查看应用系统的设计、验收文档或源代码，查看是否有关于能检测系统管理数据、鉴别信息和重要业务数据传输过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施的描述。	是□ 否□ 不适用□	
2.10.3.	是否采用加密或其他保护措施实现系统管理数据、鉴别信息和重要业务数据存储保密性。	检查主要应用系统设计文档，查看鉴别信息是否采用加密或其他有效措施实现存储保密性。	是□ 否□ 不适用□	
2.11.	**备份能力**			
2.11.1.	灾难应对能力是否达到《证券期货经营机构信息系统备份能力标准》第五级或重大灾难应对能力达到第六级要求。	检查“表0.8-系统备份能力”、“表0.8-数据备份情况”，查看灾难应对能力达标证明材料（包括：灾备系统建设情况、备份策略、应急演练记录等），确认灾难应对能力达到《证券期货经营机构信息系统备份能力标准》第五级或重大灾难应对能力达到第六级要求。	是□ 否□ 不适用□	
2.11.2.	重大灾难应对能力是否达到《证券期货经营机构信息系统备份能力标准》第六级要求。	检查“表0.8-系统备份能力”、“表0.8-数据备份情况”，查看灾难应对能力达标证明材料（包括：灾备系统建设情况、备份策略、应急演练记录等），确认重大灾难应对能力达到《证券期货经营机构信息系统备份能力标准》第六级要求。	是□ 否□ 不适用□	
2.11.3.	实时信息系统是否达到《证券期货经营机构信息系统备份能力标准》中故障应对能力的第四级要求。	检查“表0.8-系统备份能力”、“表0.8-数据备份情况”，检查公司实时信息系统故障应对能力达标证明材料（包括：备份系统建设情况、备份策略、应急演练记录等），确认故障应对能力达到《证券期货经营机构信息系统备份能力标准》中第四级要求。	是□ 否□ 不适用□	

表 H.2　网上信息系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.11.4.	法人清算系统、门户网站系统等非实时信息系统是否满足《证券期货经营机构信息系统备份能力标准》中故障应对能力的第二级要求。	检查“表0.8-系统备份能力”、“表0.8-数据备份情况”，检查公司非实时信息系统故障应对能力达标证明材料（包括：备份系统建设情况、备份策略、应急演练记录等），确认法人清算系统、门户网站系统等非实时信息系统的故障应对能力达到《证券期货经营机构信息系统备份能力标准》中故障应对能力的第二级要求。	是□ 否□ 不适用□	
2.12.	**安全审计**			
2.12.1.	应用系统是否能够对每个业务用户的关键操作进行记录，例如用户登录、用户退出、增加用户、修改用户权限等操作。	a)检查主要应用系统，查看审计范围是否覆盖到每个用户，审计策略是否覆盖系统内重要的安全相关事件，例如，用户标识与鉴别、访问控制的所有操作记录、重要用户行为、系统资源的异常使用、重要系统命令的使用等； b)测试主要应用系统，在应用系统上试图产生一些重要的安全相关事件（如进行用户登录、修改用户权限等操作），查看应用系统是否对其进行了审计，验证应用系统安全审计的覆盖情况是否覆盖到每个用户；如果进行了审计则查看审计记录内容是否包含事件的日期、时间、发起者信息、类型、描述和结果等。	是□ 否□ 不适用□	
2.12.2.	审计记录的内容是否包括事件日期、时间、发起者信息、类型、描述和结果等。审计记录是否至少保存6个月。	检查主要应用系统的审计记录，查看是否包括事件发生的日期与时间、触发事件的主体与客体、事件的类型、事件成功或失败、身份鉴别事件中请求的来源、事件的结果等内容；检查是否保存了6个月以上的审计记录。	是□ 否□ 不适用□	
2.12.3.	是否采取有效措施防止单独中断审计进程；审计进程应作为应用系统整体进程中的一部分，并且不能单独中断。	测试主要应用系统，试图非授权终止审计进程或审计功能，删除、修改或覆盖审计记录，查看安全审计进程和记录的保护情况。	是□ 否□ 不适用□	
2.12.4.	是否提供对审计记录数据进行统计、查询、分析及生成审计报表的功能。	检查主要应用系统，查看是否为授权用户浏览和分析审计数据提供专门的审计分析功能，并能根据需要生成审计报表。	是□ 否□ 不适用□	

表 H.2　网上信息系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.12.5.	是否保证信息系统日志的完备性，确保所有重大修改被完整地记录，确保开启审计留痕功能。证券公司信息系统日志是否至少保存 15 年。	a)检查运维管理制度，是否规定保证信息系统日志的完备性，确保所有重大修改被完整地记录，信息系统日志是否至少保存 15 年； b)检查系统设计和验收文档，是否开启审计留痕功能。	是□ 否□ 不适用□	
2.12.6.	是否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。	查看每日检查记录，是否指定人员按照运维管理制度和操作流程，对日常操作执行情况进行每日检查。	是□ 否□ 不适用□	
2.12.7.	是否每季组织开展内部检查，形成检查报告。	审阅内部检查报告，检查是否每季度一次。	是□ 否□ 不适用□	
2.12.8.	是否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。	a)审阅公司年度审计计划，是否包含信息系统运维管理工作审计项目； b)检查公司年度审计报告，是否包含信息系统运维管理工作审计项目。	是□ 否□ 不适用□	
2.12.9.	检查和审计范围是否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。	检查信息系统运维管理工作审计报告，确定信息系统运维管理工作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。	是□ 否□ 不适用□	
2.12.2.	是否对检查和审计的结果采取纠正性和预防性的措施。	审阅信息系统运维管理工作审计整改报告，确定是否对检查和审计的结果采取纠正性和预防性的措施。	是□ 否□ 不适用□	
2.12.11.	是否定期检查安全隔离情况，确保各安全域之间有效隔离。	a)查看包括自建和托管机房的网络拓扑图、安全域划分情况，检查各安全域之间是否采用了防火墙或安全网关等有效隔离方式和隔离手段； b)审阅最近的网络隔离情况检查报告，判断是否定期对上述事项进行了检查。	是□ 否□ 不适用□	

表 H.2　网上信息系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.12.12.	是否组织相关人员定期对监测和报警记录进行分析、评审，发现可疑行为，形成分析报告，并采取必要的应对措施。	a)访谈系统运维负责人，询问其是否组织人员定期对监测记录进行分析、评审，是否发现可疑行为并对其采取必要的措施，是否形成分析报告； b)检查监测记录，查看是否记录监控对象、监控内容、监控的异常现象处理等方面，查看是否对异常现象及处理措施形成分析报告。	是□ 否□ 不适用□	
2.12.13.	是否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。	检查是否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，以满足审计的需要。	是□ 否□ 不适用□	
2.12.14.	是否保存监控产生的日志，保存时间不少于一年。	检查监控日志，保存时间是否不少于一年。	是□ 否□ 不适用□	
2.12.15.	是否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。	查看评估记录，是否每日分析核心交易业务系统监控日志及巡检记录，并跟踪处理日志分析中发现的异常事件。	是□ 否□ 不适用□	
2.12.16.	是否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。	查看评估报告，是否至少每季度全面评估监控日志和操作记录，分析异常情况。	是□ 否□ 不适用□	
2.12.17.	是否至少每月对运行日志和审计数据进行分析。	检查是否每月对运行日志和审计数据进行分析。	是□ 否□ 不适用□	
3.	**数据库管理**			
3.1.	**安全审计**			
3.1.1.	审计内容是否至少包括：用户的添加和删除、审计功能的启动和关闭、审计策略的调整、权限变更、系统资源的异常使用、重要的系统操作（如用户登录、退出）等。	审阅主机审计记录，检查审计内容是否包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件；审计内容至少包括：用户的添加和删除、审计功能的启动和关闭、审计策略的调整、权限变更、系统资源的异常使用、重要的系统操作（如用户登录、退出）等。	是□ 否□ 不适用□	
3.1.2.	审计记录是否包括事件的日期、时间、类型、主体标识、客体标识和结果等。	审阅主机运行日志，检查审计记录是否包括事件的日期、时间、类型、主体标识、客体标识和结果等。	是□ 否□ 不适用□	

表 H.2　网上信息系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
3.1.3.	是否保护审计记录，避免受到未预期的删除、修改或覆盖等。审计记录是否至少保存 6 个月。	检查审计记录是否至少保存 6 个月。	是□ 否□ 不适用□	
3.1.4.	审计范围是否覆盖到服务器和重要客户端上的每个数据库用户；应在保证系统运行安全和效率的前提下，启用系统审计或采用第三方安全审计产品实现审计要求。	a)通过访谈，了解是否在保证系统运行安全和效率的前提下，启用了系统审计或采用第三方安全审计产品实现审计要求，保证产生、有效记录和存储了审计日志； b)通过访谈，审阅主机和客户端审计记录，判断是否覆盖到服务器和重要客户端上的每个操作系统用户和数据库用户。	是□ 否□ 不适用□	
3.1.5.	是否能够根据记录数据进行分析，并生成审计报表。	检查主要服务器操作系统、重要终端操作系统和主要数据库管理系统的安全审计策略，查看是否为授权用户提供浏览和分析审计记录的功能，是否可以根据需要自动生成不同格式的审计报表。	是□ 否□ 不适用□	
3.1.6.	是否保护审计进程，避免受到未预期的中断。	测试主要服务器操作系统、重要终端操作系统和主要数据库管理系统，可通过非审计员的其他帐户试图中断审计进程，验证审计进程是否受到保护。	是□ 否□ 不适用□	
3.2.	**访问控制**			
3.2.1.	是否严格限制人工对数据库操作的账户权限，并分别使用不同权限的账户执行查询、插入、更新、删除等操作。	a)查看数据库账户权限管理制度，是否规定分别使用不同权限的账户执行查询、插入、更新、删除等操作； b)检查对数据库进行人工操作的记录，确认使用不同权限的账户执行查询、插入、更新、删除等操作。	是□ 否□ 不适用□	
3.3.	**身份鉴别**			
3.3.1.	口令是否符合以下条件：数字、字母、符号混排，无规律的方式。	检查口令管理制度，是否规定口令符合以下条件：数字、字母、符号混排，无规律的方式。	是□ 否□ 不适用□	
3.3.2.	口令的长度是否至少为 12 位。	检查口令管理制度，是否规定管理员用户口令的长度至少为 12 位。	是□ 否□ 不适用□	
3.3.3.	口令是否至少每季度更换 1 次，更新的口令至少 5 次内不能重复。	检查口令管理制度，是否规定管理员用户口令至少每季度更换 1 次，更新的口令至少 5 次内不能重复。	是□ 否□ 不适用□	

表 H.2　网上信息系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
3.3.4.	如果设备口令长度不支持 12 位或其他复杂度要求，口令是否使用所支持的最长长度并适当缩小更换周期；也可以使用动态密码卡等一次性口令认证方式。	检查口令管理制度，是否规定口令应使用所支持的最长长度并适当缩小更换周期，也可以使用动态密码卡等一次性口令认证方式。	是□ 否□ 不适用□	
3.3.5.	是否为数据库系统的不同用户分配不同的用户名，确保用户名具有唯一性。	检查数据库系统的用户列表，标识是否唯一。	是□ 否□ 不适用□	
3.4.	**数据库运维**			
3.4.1.	是否保持数据库的可用性，及时维护、更新软件。	a)查看数据库软件、数据库监控软件的采购合同，以及维护、更新记录； b)查看数据库监控日志，判断表空间使用率、连接数等是否保持在合理范围。	是□ 否□ 不适用□	
3.4.2.	是否对数据库的参数进行配置、调优，编制文档并保持更新。	a)访谈数据库管理员,询问是否依照数据库配置文档进行安装、配置及调优； b)查看数据库配置文档和维护记录，确认对数据库系统进行了配置、调优。	是□ 否□ 不适用□	
3.4.3.	是否定期对数据库容量进行检查和评估，形成评估报告。	a)查看公司数据库容量管理制度，是否明确要求定期对数据库系统容量进行检查和评估，并形成评估报告； b)访谈数据库管理员，查看数据库容量评估报告，确认定期对数据库容量进行了检查和评估。	是□ 否□ 不适用□	
3.4.4.	是否管理数据库、表、索引、存储过程，数据库的升级、优化、扩容、迁移。	a)查看公司数据库容量管理制度，是否明确数据库管理员应负责管理数据库、表、索引、存储过程，数据库的升级、优化、扩容、迁移； b)访谈数据库管理员，查看数据库维护记录，确认数据库管理员按照要求管理数据库、表、索引、存储过程，对数据库进行了升级、优化、扩容、迁移等维护工作。	是□ 否□ 不适用□	
3.4.5.	是否定期检查数据库的用户、口令及权限设置的正确性。	访谈数据库管理员，查看数据库维护记录，确认是否定期检查数据库的用户、口令及权限设置的正确性。	是□ 否□ 不适用□	

表 H.2　网上信息系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
4.	**网上信息系统**			
4.1.	**系统架构**			
4.1.1.	通过网上证券信息系统向客户提供证券交易行情信息的，是否提示行情源。	利用测试账户登陆网上证券信息系统，确认向投资者提示了行情源信息。	是□ 否□ 不适用□	
4.1.2.	向客户提供证券信息的，是否说明信息来源，并提示投资者对行情信息及证券信息等进行核实。	利用测试账户登陆网上证券信息系统，确认向投资者提示了资讯信息的信息来源，并提示投资者对行情信息及证券信息等进行核实。	是□ 否□ 不适用□	
4.1.3.	集中交易系统是否逐笔存储交易委托、银证转账等操作的客户交易终端信息。	a)检查设计文档或验收文档，查看是否采取适当技术，确保集中交易系统能够逐笔记录客户交易终端 IP 地址、IMEI、WIFI MAC 地址、电话号码等信息； b)检查集中交易系统交易记录，检查是否包含包括客户交易终端 IP 地址、IMEI、WIFI MAC 地址、电话号码等信息。	是□ 否□ 不适用□	
4.1.4.	网上交易软件是否采取安全的密码输入方式，增强防御恶意程序窃取密码的功能。	a)查看网上交易软件设计文档，确认采用了安全的密码输入方式，可以防御恶意程序窃取密码； b)查看网上交易软件安全测试报告，确认密码输入方式可以防御恶意程序窃取密码。	是□ 否□ 不适用□	
4.2.	**结构安全**			
4.2.1.	网上信息系统是否具备 2 个或 2 个以上的不同运营商的互联网接入。	检查“表 0.7 附表-该机房的网上信息系统互联网通信情况”、网络设计或验收文档，查看是否具备 2 个或 2 个以上的不同运营商的互联网接入。	是□ 否□ 不适用□	
4.2.2.	网上信息系统服务端是否存在有效屏蔽系统技术错误信息的机制，不将系统产生的错误信息直接反馈给客户。	a)访谈技术开发人员，确认系统服务端存在屏蔽客户端显示技术错误信息的措施； b)在技术人员协助下，测试该种措施的有效性。	是□ 否□ 不适用□	

表 H.2　网上信息系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
4.2.3.	网上开展证券业务的网络系统、安全系统、应用系统等重要环节是否具备足够的冗余，以应对网站及网上交易可能出现的突发峰值。	检查“表 0.6-网上信息系统站点分布信息情况”、“表 0.7 附表-该机房的网上委托站点基本情况”、“表 0.7 附表-该机房的网上委托站点详细情况”、“表 0.7 附表-该机房的网上行情站点基本情况”、“表 0.7 附表-该机房的网上行情站点详细情况”、“表 0.7 附表-该机房的手机证券站点基本情况”、“表 0.7 附表-该机房的手机证券站点详细情况”、测试报告，判断网络线路负载率、交易站点压力测试峰值与本年度峰值的比对情况等，确认系统重要环节具备足够的容量冗余。	是□ 否□ 不适用□	
4.2.4.	网上开展证券业务的网络系统、安全系统、应用系统等重要环节是否具备良好的可扩充性，以应对业务增长和市场的变化。	a)审阅系统架构图并访谈系统管理员，确认网络系统、安全系统、应用系统等重要环节具备良好的可扩充性； b)获取近期系统扩充资料，评价系统的可扩展性。	是□ 否□ 不适用□	
4.3.	**系统运维**			
4.3.1.	特殊紧急情况下通过互联网进行远程操作后，是否及时关闭相关端口。	a)访谈安全管理员，了解特殊情况下通过互联网进行远程操作的控制策略、操作流程及对应采取的安全措施； b)审阅远程操作的工作日志及流程记录，查看远程操作有日志或监控留痕，确认远程操作后关闭相关端口。	是□ 否□ 不适用□	
4.3.2.	网上证券服务端是否对不完整、被篡改、重发的数据包进行监控，对登录、委托方式、品种、价格、数量、操作频率、转账等异常行为进行跟踪、监控和限制，记录其账号、IP 地址等相关信息，并通过短信、电话等方式及时提示客户，必要时进行用户临时锁定。监控和处置情况应形成记录备查。	a)访谈技术开发人员，确认对不完整、被篡改、重发的数据包进行了监控； b)访谈技术开发人员，确认对客户行为进行了监控和记录，了解向客户进行提示的方式和内容； c)检查对不完整、被篡改、重发的数据包进行了监控的记录，以及定期分析报告，确认监控工作得到贯彻执行； d)检查监控记录和客户操作日志，确认日志中包含了账号、IP 地址等相关信息。	是□ 否□ 不适用□	
4.3.3.	门户网站监控指标是否包括网页内容、日均访问量等。	检查“表 0.7 附表-该机房的网上信息系统监控情况-门户网站”，现场检查门户网站监控指标是否包括网页内容、日均访问量等。	是□ 否□ 不适用□	

表 H.2　网上信息系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
4.3.4.	是否定期评估可供客户使用的网上证券信息系统的资源状况，并根据实时监控信息、可预见的业务发展需求进行容量的需求预测，确保有充足的处理能力、存储容量和通讯带宽，满足业务增长的需要，保证网上证券服务的可用性，并能抵御一定程度的拒绝服务攻击和缓冲区溢出攻击。	a)查看评估报告，判断是否根据监控系统日志、业务发展需求等定期进行评估，保证网上证券服务的处理能力、存储容量、通讯带宽等的可用性； b)检查渗透测试报告，判断网上证券服务是否能够抵御一定程度的拒绝服务攻击和缓冲区溢出攻击。	是□ 否□ 不适用□	
4.3.5.	是否定期对网站程序代码进行全面检查和评估，并及时修补，避免各种漏洞的存在。	检查网站程序代码审查报告，确认定期对网站程序代码进行全面检查和评估，并及时修补，避免各种漏洞的存在。	是□ 否□ 不适用□	
4.4.	**安全管理**			
4.4.1.	安全风险评估是否包括漏洞扫描、攻击测试、病毒扫描、木马检测等，针对不同的威胁设置相应的检查频率。	检查安全风险评估报告，评估是否包括漏洞扫描、攻击测试、病毒扫描、木马检测等，确认检查频率能够有效应对不同的威胁。	是□ 否□ 不适用□	
4.4.2.	基于浏览器的网上证券下单网页是否使用 HTTPS 等加密方式与服务端交互，服务端是否具备防范 SQL 注入式攻击、跨站脚本攻击等网页攻击的能力，同时关闭 HTTP 服务器的 Web 远程维护功能。	检查“表 0.7 附表-该机房的网页下单站点情况-下单网页网址”、“表 0.7 附表-该机房的网页下单站点情况-下单网页 IP 地址”，查看网上交易软件安全测试报告，确认使用 HTTPS 等加密方式与服务端交互，服务端应具备防范 SQL 注入式攻击、跨站脚本攻击等网页攻击的能力，同时关闭 HTTP 服务器的 Web 远程维护功能。	是□ 否□ 不适用□	
4.4.3.	网上证券信息系统采用的认证授权和加密体系是否通过国家信息安全机构的安全性测评，具备足够的强度和抗攻击能力，并根据在网上开展证券业务的安全性需要和信息技术的发展，定期检查、评估和及时调整。	a)查看安全性测评报告，判断网上证券信息系统采用的认证授权和加密体系是否通过国家信息安全机构的安全性测评，具备足够的强度和抗攻击能力； b)查看网上证券信息系统采用的认证授权和加密体系的定期检查、评估报告，确认网上证券信息系统的认证授权和加密体系定期进行了评估和及时调整。	是□ 否□ 不适用□	

表 H.2　网上信息系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
4.5.	**身份鉴别**			
4.5.1.	网上信息系统服务端是否能向客户提供可证明服务端自身身份的信息，如提供预留验证信息服务，在网上交易客户登录时回显，帮助客户有效识别仿冒的网上交易信息系统，防范利用仿冒的网上交易信息系统进行诈骗活动。	a)访谈公司网上交易系统的预留验证信息相关服务的情况； b)检查网上信息系统是否存在可设置预留验证信息的功能模块，且设置可成功保存。	是□ 否□ 不适用□	
4.5.2.	网上信息系统是否提供可靠的身份验证机制，除采用账号名、口令、验证码的身份认证方式外，是否向客户提供一种以上强度更高的身份认证方式供客户选择使用，如客户端电脑或手机特征码绑定、软硬件证书、动态口令等认证方式，确认客户的身份和登录的合法性，防止不法分子利用木马等黑客程序窃取客户账号和口令。	a)检查“表 0.6-网上信息系统身份认证方式”、“表 0.6-软件数字证书建设情况”，访谈其它认证机制的实施情况； b)检查除静态口令外的强度较高的用户身份认证机制的说明，例如数字证书、动态口令、电脑或手机特征码绑定等与信息系统的实际情况是否一致。	是□ 否□ 不适用□	
4.5.3.	网上信息系统客户端是否能向客户提示最近一次登录的日期、时间、地址等信息。	利用测试账户登录，检查确认向客户提示了最近一次登录的日期、时间、地址等信息。	是□ 否□ 不适用□	
4.5.4.	是否根据自身系统的特点和需求，结合试点工作案例以及其他金融企业成熟做法，制定“网上交易强身份认证系统”实施方案（以下简称实施方案）。实施方案应包括但不限于：组织保障机制、系统技术架构、产品选型方案、业务管理及服务支持体系设计、应急处置措施、实施计划及进度安排等方面内容。	a)检查是否有“网上交易强身份认证系统”实施方案； b)检查方案内容是否包括但不限于：组织保障机制、系统技术架构、产品选型方案、业务管理及服务支持体系设计、应急处置措施、实施计划及进度安排等方面内容。	是□ 否□ 不适用□	
4.5.5.	特殊紧急情况下需要通过互联网进行远程操作时，是否通过限制登录 IP、使用数字证书或动态口令、全程监控等措施确保安全。	a)访谈安全管理员，了解特殊情况下通过互联网进行远程操作的控制策略、操作流程及对应采取的安全措施； b)审阅远程操作的工作日志及流程记录，确认远程操作有日志或监控留痕。	是□ 否□ 不适用□	

表 H.2　网上信息系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
4.5.6.	网上信息系统服务端是否监控并能够抵御连续猜测，避免攻击者通过群体大规模对合法证券账户进行非法用户登陆的请求，导致大量用户账户被异常锁定，正常用户无法登录。	a)访谈技术开发人员和网络安全管理员，确认对通过群体大规模合法证券账户进行非法用户登陆客户行为导致客户账户锁定行为的监控和防备措施； b)审阅网络安全测试记录，确认可有效避免该类攻击行为。	是□ 否□ 不适用□	
4.5.7.	是否防止用户使用简单口令，并能够抵御连续猜测等对客户账户恶意攻击行为。	a)查看口令管理办法，确认设置了弱口令检查机制，并能够抵御连续猜测； b)现场检查对弱口令和连续猜测等攻击行为的抵御能力； c)检查系统日志，确认能够抵御弱口令、连续猜测等攻击行为。	是□ 否□ 不适用□	
4.6.	**访问控制**			
4.6.1.	是否禁止开发、测试和运营人员未经授权访问、修改非职责范围内的网上证券信息系统。	a)检查开发、测试和运行相关规章制度，是否禁止开发、测试和运营人员未经授权访问营运系统； b)检查网上证券信息系统日志记录，是否有开发、测试和运营人员未经授权访问营运系统。	是□ 否□ 不适用□	
4.7.	**客户端管理**			
4.7.1.	网上证券客户端是否具备反调试能力。	a)访谈技术人员了解网上证券客户端软件程序的反调试能力； b)审阅安全测试报告，确认网上证券客户端软件具有反调试能力。	是□ 否□ 不适用□	
4.7.2.	向客户提供的交易终端软件，是否采取适当的技术，确保软件能够采集到客户交易终端电话号码、互联网通讯协议地址（IP 地址）、媒介访问控制地址（MAC 地址）以及其他能识别客户交易终端的特征代码。	a)检查“表 0.6-网上信息系统客户端软件使用情况”、设计文档或验收文档，查看是否采取适当技术，确保交易终端软件能够采集到客户交易终端的特征代码，包括 IP 地址、IMEI、WIFI MAC 地址、电话号码等信息； b)检查客户交易记录中，是否包含包括 IP 地址、IMEI、WIFI MAC 地址、电话号码等信息。	是□ 否□ 不适用□	

表 H.2　网上信息系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
4.7.3.	向客户提供的交易终端软件，是否采取适当的技术，确保软件能够采集到客户交易终端信息。由第三方提供交易终端软件的，应当建立软件认证许可制度，要求第三方采取适当的技术，确保软件能够采集到客户交易终端信息。客户交易终端软件应当具备先提醒升级、再自动升级为最新版本的功能。	a)检查第三方设计文档或验收文档，查看是否采取适当技术，确保交易终端软件能够采集到客户交易终端的特征代码，包括 IP 地址、IMEI、WIFI MAC 地址、电话号码等信息； b)检查客户交易记录中，是否包含包括 IP 地址、IMEI、WIFI MAC 地址、电话号码等信息； c)检查设计文档或验收文档，查看客户交易终端软件是否具备先提醒升级、再自动升级为最新版本的功能； d)测试验证客户交易终端软件是否具备先提醒升级、再自动升级为最新版本的功能。	是□ 否□ 不适用□	
4.7.4.	是否按照规定的要求建设、改造和维护相关信息系统，以妥善管理客户交易终端信息，并提供符合技术规范的查询接口。是否采取必要的技术手段，满足交易时段客户信息查询的需要。	a)查看管理客户交易终端信息的系统设计文档，访谈技术人员，信息系统是否妥善管理客户交易终端信息，并提供符合技术规范的查询接口。应当采取必要的技术手段，满足交易时段客户信息查询的需要； b)查看管理客户交易终端信息的系统上线的验收文档，系统建设改造和维护是否达到设计要求。	是□ 否□ 不适用□	
4.7.5.	客户端软件，是否对其授权第三方发布的证券委托软件进行审核、监管。	a)查看第三方发布的证券委托软件管理办法，确认有对客户端软件管理和发布的相关规定； b)查看对授权第三方发布证券委托软件的相关记录，确认证券公司是否对其授权第三方发布的证券委托软件进行审核、监管。	是□ 否□ 不适用□	
4.7.6.	是否采取有效措施对门户网站上提供下载的网上证券客户端软件程序进行保护，客户端软件程序编译封装、形成下载文件后，是否安排专人对其进行严格的病毒扫描和木马检查，并通过专用安全手段传输至网站文件下载服务器。	a)检查网上证券客户端软件编译封装操作手册；确认是否采取有效措施对门户网站上提供下载的网上证券客户端软件程序进行保护； b)查看网上证券客户端病毒、木马扫描记录，确认客户端软件程序编译封装、形成下载文件后，安排专人对其进行严格的病毒扫描和木马检查，并通过专用安全手段传输至网站文件下载服务器。	是□ 否□ 不适用□	

表 H.2　网上信息系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
4.7.7.	网上证券客户端是否具有唯一连接到本证券公司网上证券接入系统的保障机制。网上证券客户端应提供足够的识别信息，以保证网上证券服务端能够对发出连接请求的客户端与证券公司所提供下载的程序进行一致性验证。	a)查看网上证券客户端是否具有唯一连接到本证券公司网上证券接入系统的保障机制； b)检查网上证券客户端连接日志，确认是否对发出连接请求的客户端与证券公司所提供下载的程序进行了一致性验证。	是□ 否□ 不适用□	
4.7.8.	当客户访问网上证券服务端时，未经客户许可，是否禁止以任何方式在客户端系统中安装插件。	查看网上证券服务端设计文档，确认当客户访问网上证券服务端时，未经客户许可，未以任何方式在客户端系统中安装插件。	是□ 否□ 不适用□	
4.7.9.	是否建立确认机制以保证客户获得正确的移动证券客户端软件。	查看移动证券客户端软件设计文档，确认能够保证客户获得正确的移动证券客户端软件。	是□ 否□ 不适用□	
4.8.	**门户网站**			
4.8.1.	是否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。	检查“表 0.7 附表-门户网站防篡改措施”，查看网站防篡改说明，是否可以防止网页内容、可下载的客户端软件等被未经授权的修改。	是□ 否□ 不适用□	
4.8.2.	门户网站是否禁止存放客户资料、交易数据等客户敏感数据。	审阅门户网站说明，检查是否禁止存放客户资料、交易数据等客户敏感数据。	是□ 否□ 不适用□	
4.8.3.	是否建立对门户网站内容的审核制度、完整的发布流程和监控机制。	查看门户网站管理制度，是否建立对门户网站内容发布的审核、管理和监控机制。	是□ 否□ 不适用□	
4.8.4.	是否对网页内容进行监控，对有害信息进行过滤，防止网站出现不良信息。	审阅门户网站说明，是否对网页内容进行监控，对有害信息进行过滤，防止网站出现不良信息。	是□ 否□ 不适用□	
4.8.5.	当网站上的页面内容、提供给投资者下载的客户端软件及其他文件被异常修改时，是否能自动告警或自动恢复，防止被捆绑木马程序。	查看网站安全检查报告，当网站上的页面内容、提供给投资者下载的客户端软件及其他文件被异常修改时，是否能自动告警或自动恢复，防止被捆绑木马程序。	是□ 否□ 不适用□	
4.8.6.	网上证券信息系统是否部署在中华人民共和国境内，满足技术审计、监管部门现场检查及中国司法机构调查取证等要求。部署网上证券信息系统的有形场所，是否符合国家安全标准的有关要求。	检查“表 0.7 附表-该机房的网上信息系统详细情况-所在机房名称”、门户网站说明，网上信息系统是否部署在中华人民共和国境内，满足技术审计、监管部门现场检查及中国司法机构调查取证等要求。	是□ 否□ 不适用□	

表 H.2　网上信息系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
4.8.7.	网上证券信息系统是否自主运营、自主管理。如涉及第三方（指除证券公司及其客户以外的任何一方），应与第三方签订保密协议和服务级别协议，并明确责任，采取措施防止通过第三方泄露用户信息。	a)查看“表 0.7 附表-依托第三方电子商务平台的情况”、“表 0.7 附表-门户网站系统情况”、网上证券信息系统说明，是否自主运营、自主管理； b)如涉及第三方（指除证券公司及其客户以外的任何一方），检查与第三方签订的保密协议和服务级别协议，协议内容是否明确责任，采取措施防止通过第三方泄露用户信息。	是□ 否□ 不适用□	
4.8.8.	门户网站是否按照国家主管部门的有关规定办理 ICP 备案，在网站首页公布 ICP 备案号，并提供备案信息的链接。	a)检查“表 0.7 附表-门户网站系统情况-ICP 备案号”、向当地有关部门办理的网站备案文件，是否与资源调查表所填信息相符； b)现场观察在网站首页是否公布了 ICP 备案号，并提供客户查询门户网站备案信息的链接。	是□ 否□ 不适用□	
4.8.9.	网上客户业务处理的日志是否单独存放。	检查网上客户业务处理的日志是否另处存放。	是□ 否□ 不适用□	
4.9.	**数据安全**			
4.9.1.	通过互联网、卫星网进行通信时，建立通信连接之前，应用系统是否利用密码技术或可靠的身份认证技术进行会话初始化验证。	检查“表 0.6-网上信息系统身份认证方式”、“表 0.6-软件数字证书建设情况”，检查设计、验收文档或源代码，访谈技术人员，查看是否有关于保护通信保密性的说明，如果有则查看在通信双方建立连接之前利用密码技术进行会话初始化验证的描述。	是□ 否□ 不适用□	
4.9.2.	通过互联网、卫星网传递系统管理数据、鉴别信息和重要业务数据时，是否对整个报文或会话过程进行加密。	检查设计、验收文档或源代码，访谈技术人员，查看其是否有关于保护通信保密性的说明，如果有则查看对整个报文或会话过程是否进行加密的描述。	是□ 否□ 不适用□	
4.9.3.	网上客户端的客户身份信息和交易数据等重要数据传输是否采用国家信息安全机构认可的加密技术和加密强度，并最低达到 SSL 协议 128 位的加密强度。	查看系统设计文档，访谈技术开发人员，了解业务数据在网络传输中的加密方式，确认使用的加密产品和加密算法是否经国家密码管理机构认可，并最低达到 SSL 协议 128 位的加密强度。	是□ 否□ 不适用□	

表 H.2　网上信息系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
4.9.4.	加解密是否在投资者与证券公司实际控制的设备中进行，不得存在任何中间环节对数据进行加解密。	a)访谈应用系统管理员，询问集中交易系统数据加密传输方式； b)检查设计或验收文档，查看集中交易系统，是否明确说明只在投资者与证券公司实际控制的设备中进行，不得存在任何中间环节对数据进行加解密。	是□ 否□ 不适用□	
4.9.5.	移动证券系统是否自主运营，实现数据从用户终端到网上证券服务端之间的加密传送和控制，并随着技术的发展，不断提高加密强度，完善认证算法。	a)访谈技术开发人员，数据在终端和服务端间的传输是否进行了加密和控制； b)审阅安全测试记录，确认加密和控制措施的有效性。	是□ 否□ 不适用□	
4.9.6.	移动证券客户端是否具备一定加密强度的用户认证功能，保护客户账号和口令信息。	访谈技术开发人员，了解移动客户端用户认证的方式，是否具备一定加密强度的用户认证功能，并评价认证方式的有效性。	是□ 否□ 不适用□	
4.9.7.	门户网站中客户账号及口令，是否采用加密方式传输，并最低达到 SSL 协议 128 位的加密强度。	检查门户网站设计文档，访谈技术开发人员，了解业务数据在网络传输中的加密方式，确认使用的加密产品和加密算法是否经国家密码管理机构认可，并最低达到 SSL 协议 128 位的加密强度。	是□ 否□ 不适用□	
4.9.8.	网上证券信息系统未经证券公司授权，是否未与第三方进行任何形式的数据交换，并具备经过认证后仅向授权的第三方指定地址发送信息的功能。	a)检查系统设计文档，访谈安全管理员，了解网上证券信息系统与第三方间进行的数据交换情况及采取的认证措施； b)审阅授权的第三方数据交换清单和网络拓扑图，确定涉及第三方的环节，并确认第三方有授权及认证记录。	是□ 否□ 不适用□	
4.9.9.	网上证券客户端在本地计算机储存客户账户、交易数据等重要信息时，是否提示客户，经客户确认后以加密方式存储。	a)审阅系统设计文档，了解网上证券客户端在本地计算机储存客户账户、交易数据等重要信息时，是否提示客户，经客户确认后以加密方式存储； b)现场测试网上客户端在本地计算机储存客户账户、交易数据等重要信息时，是否提示客户，并经客户确认后以加密方式存储。	是□ 否□ 不适用□	

表 H.2　网上信息系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
4.10.	**外包管理**			
4.10.1.	网上证券信息系统应自主运营、自主管理。如涉及第三方（指除证券公司及其客户以外的任何一方），是否与第三方签订保密协议和服务级别协议，并明确责任，采取措施防止通过第三方泄露用户信息。	a)检查与第三方签署的保密协议和服务级别协议，判断是否明确了第三方泄露用户信息的责任； b)检查第三方操作记录，判断是否采取措施防止通过第三方泄露用户信息，如第三方维护时只提供临时密码等。	是□ 否□ 不适用□	
4.11.	**应急处置**			
4.11.1.	发现假冒本公司网上证券服务的非法活动或者网上证券信息系统出现重大安全事件后，是否及时向监管部门、公安机关报告。在启动实施网上证券信息系统应急预案时应及时向投资者公告。对于假冒本公司的非法活动应及时通过证券公司网站、网上证券客户端、电话语音系统或短信平台等提醒投资者注意。	a)访谈系统管理员和安全管理员，了解对网上证券服务异常情况的报备情况； b)审阅历史报备文档资料，确认安全事件报备工作满足要求。	是□ 否□ 不适用□	
4.12.	**系统托管**			
4.12.1	二级系统托管是否满足《证券期货业信息系统托管基本要求》（JR/T 0133-2015)的相关要求。	检查托管服务合同和相关文档，确认按照信息安全等级保护二级要求进行定级的系统选购了二级系统托管服务。	是□ 否□ 不适用□	
4.12.2	三级系统托管是否满足《证券期货业信息系统托管基本要求》（JR/T 0133-2015)的相关要求。	检查托管服务合同和相关文档，确认按照信息安全等级保护三级要求进行定级的系统选购了三级系统托管服务。	是□ 否□ 不适用□	
4.12.3	未定级系统托管是否满足《证券期货业信息系统托管基本要求》（JR/T 0133-2015)的相关要求。	检查托管服务合同和相关文档，确认未进行信息安全等级保护定级备案的信息系统选购了二级系统托管服务。	是□ 否□ 不适用□	

附 录 I
（规范性附录）
第三方存管系统审计底稿

表I.1至表I.2给出了第三方存管系统审计的程序、内容及相关记录要求。

表I.1 第三方存管系统审计底稿

被审计部门：	索引号：DSFCGXT
审计主题：第三方存管系统	审计年度：
审计结论、意见及建议： 编制人： 年 月 日 （部门盖章）	
复核意见： 复核人： 年 月 日 （部门盖章）	
被审计部门意见： 年 月 日 （部门盖章）	

表 I.1　第三方存管系统审计底稿（续）

审计证据列表：

表I.2　第三方存管系统审计底稿

序号	审计项	审计程序	审计结论	备注
1	主机管理			
1.1.	身份鉴别			
1.1.1.	操作系统管理员口令是否符合以下条件：数字、字母、符号混排，无规律的方式。	检查口令管理制度，是否规定口令符合以下条件：数字、字母、符号混排，无规律的方式。	是□ 否□ 不适用□	
1.1.2.	操作系统管理员口令的长度是否为12位。	检查口令管理制度，是否规定管理员用户口令的长度至少为12位。	是□ 否□ 不适用□	
1.1.3.	操作系统管理员口令是否每季度更换1次，更新的口令至少5次内不能重复。	检查口令管理制度，是否规定管理员用户口令至少每季度更换1次，更新的口令至少5次内不能重复。	是□ 否□ 不适用□	
1.1.4.	如果受限于操作系统，使得管理员口令长度不支持12位或其他复杂度要求，口令是否使用所支持的最长长度并适当缩小更换周期；也可以使用动态密码卡等一次性口令认证方式。	检查口令管理制度，是否规定如果设备口令长度不支持12位或其他复杂度要求，口令应使用所支持的最长长度并适当缩小更换周期，也可以使用动态密码卡等一次性口令认证方式。	是□ 否□ 不适用□	
1.1.5.	是否启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施。	a)检查重要服务器操作系统的身份鉴别策略，查看是否配置了登录失败处理功能、设置了非法登录次数的限制值； b)查看是否设置网络登录连接超时，并自动退出。	是□ 否□ 不适用□	
1.1.6.	当对服务器进行远程管理时，是否采取必要措施，防止鉴别信息在网络传输过程中被窃听。	查看“表0.13附表一-信息系统名称”、“表0.13附表一-本系统中密码机使用情况”，访谈系统管理员，询问是否对操作系统采用了远程管理方式，如果采用远程管理方式，查看是否具有防止鉴别信息在网络传输过程中被窃听的措施。	是□ 否□ 不适用□	
1.1.7.	是否为操作系统的不同用户分配不同的用户名，确保用户名具有唯一性。	检查操作系统的用户列表，标识是否唯一，或采取堡垒机等措施。	是□ 否□ 不适用□	
1.1.8.	通过本地控制台管理主机设备时，是否采用一种或一种以上身份鉴别技术。	查看安全策略文档，检查本地控制台管理主机设备是否采用一种或一种以上身份鉴别技术。	是□ 否□ 不适用□	
1.1.9.	以远程方式登录主机设备，是否采用两种或两种以上组合的鉴别技术进行身份鉴别。	查看安全策略文档，检查远程方式登录主机设备是否采用两种或两种以上组合的鉴别技术进行身份鉴别。	是□ 否□ 不适用□	

表 I.2　第三方存管系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
1.2.	**访问控制**			
1.2.1.	是否启用访问控制功能，依据安全策略控制用户对资源的访问。	检查重要服务器操作系统的访问控制策略，查看是否对重要文件的访问权限进行了限制，对系统不需要的服务、共享路径等进行了禁用或删除。	是□ 否□ 不适用□	
1.2.2.	是否实现操作系统和数据库系统特权用户的权限分离；HP Tandem、IBM OS400系列、运行DB2数据库的IBM AIX等专用系统的特权用户除外。	如果系统支持操作系统和数据库系统特权用户的权限分离，应检查重要数据库管理系统的特权用户和重要操作系统的特权用户，查看不同管理员的系统账户权限是否不同，且不应由同一人担任。	是□ 否□ 不适用□	
1.2.3.	是否严格限制默认账户的访问权限，重命名系统默认账户，修改这些账户的默认口令。a)系统无法修改访问权限的特殊默认账户，可不修改访问权限；b)系统无法重命名的特殊默认账户，可不重命名。	检查重要服务器操作系统的访问控制策略，查看是否已禁用或者限制匿名/默认帐户的访问权限，是否重命名系统默认帐户、修改这些帐户的默认口令。	是□ 否□ 不适用□	
1.2.4.	是否及时删除多余的、过期的账户，避免共享账户的存在。	a)检查系统中的账号是否为用户工作必须的； b)检查是否及时删除了多余的、过期的账户	是□ 否□ 不适用□	
1.2.5.	是否根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限。	如果系统支持操作系统和数据库系统特权用户的权限分离，应检查主要服务器操作系统和主要数据库管理系统的访问控制策略，查看特权用户的权限是否进行分离，如可分为系统管理员、安全管理员、安全审计员等；查看是否采用最小授权原则。	是□ 否□ 不适用□	
1.3.	**安全审计**			
1.3.1.	服务器主机的审计内容是否包括：用户的添加和删除、审计功能的启动和关闭、审计策略的调整、权限变更、系统资源的异常使用、重要的系统操作（如用户登录、退出）等。	检查审计内容是否至少包括：用户的添加和删除、审计功能的启动和关闭、审计策略的调整、权限的变更、系统资源的异常使用、重要的系统操作（如用户登录、退出）等。	是□ 否□ 不适用□	

表 I.2　第三方存管系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
1.3.2.	服务器主机的审计记录是否包括事件的日期、时间、类型、主体标识、客体标识和结果等。	检查主要服务器操作系统、重要终端操作系统的安全审计策略，查看审计记录信息是否包括事件发生的日期与时间、触发事件的主体与客体、事件的类型、事件成功或失败、事件的结果等内容。	是□ 否□ 不适用□	
1.3.3.	是否保护审计记录，避免受到未预期的删除、修改或覆盖等。审计记录是否至少保存6个月。	a)检查主要服务器操作系统、重要终端操作系统的安全审计策略，查看是否通过日志覆盖周期、存储方式、日志文件/空间大小、日志文件操作权限等设置，实现了对审计记录的保护，使其避免受到未预期的删除、修改或覆盖等； b)检查审计记录是否至少保存6个月。	是□ 否□ 不适用□	
1.3.4.	服务器主机的审计范围是否覆盖到服务器和重要客户端上的每个操作系统用户；应在保证系统运行安全和效率的前提下，启用系统审计或采用第三方安全审计产品实现审计要求。	a)检查主要服务器操作系统、重要终端操作系统和主要数据库管理系统的安全审计策略，查看安全审计配置是否包括系统内重要用户行为、系统资源的异常和重要系统命令的使用等重要的安全相关事件； b)检查是否在确保系统运行安全和效率的前提下，启用系统审计或采用第三方安全审计产品实现审计要求。	是□ 否□ 不适用□	
1.3.5.	是否能够根据记录数据进行分析，并生成审计报表。	检查主要服务器操作系统、重要终端操作系统和主要数据库管理系统的安全审计策略，查看是否为授权用户提供浏览和分析审计记录的功能，是否可以根据需要自动生成不同格式的审计报表。	是□ 否□ 不适用□	
1.4.	**安全管理**			
1.4.1.	操作系统是否遵循最小安装的原则，仅安装需要的组件和应用程序，并通过设置升级服务器等方式保持系统补丁及时得到更新。持续跟踪厂商提供的系统升级更新情况，是否在经过充分的测试评估后对必要的系统补丁进行及时更新。	a)检查主要服务器操作系统中所安装的系统组件和应用程序是否都是必须的； b)检查是否设置了专门的升级服务器实现对主要服务器操作系统补丁的升级，主要服务器操作系统是否具有操作系统补丁更新策略； c)检查是否持续跟踪厂商提供的系统升级更新情况，对关键性补丁是否进行充分的评估测试，并记录了相关评估情况和升级过程。	是□ 否□ 不适用□	

表 I.2　第三方存管系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
1.4.2.	是否能够检测到对重要服务器进行入侵的行为，能够记录入侵的源IP、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警；针对重要服务器的入侵行为检测是否通过网络级或主机级入侵检测系统等方式实现。	a)查看“表0.3-该机房的攻击防护措施”，检查入侵防范系统的入侵防范策略，查看是否能够记录对主要服务器攻击的源IP、攻击类型、攻击目标、攻击时间等，在发生严重入侵事件时是否提供报警（如声音、短信和EMAIL等）；应当同时检查入侵防范系统的特征库是否保持最新状态； b)渗透测试主要服务器操作系统和主要数据库管理系统，查看入侵防范系统是否及时正确记录了本次攻击行为，并自动报警。	是□ 否□ 不适用□	
1.4.3.	是否能够对重要程序的完整性进行检测，并在检测到完整性受到破坏后具有恢复的措施。如不能正常恢复，是否停止有关服务，并提供报警。	检查主要服务器完整性保护情况说明，确认提供对重要程序的完整性进行检测，并在检测到完整性受到破坏后具有恢复的措施的功能。	是□ 否□ 不适用□	
1.4.4.	是否对所有服务器和终端设备安装防木马、病毒等防恶意代码软件，定期进行全面检查，并及时更新防恶意代码软件版本和恶意代码库。a)原则上所有主机应安装防恶意代码软件，系统不支持该要求的除外； b) 未安装防恶意代码软件的主机，应采取有效措施进行恶意代码防范。	查看“表N03-该机房的病毒木马防护软件情况”，检查关键服务器的恶意代码防范策略，对支持安装防恶意代码软件的主机操作系统，查看是否安装了实时检测与查杀恶意代码的软件产品，并且及时更新了软件版本和恶意代码库。	是□ 否□ 不适用□	
1.4.5.	是否支持防恶意代码软件的统一管理。	a)访谈安全管理员，询问防恶意代码软件是否由专人负责进行管理和维护； b)检查主机防恶意代码软件维护记录，确认防恶意代码软件由专人统一管理。	是□ 否□ 不适用□	
1.4.6.	主机防恶意代码产品是否具有与网络防恶意代码产品不同的恶意代码库。	检查主机防恶意代码软件或硬件，查看其厂家名称、产品版本号和恶意代码库名称等，查看其是否与网络防恶意代码软件有不同的恶意代码库。	是□ 否□ 不适用□	

表 I.2　第三方存管系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
1.4.7.	是否提高所有用户的防病毒意识，告知及时升级防病毒软件，在读取移动存储设备上的数据以及网络上接收文件或邮件之前，先进行病毒检查，对外来计算机或存储设备接入网络系统之前也应进行病毒检查。	访谈系统运维负责人，询问是否对员工进行基本恶意代码防范意识的教育，是否告知应及时升级软件版本，使用外来设备、网络上接收文件和外来计算机或存储设备接入网络系统之前进行病毒检查等。	是□ 否□ 不适用□	
1.4.8.	是否定期检查主机防病毒产品的恶意代码库的升级情况并进行记录，对截获的危险病毒或恶意代码进行及时分析处理，并形成书面的报表和总结汇报。	a)询问安全管理员，主机防病毒产品的恶意代码库的升级机制； b)检查恶意代码库的升级记录，判断是否定期； c)检查恶意代码分析报告，确认对主机防病毒产品上截获的危险病毒或恶意代码进行了及时分析处理。	是□ 否□ 不适用□	
1.4.9.	是否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。	a)查看病毒扫描记录，判断是否定期对服务器进行全面病毒扫描； b)检查病毒扫描时间，确认未在交易时段内进行。	是□ 否□ 不适用□	
1.5.	**资源控制**			
1.5.1.	是否通过设定终端接入方式、网络地址范围等条件限制终端登录。	检查主要服务器操作系统的资源控制策略，查看是否设定了终端接入方式、网络地址范围等条件限制终端登录。	是□ 否□ 不适用□	
1.5.2.	是否根据安全策略设置登录终端的操作超时锁定。	a)访谈运维负责人，询问是否存在登录终端的操作超时锁定的安全策略； b)现场测试安全策略的有效性。	是□ 否□ 不适用□	
1.5.3.	是否限制单个用户对系统资源的最大或最小使用限度。	检查主要服务器操作系统和主要数据库管理系统的资源控制策略，查看是否设置了单个用户或应用对系统资源的最大或最小使用限度。	是□ 否□ 不适用□	
1.6.	**主机运维**			
1.6.1.	是否对重要服务器进行监视，包括监视服务器的CPU、硬盘、内存、网络等资源的使用情况。	查看“表0.5-系统监控情况”，检查主要服务器操作系统的资源控制策略，查看是否对CPU、硬盘、内存和网络等资源的使用情况进行监控。	是□ 否□ 不适用□	
1.6.2.	重要服务器的CPU利用率、内存、磁盘存储空间等指标超过预先规定的阈值后是否实时进行报警。	检查重要服务器监控系统的日志记录，CPU利用率、内存、磁盘存储空间等指标超过预先规定的阈值后是否实时进行报警。	是□ 否□ 不适用□	

表 I.2　第三方存管系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
1.6.3.	是否对操作系统的参数配置、调优，编制文档并保持更新。	a)访谈系统管理员，询问是否知悉其职责范围； b)检查维护记录，确认及时维修、更换故障设备和更新软件，关闭了与业务无关的服务，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； c)检查参数配置文档，确认及时对应用系统、操作系统的参数进行了配置、调优； d)检查系统容量评估报告，确认定期对系统容量进行了检查和评估。	是□ 否□ 不适用□	
2.	**系统管理**			
2.1.	**系统架构**			
2.1.1.	是否为证券交易所或登记结算机构采集客户交易终端信息提供相应的数据接口，并符合国家信息安全标准。	检查客户交易终端信息数据采集接口功能设计和验收文档，确认为证券交易所或登记结算机构采集客户交易终端信息提供相应的数据接口。	是□ 否□ 不适用□	
2.1.2.	是否提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的数据格式或长度符合系统设定要求。	a)检查设计或验收文档，查看是否有对人机接口输入或通信接口输入的数据进行有效性检验； b)测试主要应用系统，查看应用系统是否能明确拒绝不符合格式要求数据。	是□ 否□ 不适用□	
2.1.3.	是否提供自动保护功能，当故障发生时自动保护当前所有状态，保证系统能够进行恢复。	a)检查设计或验收文档，查看是否在故障发生时自动保护当前所有状态保证系统能够进行恢复的描述； b)测试主要应用系统，验证是否提供自动保护功能，当故障发生时自动保护当前所有状态，保证系统能够进行恢复。	是□ 否□ 不适用□	
2.2.	**系统建设**			
2.2.1.	在开展信息系统新建、升级、变更、换代等建设项目时，是否进行充分论证和测试，论证材料包括需求分析、立项报告等。	a)访谈信息技术负责人，询问是否在开展信息系统新建、升级、变更、换代等建设项目时，进行充分论证和测试，以及确保落实的机制； b)检查是否具有相关测试报告、论证材料（包括需求分析、立项报告等）。	是□ 否□ 不适用□	

表 I.2　第三方存管系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.2.2.	是否制定详细的工程实施方案控制实施过程，并要求工程实施单位能正式地执行安全工程过程。	a)检查系统建设方面的管理制度，查看其是否包括工程实施过程的控制方法、实施参与人员的行为准则等方面内容； b)检查工程实施方案，查看其是否包括工程时间限制、进度控制和质量控制等方面内容，是否按照工程实施方面的管理制度进行各类控制、产生阶段性文档等。	是□ 否□ 不适用□	
2.2.3.	是否向用户提供系统建设文档和运行维护所需文档。	检查系统交付提交的文档，查看是否有指导用户进行系统运维的文档等，提交的文档是否符合管理规定的要求。	是□ 否□ 不适用□	
2.2.4.	是否书面规定系统交付的控制方法和人员行为准则。	检查系统建设方面的管理制度，查看其是否包括系统交付的控制方法和人员行为准则的规定。	是□ 否□ 不适用□	
2.2.5.	是否指定专门部门管理系统交付，并按照要求完成交付工作。	访谈系统建设负责人，询问是否有专门的部门负责系统交接工作，系统交接工作是否根据交付清单对所交接的设备、文档、软件等进行清点。	是□ 否□ 不适用□	
2.2.6.	是否建立交付流程，对建成的信息系统交付运行维护的活动进行规范。	检查交付管理制度，查看交付流程是否对建成的信息系统交付运行维护的活动进行规范。	是□ 否□ 不适用□	
2.2.7.	是否制定交付工作清单，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。	检查是否具有系统交付清单，查看交付清单是否说明系统交付的各类设备、软件、文档等。	是□ 否□ 不适用□	
2.2.8.	是否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。	a)访谈系统建设负责人，询问系统正式运行前是否对运行维护人员进行过培训，针对哪些方面进行过培训； b)检查是否有系统交付技术培训记录，查看是否包括培训内容、培训时间和参与人员等。	是□ 否□ 不适用□	
2.2.9.	是否制定交付实施计划，划定交付双方的职责，交付的步骤，并对交付过程留存记录。	检查是否具有交付实施计划，查看交付实施计划是否划定交付双方的职责，交付的步骤，并对交付过程留存记录。	是□ 否□ 不适用□	
2.2.10.	是否制定信息系统备份能力建设工作计划。	检查信息技术部门是否编制了信息系统备份能力建设工作计划。	是□ 否□ 不适用□	

表 I.2 第三方存管系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.3.	**测试验收**			
2.3.1.	是否建立完整、规范的系统测试操作流程，对测试工作的计划、实施及总结做出详细的规定。对于在生产系统上进行的测试工作，必须制定详细的系统及数据备份、测试环境搭建、测试后系统及数据恢复、生产系统审核等计划，确保生产系统的安全。	检查系统测试操作流程，是否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。	是□ 否□ 不适用□	
2.3.2.	测试验收前是否根据设计方案或合同要求等制订测试验收方案，在测试验收过程中详细记录测试验收结果，并形成测试验收报告。	a)访谈系统建设负责人，询问是否根据设计方案或合同要求组织相关部门和人员制定工程测试验收方案，并对系统测试验收报告进行审定； b)检查是否具有工程测试验收方案，查看其是否明确说明参与测试的部门、人员、测试验收内容、现场操作过程等内容，过程控制是否符合管理规定的要求.	是□ 否□ 不适用□	
2.3.3.	是否组织相关部门和相关人员对系统测试验收报告进行审定，并签字确认。	检查是否具有系统测试验收报告，是否有相关部门和人员对系统测试验收报告进行审定的意见。	是□ 否□ 不适用□	
2.3.4.	是否委托第三方测试单位测试系统安全性，并出具安全性测试报告。	检查是否具有系统测试验收报告，是否有第三方测试机构的签字或盖章。	是□ 否□ 不适用□	
2.3.5.	是否书面规定系统测试验收的控制方法和人员行为准则。	检查系统建设方面的管理制度，查看其是否包括对系统测试验收的控制方法和人员行为准则规定。	是□ 否□ 不适用□	
2.3.6.	是否指定或授权专门的部门负责系统测试验收的管理，并按照管理规定的要求完成系统测试验收工作。	访谈系统建设负责人，询问是否有专门的部门负责测试验收工作，由何部门负责；是否委托第三方测试机构对信息系统进行独立的安全性测试。	是□ 否□ 不适用□	
2.3.7.	是否为系统测试配备必要的人员和设备资源，需要时协调关联单位配合测试。	访谈开发负责人，询问是否为系统测试配备必要的人员和设备资源，需要时协调关联单位配合测试。	是□ 否□ 不适用□	

表 I.2　第三方存管系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.3.8.	是否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覆盖功能、性能、容量、安全性、稳定性等方面。测试完成后对测试结果进行分析评估，并给出测试报告。	a)访谈开发负责人，询问是否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； b)检查是否具有测试方案，是否包括覆盖功能、性能、容量、安全性、稳定性等方面； c)检查近期上线系统的测试报告。	是□ 否□ 不适用□	
2.3.9.	是否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。模拟环境是否与生产环境进行有效隔离，不得对生产环境进行干扰。	检查“表 0.3-网络边界防护情况-交易业务网与模拟环境测试网络”，检查系统模拟环境逻辑架构，查看系统模拟环境在逻辑架构上是否与生产环境一致，是否与生产环境有效隔离。	是□ 否□ 不适用□	
2.3.10.	是否根据测试方案的设计，合理配置模拟环境测试所需的设备，识别设备不同可能带来的测试结果正确性风险。	a)访谈开发负责人，询问是否根据测试方案的设计，合理配置模拟环境测试所需的设备，识别设备不同可能带来的测试结果正确性风险； b)检查系统测试方案、测试报告，查看是否有设备不同可能带来的测试结果正确性风险的说明。	是□ 否□ 不适用□	
2.3.11.	是否根据需要，要求生产系统运维人员和业务部门组织业务人员参与模拟环境测试。	a)访谈开发负责人，询问是否根据需要，要求生产系统运维人员和业务部门组织业务人员参与模拟环境测试； b)查看测试通知或记录，是否有生产系统运维人员和业务部门组织业务人员参与。	是□ 否□ 不适用□	
2.3.12.	模拟环境使用的密码是否与生产系统严格区分，系统管理员宜由不同的人员担任。	访谈开发负责人，询问模拟环境使用的密码是否与生产系统严格区分，系统管理员由不同的人员担任。	是□ 否□ 不适用□	
2.3.13.	生产环境测试前是否备份当前系统的数据和配置。	a)检查系统测试管理制度和操作流程，查看数据和配置备份要求； b)抽查在生产系统上进行测试的工作记录，检查是否做好数据备份。	是□ 否□ 不适用□	
2.3.14.	是否提前发布生产环境测试的系统测试公告。	a)访谈开发负责人，询问是否提前发布生产环境测试系统测试公告； b)查看一次使用生产环境测试的测试公告。	是□ 否□ 不适用□	

表 I.2　第三方存管系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.3.15.	是否由生产系统运维人员在生产环境下组织完成生产环境测试。	a)访谈开发负责人，询问是否由生产系统运维人员在生产环境下组织完成生产环境测试； b)查看一次生产环境测试的测试方案、测试记录，是否由生产系统运维人员在生产环境下组织完成生产环境测试。	是□ 否□ 不适用□	
2.3.16.	是否根据需要，要求业务部门组织业务人员参与生产环境测试。	a)访谈开发负责人，询问是否根据需要，要求业务部门组织业务人员参与生产环境测试； b)查看一次生产环境测试的测试方案、测试记录，是否根据需要，要求业务部门组织业务人员参与生产环境测试。	是□ 否□ 不适用□	
2.3.17.	是否根据生产环境测试的结果设计系统升级过程及应急预案。	a)访谈开发负责人，询问是否根据生产环境测试的结果设计系统升级过程及应急预案； b)抽查一次生产环境测试报告和系统变更方案。	是□ 否□ 不适用□	
2.3.18.	如果生产环境测试内容涉及其他相关系统，是否协调其他系统用户参与测试。	a)访谈开发负责人，询问如果生产环境测试内容涉及其他相关系统，是否协调其他系统用户参与测试； b)抽查测试方案、测试记录，是否体现其他系统用户。	是□ 否□ 不适用□	
2.3.19.	涉及核心交易业务系统的上线测试，是否组织全市场或全公司各相关部门测试。	a)访谈开发负责人，询问涉及核心交易业务系统的上线测试，是否组织全市场或全公司各相关部门测试； b)抽查核心系统上线测试方案、测试记录，是否体现参测机构及部门。	是□ 否□ 不适用□	
2.3.20.	测试后是否恢复生产环境并验证恢复的有效性。	a)访谈开发负责人，询问测试后是否恢复生产环境并验证恢复的有效性； b)抽查测试方案、恢复验证记录。	是□ 否□ 不适用□	
2.3.21.	是否禁止交易时段使用生产环境进行测试。	a)访谈开发负责人，询问是否交易时段不得使用生产环境进行测试； b)抽查测试方案、测试记录、测试报告，查看是否在交易时段测试。	是□ 否□ 不适用□	
2.3.22.	是否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。	查看测试记录，是否在设备和软件投入使用前进行必要的验证性测试。	是□ 否□ 不适用□	

表 I.2　第三方存管系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.4.	**系统运维**			
2.4.1.	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。	a)检查运维管理制度，是否包括机房管理、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； b)检查运维操作流程，是否包括日常操作、事件处理、问题处理、系统变更、应急处置等。	是□ 否□ 不适用□	
2.4.2.	交易业务系统的操作规程是否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。	检查交易业务系统的操作规程，是否包括操作的对象、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。	是□ 否□ 不适用□	
2.4.3.	是否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进行记录留痕，记录的保存时间不少于一年。	检查一年内对交易业务系统的操作记录，是否严格按照操作手册执行运维操作。	是□ 否□ 不适用□	
2.4.4.	特殊操作、临时操作是否经批准后方可双岗执行。操作过程是否进行记录留痕，记录的保存时间是否不少于一年。	抽查公司一年内特殊操作和临时操作的记录，检查相关操作是否经过审批，是否有操作人员和复核人员签名确认。	是□ 否□ 不适用□	
2.4.5.	是否依据业务、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。	抽查修订记录，确认业务或信息系统发生重大变更时，是否对相关系统操作手册及规程进行修订并经过审批。	是□ 否□ 不适用□	
2.4.6.	是否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，是否开启自动监控系统和自动报警系统。	a)访谈运维负责人，询问是否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； b)检查巡检记录，是否包括报单数、成交数、委托数、CPU 使用率、内存使用率等指标。	是□ 否□ 不适用□	
2.4.7.	是否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。	a)访谈运维负责人，询问是否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； b)检查定期检查、评估的记录或报告，确定是否设定了预警阈值。	是□ 否□ 不适用□	

表 I.2　第三方存管系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.4.8.	主机监控指标是否包括：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。	a)检查“表 0.4-系统监控情况”，检查系统设计和验收文档，服务器监控指标是否包括设备运行状态、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； b)现场检查主机监控情况。	是□ 否□ 不适用□	
2.4.9.	存储监控指标是否包括：设备运行状态、数据交换延时、存储电池状态等。	a)检查“表 0.4-系统监控情况”，检查系统设计和验收文档，存储监控指标是否包括设备运行状态、数据交换延时、存储电池状态等； b)现场检查存储监控情况。	是□ 否□ 不适用□	
2.4.10.	数据库监控指标是否包括日志信息、表空间使用率、连接数等。	a)检查“表 0.4-系统监控情况”，检查系统设计和验收文档，数据库监控指标是否包括日志信息、表空间使用率、连接数等； b)现场检查数据库监控情况。	是□ 否□ 不适用□	
2.4.11.	核心交易业务相关的应用系统监控指标是否包括进程的活动状态、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。	a)检查“表 0.4-系统监控情况”，检查系统设计和验收文档，检查相关的应用系统监控指标，是否包括进程的活动状态、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； b)现场检查应用系统监控情况。	是□ 否□ 不适用□	
2.4.12.	是否针对不同系统设置合理的监测频度。	a)访谈运维负责人，询问是否针对不同系统设置合理的监测频度； b)查阅相关系统设置文档，是否有监测频度的说明； c)根据监测频度说明，检查相关参数设置情况。	是□ 否□ 不适用□	
2.4.13.	持续跟踪厂商提供的系统升级更新情况，是否在经过充分的测试评估后对必要的补丁进行及时更新，并在安装系统补丁前对现有的重要文件进行备份。	a)访谈系统管理员，了解系统补丁更新程序和评估方法； b)查看系统补丁更新记录，确认持续跟踪厂商提供的系统升级更新情况，确认在对重要文件进行备份后，才实施系统补丁程序的安装。	是□ 否□ 不适用□	

表 I.2　第三方存管系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.4.14.	是否依据操作手册对系统进行维护，详细记录操作日志，包括重要的日常操作、运行维护记录、参数的设置和修改等内容，严禁进行未经授权的操作。	a)访谈信息技术部门负责人和操作人员，了解对系统进行维护审批和操作步骤； b)检查运维操作手册和操作日志，确认是否包括重要的日常操作、运行维护记录、参数的设置和修改等内容，确认按照授权进行操作。	是□ 否□ 不适用□	
2.4.15.	是否保持系统的可用性，及时维修、更换故障设备和更新软件。	检查运维操作手册,是否包括保持系统的可用性，及时维修、更换故障设备和更新软件。	是□ 否□ 不适用□	
2.4.16.	是否负责应用系统的参数配置、调优，编制文档并保持更新。	检查运维操作手册,是否包括对应用系统、操作系统的参数进行配置、调优，编制文档并保持更新。	是□ 否□ 不适用□	
2.4.17.	是否定期对系统容量进行检查和评估，形成评估报告。	检查系统容量评估报告，是否定期对系统容量进行检查和评估。	是□ 否□ 不适用□	
2.4.18.	是否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。	检查运维操作手册,是否包括管理系统和应用程序服务进程，并关闭与业务无关的服务。	是□ 否□ 不适用□	
2.4.19.	是否对新上线的设备在接入运行网络前进行全面的安全检查。	a)访谈安全管理员，了解设备上线前的安全检查流程； b)查看设备上线前的漏洞扫描、渗透测试、病毒扫描、木马检测等扫描报告。	是□ 否□ 不适用□	
2.5.	**变更管理**			
2.5.1.	是否确认系统中要发生的变更，并制定相应的变更方案；重要系统变更前是否制定详细的变更方案、失败恢复方案、专项应急预案。	a)访谈系统运维负责人，询问系统变更机制或流程，是否针对系统的重大变更制定变更方案、失败恢复方案、专项应急预案； b)现场检查变更方案，抽查重要系统变更是否制定详细的变更方案、失败恢复方案、专项应急预案。	是□ 否□ 不适用□	
2.5.2.	是否建立变更控制的申报和审批文件化程序，对变更影响进行分析并文档化，记录变更实施过程，并妥善保存所有文档和记录。	检查是否有变更管理制度，查看其是否覆盖变更前审批、变更过程记录、变更后通报等方面内容，是否包括变更申报、审批程序，是否规定需要申报的变更类型、申报流程、审批部门、批准人等方面内容。	是□ 否□ 不适用□	

表 I.2　第三方存管系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.5.3.	是否建立中止变更并从失败变更中恢复的文件化程序，明确过程控制方法和人员职责，必要时对恢复过程进行演练。	检查系统变更方案，查看其是否覆盖变更类型、变更原因、变更过程、变更前评估、变更失败恢复程序等方面内容，查看其是否有主管领导的批准签字。	是□ 否□ 不适用□	
2.5.4.	是否建立系统变更流程，对信息系统的变更活动进行规范。	检查变更管理流程。	是□ 否□ 不适用□	
2.5.5.	是否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。	检查系统变更记录，系统变更中的角色是否包括申请人、审批人、实施人、复核人。	是□ 否□ 不适用□	
2.5.6.	变更申请人是否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。	检查系统变更申请，申请中是否有明确的变更方案，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。	是□ 否□ 不适用□	
2.5.7.	变更审批人是否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。	a)检查变更风险评估报告，判断变更审批人是否充分评估变更的技术风险和业务风险； b)检查变更审批记录，是否审批记录留痕并满足审计需要。	是□ 否□ 不适用□	
2.5.8.	变更审批人是否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。	检查变更审批记录，变更审批人是否确定了变更实施时间窗口，做到了除紧急变更外，不得在交易时段进行变更实施。	是□ 否□ 不适用□	
2.5.9.	是否按照测试方案，组织变更前后的测试，测试后是否提交测试记录或报告。	检查变更测试记录或报告，是否按照测试方案，组织变更前后的测试。	是□ 否□ 不适用□	
2.5.10.	变更实施人是否按照变更实施方案进行变更，并及时更新配置库。	a)检查系统变更记录，变更实施人是否按照变更实施方案进行变更； b)检查系统配置库，是否变更后及时更新配置库。	是□ 否□ 不适用□	
2.5.11.	变更复核人是否对变更记录和变更结果进行评估，评估内容是否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。	检查变更复核记录，变更复核人是否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。	是□ 否□ 不适用□	

表 I.2　第三方存管系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.6.	**安全管理**			
2.6.1.	是否建立至少每季度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。	a)访谈系统管理员，询问是否定期对系统进行漏洞扫描，扫描周期多长，发现漏洞是否及时修补，在安装系统补丁前是否对重要文件进行备份，是否先在测试环境中测试通过再安装； b)检查是否至少每季进行一次漏洞扫描，并对漏洞风险持续跟踪，在经过充分的验证测试后，对必要的漏洞开展修补工作。	是□ 否□ 不适用□	
2.7.	**身份鉴别**			
2.7.1.	是否提供专用的登录控制模块对登录用户进行身份标识和鉴别。	检查主要应用系统设计和验收文档，查看是否提供身份标识和鉴别功能。	是□ 否□ 不适用□	
2.7.2.	是否提供用户身份标识唯一和鉴别信息复杂度检查功能，保证应用系统中不存在重复用户身份标识，身份鉴别信息不易被冒用。	检查主要应用系统设计和验收文档，查看是否采用了措施保证身份标识具有唯一性，是否对登录用户的口令最小长度、复杂度和更换周期等进行了要求和限制，保证身份鉴别信息不易被冒用。	是□ 否□ 不适用□	
2.7.3.	是否提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施。	检查主要应用系统设计和验收文档，查看是否提供登录失败处理功能，是否根据安全策略设置了登录失败次数等参数。	是□ 否□ 不适用□	
2.7.4.	是否启用身份鉴别、用户身份标识唯一性检查、用户身份鉴别信息复杂度检查以及登录失败处理功能，并根据安全策略配置相关参数。	a)测试主要应用系统，可通过试图以合法和非法用户分别登录系统，验证身份标识和鉴别功能是否有效； b)测试主要应用系统，可通过多次输入错误的密码，验证登录失败处理功能是否有效； c)渗透测试主要应用系统，如多次猜测用户口令，验证应用系统身份标识和鉴别功能是否不存在明显的弱点。应当从互联网向被测试对象进行渗透测试。	是□ 否□ 不适用□	
2.7.5.	管理用户通过受控本地控制台管理应用系统时，是否采用一种或一种以上身份鉴别技术。	检查应用系统设计和验收文档，当管理用户通过受控本地控制台管理应用系统时，是否采用了一种或一种以上身份鉴别技术。	是□ 否□ 不适用□	

表 I.2　第三方存管系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.7.6.	管理用户以远程方式登录应用系统，是否采用两种或两种以上组合的鉴别技术进行身份鉴别。	检查应用系统设计和验收文档，当管理用户以远程方式登录应用系统，是否采用了两种或两种以上组合的鉴别技术进行身份鉴别。	是□ 否□ 不适用□	
2.7.7.	面向互联网服务的系统是否提供两种或两种以上组合的鉴别技术供用户选择。	检查应用系统设计和验收文档，面向互联网服务的系统是否向用户提供两种或两种以上组合的鉴别技术供用户选择。	是□ 否□ 不适用□	
2.7.8.	是否禁止设置弱口令，若系统条件允许，口令是否采用数字、字母、符号混排且无规律的方式。	检查口令管理制度，是否规定口令应采用数字、字母、符号混排且无规律的方式。	是□ 否□ 不适用□	
2.7.9.	是否禁止设置弱口令，若系统条件允许，管理员口令长度原则上不低于 12 位。	检查口令管理制度，是否规定管理员用户口令的长度至少为 12 位。	是□ 否□ 不适用□	
2.7.10.	核心交易业务系统是否提示并阻止用户使用弱口令登录。	检查核心交易业务系统设计和验收文档，确定核心交易业务系统是否提示并阻止用户使用弱口令登录。	是□ 否□ 不适用□	
2.7.11.	是否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。	检查口令管理制度，是否规定管理员用户口令至少每季度更换 1 次，更新的口令至少 5 次内不能重复。	是□ 否□ 不适用□	
2.7.12.	应用系统的账户及口令是否采用加密方式存储、传输，加密产品的使用是否符合国家有关规定。	检查口令管理制度，是否规定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。	是□ 否□ 不适用□	
2.7.13.	是否重点加强对匿名/默认用户的管理，防止被非法使用。	a)检查账户列表，是否没有匿名/默认用户； b)若有匿名/默认用户，测试是否不能被非法使用。	是□ 否□ 不适用□	
2.7.14.	是否及时注销不再使用的账户。	检查在岗人员名单和账户列表，确定没有未注销的不再使用的账户。	是□ 否□ 不适用□	
2.7.15.	是否设置抵御连续猜测等对客户账户恶意攻击行为的策略。	a)检查连续猜测等对客户账户恶意攻击行为的策略； b)现场测试系统抵御连续猜测客户账户的攻击行为。	是□ 否□ 不适用□	

表 I.2　第三方存管系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.8.	**访问控制**			
2.8.1.	是否提供访问控制和权限管理机制，依据安全策略控制用户对文件等客体的访问，防止客户的授权被恶意提升或转授，防止客户使用未经授权的功能，防止客户进行访问未经授权的数据等非法访问活动。	a)检查应用系统设计和验收文档，查看是否依据安全策略控制用户对文件等客体的访问； b)测试主要应用系统，可通过以不同权限的用户登录系统，查看其拥有的权限是否与系统赋予的权限一致，验证应用系统访问控制功能是否有效。	是□ 否□ 不适用□	
2.8.2.	访问控制的覆盖范围是否包括与资源访问相关的主体、客体及它们之间的操作。	检查应用系统设计和验收文档，查看其访问控制的覆盖范围是否包括与信息安全直接相关的主体、客体及它们之间的操作。	是□ 否□ 不适用□	
2.8.3.	是否由授权主体配置访问控制策略，并严格限制默认账户的访问权限。	a)检查应用系统设计和验收文档，查看其访问控制的覆盖范围是否包括与信息安全直接相关的主体、客体及它们之间的操作； b)测试主要应用系统，可通过以默认用户登录系统，并进行一些合法和非法操作，验证系统是否严格限制了默认帐户的访问权限。	是□ 否□ 不适用□	
2.8.4.	是否授予不同账户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系。	a)检查应用系统的用户角色或权限的分配情况，查看是否仅授予不同帐户为完成各自承担任务所需的最小权限，特权用户的权限是否分离，权限之间是否相互制约，如系统管理员不能进行审计操作、审计员不能进行系统管理操作等； b)渗透测试主要应用系统，进行试图绕过访问控制的操作，验证应用系统的访问控制功能是否不存在明显的弱点。	是□ 否□ 不适用□	
2.8.5.	是否根据业务需求和系统安全分析确定系统的访问控制策略。	a)访谈系统运维负责人，询问是否指定专门的部门或人员负责系统管理，如根据业务需求和系统安全分析制定系统的访问控制策略，控制分配文件及服务的访问权限； b)查看访问控制策略文档，判断是否根据业务需求和系统安全分析制定了系统的访问控制策略。	是□ 否□ 不适用□	

表 I.2　第三方存管系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.8.6.	是否指定专人对系统进行管理，划分系统管理员角色，明确各个角色的权限、责任和风险，权限设定是否遵循最小授权原则。	访谈系统运维负责人，询问是否对系统管理员用户进行分类，明确各个角色的权限、责任和风险，权限设定是否遵循最小授权原则。	是□ 否□ 不适用□	
2.9.	**资源控制**			
2.9.1.	用户登录应用系统后在规定的时间内未执行任何操作，是否自动退出系统。	测试主要应用系统，当应用系统的通信双方中的一方在一段时间内未作任何响应，查看另一方是否能够自动结束会话。	是□ 否□ 不适用□	
2.9.2.	是否能够对系统的最大并发会话连接数进行限制。	检查主要应用系统的配置参数，查看是否提供对最大并发会话连接数进行限制。	是□ 否□ 不适用□	
2.9.3.	是否能够对单个账户的多重并发会话进行限制。	测试主要应用系统，可通过对系统进行超过规定的单个帐户的多重并发会话数进行连接，验证系统是否能够正确地限制单个帐户的多重并发会话数。	是□ 否□ 不适用□	
2.9.4.	是否能够对一个时间段内可能的并发会话连接数进行限制。	检查主要应用系统的配置参数，查看是否提供对最大并发会话连接数进行限制。	是□ 否□ 不适用□	
2.9.5.	是否能够对一个访问账户或一个请求进程占用的资源分配最大限额和最小限额。	检查主要应用系统设计和验收文档，查看是否对一个访问帐户或一个请求进程占用的资源分配最大限额和最小限额。	是□ 否□ 不适用□	
2.9.6.	是否能够对系统服务水平降低到预先规定的最小值进行检测和报警。	a)检查主要应用系统设计和验收文档，查看是否有服务水平最小值的设定，当系统的服务水平降低到预先设定的最小值时，系统报警； b)测试主要应用系统，可试图使服务水平降低到预先规定的最小值，验证系统是否能够正确检测并报警。	是□ 否□ 不适用□	
2.9.7.	是否提供服务优先级设定功能，并在安装后根据安全策略设定访问账户或请求进程的优先级，根据优先级分配系统资源。	检查主要应用系统设计和验收文档，查看是否能根据安全策略设定主体的服务优先级，根据优先级分配系统资源。	是□ 否□ 不适用□	

表 I.2　第三方存管系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.10.	**数据安全**			
2.10.1.	通过互联网、卫星网进行通信时，是否采用密码技术保证通信过程中数据的完整性。	a)检查设计、验收文档或源代码，查看其是否有关于保护通信完整性的说明，如果有则查看是否有根据校验码判断对方数据有效性，以及散列（Hash）密码计算报文校验码的描述； b)对于通过互联网、卫星网进行通信的系统，通过截包分析，检查通信报文是否经过加密保护。	是□ 否□ 不适用□	
2.10.2.	是否能够检测到系统管理数据、鉴别信息和重要业务数据在传输过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施。	如果主要主机操作系统能够进行远程管理，则应查看应用系统的设计、验收文档或源代码，查看是否有关于能检测系统管理数据、鉴别信息和重要业务数据传输过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施的描述。	是□ 否□ 不适用□	
2.10.3.	是否采用加密或其他保护措施实现系统管理数据、鉴别信息和重要业务数据存储保密性。	检查主要应用系统设计文档，查看鉴别信息是否采用加密或其他有效措施实现存储保密性。	是□ 否□ 不适用□	
2.11.	**备份能力**			
2.11.1.	灾难应对能力是否达到《证券期货经营机构信息系统备份能力标准》第五级或重大灾难应对能力达到第六级要求。	检查“表0.8-系统备份能力”、“表0.8-数据备份情况”，查看灾难应对能力达标证明材料（包括：灾备系统建设情况、备份策略、应急演练记录等），确认灾难应对能力达到《证券期货经营机构信息系统备份能力标准》第五级或重大灾难应对能力达到第六级要求。	是□ 否□ 不适用□	
2.11.2.	重大灾难应对能力是否达到《证券期货经营机构信息系统备份能力标准》第六级要求。	检查“表0.8-系统备份能力”、“表0.8-数据备份情况”，查看灾难应对能力达标证明材料（包括：灾备系统建设情况、备份策略、应急演练记录等），确认重大灾难应对能力达到《证券期货经营机构信息系统备份能力标准》第六级要求。	是□ 否□ 不适用□	
2.11.3.	实时信息系统是否达到《证券期货经营机构信息系统备份能力标准》中故障应对能力的第四级要求。	检查“表0.8-系统备份能力”、“表0.8-数据备份情况”，检查公司实时信息系统故障应对能力达标证明材料（包括：备份系统建设情况、备份策略、应急演练记录等），确认故障应对能力达到《证券期货经营机构信息系统备份能力标准》中第四级要求。	是□ 否□ 不适用□	

表 I.2　第三方存管系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.11.4.	法人清算系统、门户网站系统等非实时信息系统是否满足《证券期货经营机构信息系统备份能力标准》中故障应对能力的第二级要求。	检查“表0.8-系统备份能力”、“表0.8-数据备份情况”，检查公司非实时信息系统故障应对能力达标证明材料（包括：备份系统建设情况、备份策略、应急演练记录等），确认法人清算系统、门户网站系统等非实时信息系统的故障应对能力达到《证券期货经营机构信息系统备份能力标准》中故障应对能力的第二级要求。	是□ 否□ 不适用□	
2.12.	**安全审计**			
2.12.1.	应用系统是否能够对每个业务用户的关键操作进行记录，例如用户登录、用户退出、增加用户、修改用户权限等操作。	a)检查主要应用系统，查看审计范围是否覆盖到每个用户，审计策略是否覆盖系统内重要的安全相关事件，例如，用户标识与鉴别、访问控制的所有操作记录、重要用户行为、系统资源的异常使用、重要系统命令的使用等； b)测试主要应用系统，在应用系统上试图产生一些重要的安全相关事件（如进行用户登录、修改用户权限等操作），查看应用系统是否对其进行了审计，验证应用系统安全审计的覆盖情况是否覆盖到每个用户；如果进行了审计则查看审计记录内容是否包含事件的日期、时间、发起者信息、类型、描述和结果等。	是□ 否□ 不适用□	
2.12.2.	审计记录的内容是否包括事件日期、时间、发起者信息、类型、描述和结果等。审计记录是否至少保存6个月。	检查主要应用系统的审计记录，查看是否包括事件发生的日期与时间、触发事件的主体与客体、事件的类型、事件成功或失败、身份鉴别事件中请求的来源、事件的结果等内容；检查是否保存了6个月以上的审计记录。	是□ 否□ 不适用□	
2.12.3.	是否采取有效措施防止单独中断审计进程；审计进程应作为应用系统整体进程中的一部分，并且不能单独中断。	测试主要应用系统，试图非授权终止审计进程或审计功能，删除、修改或覆盖审计记录，查看安全审计进程和记录的保护情况。	是□ 否□ 不适用□	
2.12.4.	是否提供对审计记录数据进行统计、查询、分析及生成审计报表的功能。	检查主要应用系统，查看是否为授权用户浏览和分析审计数据提供专门的审计分析功能，并能根据需要生成审计报表。	是□ 否□ 不适用□	

表 I.2　第三方存管系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.12.5.	是否保证信息系统日志的完备性，确保所有重大修改被完整地记录，确保开启审计留痕功能。证券公司信息系统日志是否至少保存 15 年。	a)检查运维管理制度，是否规定保证信息系统日志的完备性，确保所有重大修改被完整地记录，信息系统日志是否至少保存 15 年； b)检查系统设计和验收文档，是否开启审计留痕功能。	是□ 否□ 不适用□	
2.12.6.	是否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。	查看每日检查记录，是否指定人员按照运维管理制度和操作流程，对日常操作执行情况进行每日检查。	是□ 否□ 不适用□	
2.12.7.	是否每季组织开展内部检查，形成检查报告。	审阅内部检查报告，检查是否每季度一次。	是□ 否□ 不适用□	
2.12.8.	是否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。	a)审阅公司年度审计计划，是否包含信息系统运维管理工作审计项目； b)检查公司年度审计报告，是否包含信息系统运维管理工作审计项目。	是□ 否□ 不适用□	
2.12.9.	检查和审计范围是否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。	检查信息系统运维管理工作审计报告，确定信息系统运维管理工作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。	是□ 否□ 不适用□	
2.12.10.	是否对检查和审计的结果采取纠正性和预防性的措施。	审阅信息系统运维管理工作审计整改报告，确定是否对检查和审计的结果采取纠正性和预防性的措施。	是□ 否□ 不适用□	
2.12.11.	是否定期检查安全隔离情况，确保各安全域之间有效隔离。	a)查看包括自建和托管机房的网络拓扑图、安全域划分情况，检查各安全域之间是否采用了防火墙或安全网关等有效隔离方式和隔离手段； b)审阅最近的网络隔离情况检查报告，判断是否定期对上述事项进行了检查。	是□ 否□ 不适用□	

表 I.2　第三方存管系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.12.12.	是否组织相关人员定期对监测和报警记录进行分析、评审，发现可疑行为，形成分析报告，并采取必要的应对措施。	a)访谈系统运维负责人，询问其是否组织人员定期对监测记录进行分析、评审，是否发现可疑行为并对其采取必要的措施，是否形成分析报告； b)检查监测记录，查看是否记录监控对象、监控内容、监控的异常现象处理等方面，查看是否对异常现象及处理措施形成分析报告。	是□ 否□ 不适用□	
2.12.13.	是否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。	检查是否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，以满足审计的需要。	是□ 否□ 不适用□	
2.12.14.	是否保存监控产生的日志，保存时间不少于一年。	检查监控日志，保存时间是否不少于一年。	是□ 否□ 不适用□	
2.12.15.	是否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。	查看评估记录，是否每日分析核心交易业务系统监控日志及巡检记录，并跟踪处理日志分析中发现的异常事件。	是□ 否□ 不适用□	
2.12.16.	是否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。	查看评估报告，是否至少每季度全面评估监控日志和操作记录，分析异常情况。	是□ 否□ 不适用□	
2.12.17.	是否至少每月对运行日志和审计数据进行分析。	检查是否每月对运行日志和审计数据进行分析。	是□ 否□ 不适用□	
3.	**数据库管理**			
3.1.	**安全审计**			
3.1.1.	审计内容是否至少包括：用户的添加和删除、审计功能的启动和关闭、审计策略的调整、权限变更、系统资源的异常使用、重要的系统操作（如用户登录、退出）等。	审阅主机审计记录，检查审计内容是否包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件；审计内容至少包括：用户的添加和删除、审计功能的启动和关闭、审计策略的调整、权限变更、系统资源的异常使用、重要的系统操作（如用户登录、退出）等。	是□ 否□ 不适用□	
3.1.2.	审计记录是否包括事件的日期、时间、类型、主体标识、客体标识和结果等。	审阅主机运行日志，检查审计记录是否包括事件的日期、时间、类型、主体标识、客体标识和结果等。	是□ 否□ 不适用□	

表 I.2　第三方存管系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
3.1.3.	是否保护审计记录，避免受到未预期的删除、修改或覆盖等。审计记录是否至少保存6个月。	检查审计记录是否至少保存 6 个月。	是□ 否□ 不适用□	
3.1.4.	审计范围是否覆盖到服务器和重要客户端上的每个数据库用户；应在保证系统运行安全和效率的前提下，启用系统审计或采用第三方安全审计产品实现审计要求。	a)通过访谈，了解是否在保证系统运行安全和效率的前提下，启用了系统审计或采用第三方安全审计产品实现审计要求，保证产生、有效记录和存储了审计日志； b)通过访谈，审阅主机和客户端审计记录，判断是否覆盖到服务器和重要客户端上的每个操作系统用户和数据库用户。	是□ 否□ 不适用□	
3.1.5.	是否能够根据记录数据进行分析，并生成审计报表。	检查主要服务器操作系统、重要终端操作系统和主要数据库管理系统的安全审计策略，查看是否为授权用户提供浏览和分析审计记录的功能，是否可以根据需要自动生成不同格式的审计报表。	是□ 否□ 不适用□	
3.1.6.	是否保护审计进程，避免受到未预期的中断。	测试主要服务器操作系统、重要终端操作系统和主要数据库管理系统，可通过非审计员的其他帐户试图中断审计进程，验证审计进程是否受到保护。	是□ 否□ 不适用□	
3.2.	**访问控制**			
3.2.1.	是否严格限制人工对数据库操作的账户权限，并分别使用不同权限的账户执行查询、插入、更新、删除等操作。	a)查看数据库账户权限管理制度，是否规定分别使用不同权限的账户执行查询、插入、更新、删除等操作； b)检查对数据库进行人工操作的记录，确认使用不同权限的账户执行查询、插入、更新、删除等操作。	是□ 否□ 不适用□	
3.3.	**身份鉴别**			
3.3.1.	口令是否符合以下条件：数字、字母、符号混排，无规律的方式。	检查口令管理制度，是否规定口令符合以下条件：数字、字母、符号混排，无规律的方式。	是□ 否□ 不适用□	
3.3.2.	口令的长度是否至少为 12 位。	检查口令管理制度，是否规定管理员用户口令的长度至少为 12 位。	是□ 否□ 不适用□	
3.3.3.	口令是否至少每季度更换1次，更新的口令至少 5 次内不能重复。	检查口令管理制度，是否规定管理员用户口令至少每季度更换 1 次，更新的口令至少 5 次内不能重复。	是□ 否□ 不适用□	

表 I.2　第三方存管系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
3.3.4.	如果设备口令长度不支持12位或其他复杂度要求，口令是否使用所支持的最长长度并适当缩小更换周期；也可以使用动态密码卡等一次性口令认证方式。	检查口令管理制度，是否规定口令应使用所支持的最长长度并适当缩小更换周期，也可以使用动态密码卡等一次性口令认证方式。	是□ 否□ 不适用□	
3.3.5.	是否为数据库系统的不同用户分配不同的用户名，确保用户名具有唯一性。	检查数据库系统的用户列表，标识是否唯一。	是□ 否□ 不适用□	
3.4.	**数据库运维**			
3.4.1.	是否保持数据库的可用性，及时维护、更新软件。	a)查看数据库软件、数据库监控软件的采购合同，以及维护、更新记录； b)查看数据库监控日志，判断表空间使用率、连接数等是否保持在合理范围。	是□ 否□ 不适用□	
3.4.2.	是否对数据库的参数进行配置、调优，编制文档并保持更新。	a)访谈数据库管理员,询问是否依照数据库配置文档进行安装、配置及调优； b)查看数据库配置文档和维护记录，确认对数据库系统进行了配置、调优。	是□ 否□ 不适用□	
3.4.3.	是否定期对数据库容量进行检查和评估，形成评估报告。	a)查看公司数据库容量管理制度，是否明确要求定期对数据库系统容量进行检查和评估，并形成评估报告； b)访谈数据库管理员，查看数据库容量评估报告，确认定期对数据库容量进行了检查和评估。	是□ 否□ 不适用□	
3.4.4.	是否管理数据库、表、索引、存储过程，数据库的升级、优化、扩容、迁移。	a)查看公司数据库容量管理制度，是否明确数据库管理员应负责管理数据库、表、索引、存储过程，数据库的升级、优化、扩容、迁移； b)访谈数据库管理员，查看数据库维护记录，确认数据库管理员按照要求管理数据库、表、索引、存储过程，对数据库进行了升级、优化、扩容、迁移等维护工作。	是□ 否□ 不适用□	
3.4.5.	是否定期检查数据库的用户、口令及权限设置的正确性。	访谈数据库管理员，查看数据库维护记录，确认是否定期检查数据库的用户、口令及权限设置的正确性。	是□ 否□ 不适用□	

表 I.2　第三方存管系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
4.	**第三方存管系统**			
4.1.	**结构安全**			
4.1.1.	第三方存管系统的日处理能力是否达到最近一年内银证转账最大日处理量的 5 倍以上。	查看“表 0.5-系统处理能力-压力测试日处理最大银证转账笔数(万笔)/本年度最大日处理银证转账笔数（万笔）/压力测试日处理最大银证查询笔数（万笔）/本年度最大日处理银证查询笔数（万笔)”，计算本年度银证转账、银证查询的压力测试最大数与日处理最大数的比值，确定是否结果大于 5。	是□ 否□ 不适用□	
4.1.2.	第三方存管系统全年实际可用性是否达到 99.9%。	查看“表 0.5-系统处理能力-本年度交易中断、严重缓慢总时长（分钟)”，计算第三方存管系统全年实际可用性是否达到 99.9%。	是□ 否□ 不适用□	
4.1.3.	各参与方第三方存管系统的前置机、加密设备、网络设备等硬件设备是否有冗余备份，当出现故障时，是否能在 30 分钟内完成备用设备的切换。	a)审阅资源数据，确认硬件设备有冗余备份,且能在 30 分钟完成备用设备切换； b)审阅第三方存管系统应急演练记录，确认可在 30 分钟内实现故障设备切换。	是□ 否□ 不适用□	
4.2.	**数据安全**			
4.2.1.	第三方存管系统数据交换机制是否支持报文校验、动态密钥交换、数字签名等安全措施。	a)访谈安全管理员或技术开发人员，了解第三方存管系统的数据交换机制是否支持报文校验、动态密钥交换、数字签名等安全措施； b)检查安全测试记录和银证转账系统，确认采取了报文校验、动态密钥交换、数字签名等安全措施保障银证转账安全。	是□ 否□ 不适用□	
4.3.	**网络通信**			
4.3.1.	与相关商业银行之间的第三方存管系统对接是否遵循总对总的原则，联接线路既可以采用银证直联，也可以通过相关中介服务机构进行联接。	审阅证券公司与银行的连接情况相关文档，确认与银行连接是否为总对总模式，联接线路既可以采用银证直联，也可以通过相关中介服务机构进行联接。	是□ 否□ 不适用□	
4.4.	**系统运维**			
4.4.1.	各参与方需要进行第三方存管系统联调或升级时，是否提前至少 5 个工作日通知相关参与方。	检查第三方存管系统维护变更记录，判断在第三方存管系统联调或升级时，是否提前至少 5 个工作日通知相关参与方。	是□ 否□ 不适用□	

表 I.2　第三方存管系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
4.4.2.	各参与方对第三方存管系统提出重大的新业务或管理需求时，是否为相关参与方留有充足的技术准备时间，原则上不少于 30 个工作日。	检查第三方存管系统维护变更记录或需求变更记录，判断对第三方存管系统提出重大的新业务或管理需求时，是否为相关参与方留有充足的技术准备时间，原则上不少于 30 个工作日。	是□ 否□ 不适用□	
4.4.3.	各相关参与方之间是否相互提供与第三方存管系统相关的信息，包括但不限于：广域网接入设备及端口类型、相关网络拓扑结构及必要参数、主机类型与配置、相关系统参数、技术接口协议、系统运行性能测试报告、主要应急预案及相关联系人等。	检查向银行、电信运营商等相关参与方提供的与第三方存管系统相关的材料，是否包括：广域网接入设备及端口类型、相关网络拓扑结构及必要参数、主机类型与配置、相关系统参数、技术接口协议、系统运行性能测试报告、主要应急预案及相关联系人等。	是□ 否□ 不适用□	
4.4.4.	是否在对相关网络及设备做重大变更时提前告知相关参与方，以免对方运行监控人采取不必要的操作。	检查对相关网络及设备做重大变更时提前告知相关参与方的通知等，判断是否提前告知相关参与方。	是□ 否□ 不适用□	
4.4.5.	各参与方在进行日终清算文件交换时，是否对日终清算文件的合法性和完整性进行校验。	a)访谈清算人员或开发维护人员，了解清算文件校验流程，确认对日终清算文件进行了合法性和完整性校验； b)现场观察日终清算文件校验过程，是否按照流程和方法执行。	是□ 否□ 不适用□	
4.5.	**应急处置**			
4.5.1.	日终清算数据送达商业银行的时间要求为：非结息日的截止时间为次日凌晨 2:00，结息日的截止时间为次日凌晨 3:00。如需延迟，是否提前至少一小时通知商业银行。	a)现场检查证券公司向商业银行传送日终清算数据的操作日志记录，确认传送时间是否符合规定要求； b)检查传送延时与商业银行的通知，如需延迟，是否提前至少一小时通知商业银行。	是□ 否□ 不适用□	
4.5.2.	各参与方如果因网络故障等原因，无法通过第三方存管系统自动传送日终清算数据到相关参与方，是否及时通知对方，并以其他方式将数据及时送达对方。	a)检查第三方存管业务涉及的应急处置管理制度，是否建立应急沟通处置机制； b)现场检查证券公司无法通过系统向商业银行传送日终清算数据时的操作记录，确认以其他方式及时传送并通知了对方； c)现场检查商业银行无法通过系统向证券公司传送日终清算数据时的操作记录，确认以其他方式及时传送并通知对方。	是□ 否□ 不适用□	

表 I.2　第三方存管系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
4.5.3.	第三方存管各参与方是否建立并完善内部责任机制和协调机制，坚持信息安全事故问责制度，做好自动留痕和书面留痕工作，以便于责任事故的认定。	a)审阅第三方存管系统故障处理流程，是否对各参与方的责任与协调方式进行了明确规定； b)审阅第三方存管系统故障的自动留痕和书面留痕记录，确认故障记录的完整性。	是□ 否□ 不适用□	
4.6	**系统托管**			
4.6.1	二级系统托管是否满足《证券期货业信息系统托管基本要求》（JR/T 0133-2015)的相关要求。	检查托管服务合同和相关文档，确认按照信息安全等级保护二级要求进行定级的系统选购了二级系统托管服务。	是□ 否□ 不适用□	
4.6.2	三级系统托管是否满足《证券期货业信息系统托管基本要求》（JR/T 0133-2015)的相关要求。	检查托管服务合同和相关文档，确认按照信息安全等级保护三级要求进行定级的系统选购了三级系统托管服务。	是□ 否□ 不适用□	
4.6.3	未定级系统托管是否满足《证券期货业信息系统托管基本要求》（JR/T 0133-2015)的相关要求。	检查托管服务合同和相关文档，确认未进行信息安全等级保护定级备案的信息系统选购了二级系统托管服务。	是□ 否□ 不适用□	

附 录 J
（规范性附录）
重要信息系统审计底稿

表J.1至表J.2给出了重要信息系统审计的程序、内容及相关记录要求。

表J.1 重要信息系统审计底稿

<table>
<tr><td>被审计部门：</td><td>索引号：ZYXT</td></tr>
<tr><td>审计主题：重要系统</td><td>审计年度：</td></tr>
<tr><td colspan="2">审计结论、意见及建议：

编制人：
年 月 日
（部门盖章）</td></tr>
<tr><td colspan="2">复核意见：

复核人：
年 月 日
（部门盖章）</td></tr>
<tr><td colspan="2">被审计部门意见：

年 月 日
（部门盖章）</td></tr>
</table>

表 J.1　重要信息系统审计底稿（续）

审计证据列表：

表J.2　重要信息系统审计底稿

序号	审计项	审计程序	审计结论	备注
1	**主机管理**			
1.1.	**身份鉴别**			
1.1.1.	操作系统管理员口令是否符合以下条件：数字、字母、符号混排，无规律的方式。	检查口令管理制度，是否规定口令符合以下条件：数字、字母、符号混排，无规律的方式。	是□ 否□ 不适用□	
1.1.2.	操作系统管理员口令的长度是否为12位。	检查口令管理制度，是否规定管理员用户口令的长度至少为12位。	是□ 否□ 不适用□	
1.1.3.	操作系统管理员口令是否每季度更换1次，更新的口令至少5次内不能重复。	检查口令管理制度，是否规定管理员用户口令至少每季度更换1次，更新的口令至少5次内不能重复。	是□ 否□ 不适用□	
1.1.4.	如果受限于操作系统，使得管理员口令长度不支持12位或其他复杂度要求，口令是否使用所支持的最长长度并适当缩小更换周期；也可以使用动态密码卡等一次性口令认证方式。	检查口令管理制度，是否规定如果设备口令长度不支持12位或其他复杂度要求，口令应使用所支持的最长长度并适当缩小更换周期，也可以使用动态密码卡等一次性口令认证方式。	是□ 否□ 不适用□	
1.1.5.	是否启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施。	a)检查重要服务器操作系统的身份鉴别策略，查看是否配置了登录失败处理功能、设置了非法登录次数的限制值； b)查看是否设置网络登录连接超时，并自动退出。	是□ 否□ 不适用□	
1.1.6.	当对服务器进行远程管理时，是否采取必要措施，防止鉴别信息在网络传输过程中被窃听。	查看“表0.13附表一-信息系统名称”、“表0.13附表一-本系统中密码机使用情况”，访谈系统管理员，询问是否对操作系统采用了远程管理方式，如果采用远程管理方式，查看是否具有防止鉴别信息在网络传输过程中被窃听的措施。	是□ 否□ 不适用□	
1.1.7.	是否为操作系统的不同用户分配不同的用户名，确保用户名具有唯一性。	检查操作系统的用户列表，标识是否唯一，或采取堡垒机等措施。	是□ 否□ 不适用□	
1.1.8.	通过本地控制台管理主机设备时，是否采用一种或一种以上身份鉴别技术。	查看安全策略文档，检查本地控制台管理主机设备是否采用一种或一种以上身份鉴别技术。	是□ 否□ 不适用□	
1.1.9.	以远程方式登录主机设备，是否采用两种或两种以上组合的鉴别技术进行身份鉴别。	查看安全策略文档，检查远程方式登录主机设备是否采用两种或两种以上组合的鉴别技术进行身份鉴别。	是□ 否□ 不适用□	

表 J.2　重要信息系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
1.2.	**访问控制**			
1.2.1.	是否启用访问控制功能，依据安全策略控制用户对资源的访问。	检查重要服务器操作系统的访问控制策略，查看是否对重要文件的访问权限进行了限制，对系统不需要的服务、共享路径等进行了禁用或删除。	是□ 否□ 不适用□	
1.2.2.	是否实现操作系统和数据库系统特权用户的权限分离；HP Tandem、IBM OS400系列、运行DB2数据库的IBM AIX等专用系统的特权用户除外。	如果系统支持操作系统和数据库系统特权用户的权限分离，应检查重要数据库管理系统的特权用户和重要操作系统的特权用户，查看不同管理员的系统账户权限是否不同，且不应由同一人担任。	是□ 否□ 不适用□	
1.2.3.	是否严格限制默认账户的访问权限，重命名系统默认账户，修改这些账户的默认口令。a)系统无法修改访问权限的特殊默认账户，可不修改访问权限；b)系统无法重命名的特殊默认账户，可不重命名。	检查重要服务器操作系统的访问控制策略，查看是否已禁用或者限制匿名/默认帐户的访问权限，是否重命名系统默认帐户、修改这些帐户的默认口令。	是□ 否□ 不适用□	
1.2.4.	是否及时删除多余的、过期的账户，避免共享账户的存在。	a)检查系统中的账号是否为用户工作必须的； b)检查是否及时删除了多余的、过期的账户	是□ 否□ 不适用□	
1.2.5.	是否根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限。	如果系统支持操作系统和数据库系统特权用户的权限分离，应检查主要服务器操作系统和主要数据库管理系统的访问控制策略，查看特权用户的权限是否进行分离，如可分为系统管理员、安全管理员、安全审计员等；查看是否采用最小授权原则。	是□ 否□ 不适用□	
1.3.	**安全审计**			
1.3.1.	服务器主机的审计内容是否包括：用户的添加和删除、审计功能的启动和关闭、审计策略的调整、权限变更、系统资源的异常使用、重要的系统操作（如用户登录、退出）等。	检查审计内容是否至少包括：用户的添加和删除、审计功能的启动和关闭、审计策略的调整、权限的变更、系统资源的异常使用、重要的系统操作（如用户登录、退出）等。	是□ 否□ 不适用□	

表 J.2　重要信息系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
1.3.2.	服务器主机的审计记录是否包括事件的日期、时间、类型、主体标识、客体标识和结果等。	检查主要服务器操作系统、重要终端操作系统的安全审计策略，查看审计记录信息是否包括事件发生的日期与时间、触发事件的主体与客体、事件的类型、事件成功或失败、事件的结果等内容。	是□ 否□ 不适用□	
1.3.3.	是否保护审计记录，避免受到未预期的删除、修改或覆盖等。审计记录是否至少保存6个月。	a)检查主要服务器操作系统、重要终端操作系统的安全审计策略，查看是否通过日志覆盖周期、存储方式、日志文件/空间大小、日志文件操作权限等设置，实现了对审计记录的保护，使其避免受到未预期的删除、修改或覆盖等； b)检查审计记录是否至少保存6个月。	是□ 否□ 不适用□	
1.3.4.	服务器主机的审计范围是否覆盖到服务器和重要客户端上的每个操作系统用户；应在保证系统运行安全和效率的前提下，启用系统审计或采用第三方安全审计产品实现审计要求。	a)检查主要服务器操作系统、重要终端操作系统和主要数据库管理系统的安全审计策略，查看安全审计配置是否包括系统内重要用户行为、系统资源的异常和重要系统命令的使用等重要的安全相关事件； b)检查是否在确保系统运行安全和效率的前提下，启用系统审计或采用第三方安全审计产品实现审计要求。	是□ 否□ 不适用□	
1.3.5.	是否能够根据记录数据进行分析，并生成审计报表。	检查主要服务器操作系统、重要终端操作系统和主要数据库管理系统的安全审计策略，查看是否为授权用户提供浏览和分析审计记录的功能，是否可以根据需要自动生成不同格式的审计报表。	是□ 否□ 不适用□	
1.4.	**安全管理**			
1.4.1.	操作系统是否遵循最小安装的原则，仅安装需要的组件和应用程序，并通过设置升级服务器等方式保持系统补丁及时得到更新。持续跟踪厂商提供的系统升级更新情况，是否在经过充分的测试评估后对必要的系统补丁进行及时更新。	a)检查主要服务器操作系统中所安装的系统组件和应用程序是否都是必须的； b)检查是否设置了专门的升级服务器实现对主要服务器操作系统补丁的升级，主要服务器操作系统是否具有操作系统补丁更新策略； c)检查是否持续跟踪厂商提供的系统升级更新情况，对关键性补丁是否进行充分的评估测试，并记录了相关评估情况和升级过程。	是□ 否□ 不适用□	

表 J.2 重要信息系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
1.4.2.	是否能够检测到对重要服务器进行入侵的行为，能够记录入侵的源IP、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警；针对重要服务器的入侵行为检测是否通过网络级或主机级入侵检测系统等方式实现。	a)查看“表0.3-该机房的攻击防护措施”，检查入侵防范系统的入侵防范策略，查看是否能够记录对主要服务器攻击的源IP、攻击类型、攻击目标、攻击时间等，在发生严重入侵事件时是否提供报警（如声音、短信和EMAIL等）；应当同时检查入侵防范系统的特征库是否保持最新状态； b)渗透测试主要服务器操作系统和主要数据库管理系统，查看入侵防范系统是否及时正确记录了本次攻击行为，并自动报警。	是□ 否□ 不适用□	
1.4.3.	是否能够对重要程序的完整性进行检测，并在检测到完整性受到破坏后具有恢复的措施。如不能正常恢复，是否停止有关服务，并提供报警。	检查主要服务器完整性保护情况说明，确认提供对重要程序的完整性进行检测，并在检测到完整性受到破坏后具有恢复的措施的功能。	是□ 否□ 不适用□	
1.4.4.	是否对所有服务器和终端设备安装防木马、病毒等防恶意代码软件，定期进行全面检查，并及时更新防恶意代码软件版本和恶意代码库。a)原则上所有主机应安装防恶意代码软件，系统不支持该要求的除外； b) 未安装防恶意代码软件的主机，应采取有效措施进行恶意代码防范。	查看“表N03-该机房的病毒木马防护软件情况”，检查关键服务器的恶意代码防范策略，对支持安装防恶意代码软件的主机操作系统，查看是否安装了实时检测与查杀恶意代码的软件产品，并且及时更新了软件版本和恶意代码库。	是□ 否□ 不适用□	
1.4.5.	是否支持防恶意代码软件的统一管理。	a)访谈安全管理员，询问防恶意代码软件是否由专人负责进行管理和维护； b)检查主机防恶意代码软件维护记录，确认防恶意代码软件由专人统一管理。	是□ 否□ 不适用□	
1.4.6.	主机防恶意代码产品是否具有与网络防恶意代码产品不同的恶意代码库。	检查主机防恶意代码软件或硬件，查看其厂家名称、产品版本号和恶意代码库名称等，查看其是否与网络防恶意代码软件有不同的恶意代码库。	是□ 否□ 不适用□	

表 J.2　重要信息系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
1.4.7.	是否提高所有用户的防病毒意识，告知及时升级防病毒软件，在读取移动存储设备上的数据以及网络上接收文件或邮件之前，先进行病毒检查，对外来计算机或存储设备接入网络系统之前也应进行病毒检查。	访谈系统运维负责人，询问是否对员工进行基本恶意代码防范意识的教育，是否告知应及时升级软件版本，使用外来设备、网络上接收文件和外来计算机或存储设备接入网络系统之前进行病毒检查等。	是□ 否□ 不适用□	
1.4.8.	是否定期检查主机防病毒产品的恶意代码库的升级情况并进行记录，对截获的危险病毒或恶意代码进行及时分析处理，并形成书面的报表和总结汇报。	a)询问安全管理员，主机防病毒产品的恶意代码库的升级机制； b)检查恶意代码库的升级记录，判断是否定期； c)检查恶意代码分析报告，确认对主机防病毒产品上截获的危险病毒或恶意代码进行了及时分析处理。	是□ 否□ 不适用□	
1.4.9.	是否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。	a)查看病毒扫描记录，判断是否定期对服务器进行全面病毒扫描； b)检查病毒扫描时间，确认未在交易时段内进行。	是□ 否□ 不适用□	
1.5.	**资源控制**			
1.5.1.	是否通过设定终端接入方式、网络地址范围等条件限制终端登录。	检查主要服务器操作系统的资源控制策略，查看是否设定了终端接入方式、网络地址范围等条件限制终端登录。	是□ 否□ 不适用□	
1.5.2.	是否根据安全策略设置登录终端的操作超时锁定。	a)访谈运维负责人，询问是否存在登录终端的操作超时锁定的安全策略； b)现场测试安全策略的有效性。	是□ 否□ 不适用□	
1.5.3.	是否限制单个用户对系统资源的最大或最小使用限度。	检查主要服务器操作系统和主要数据库管理系统的资源控制策略，查看是否设置了单个用户或应用对系统资源的最大或最小使用限度。	是□ 否□ 不适用□	
1.6.	**主机运维**			
1.6.1.	是否对重要服务器进行监视，包括监视服务器的CPU、硬盘、内存、网络等资源的使用情况。	查看“表0.8-系统监控情况”，检查主要服务器操作系统的资源控制策略，查看是否对CPU、硬盘、内存和网络等资源的使用情况进行监控。	是□ 否□ 不适用□	
1.6.2.	重要服务器的CPU利用率、内存、磁盘存储空间等指标超过预先规定的阈值后是否实时进行报警。	检查重要服务器监控系统的日志记录，CPU利用率、内存、磁盘存储空间等指标超过预先规定的阈值后是否实时进行报警。	是□ 否□ 不适用□	

表 J.2　重要信息系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
1.6.3.	是否对操作系统的参数配置、调优，编制文档并保持更新。	a)访谈系统管理员，询问是否知悉其职责范围； b)检查维护记录，确认及时维修、更换故障设备和更新软件，关闭了与业务无关的服务，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； c)检查参数配置文档，确认及时对应用系统、操作系统的参数进行了配置、调优； d)检查系统容量评估报告，确认定期对系统容量进行了检查和评估。	是□ 否□ 不适用□	
2.	**系统管理**			
2.1.	**系统架构**			
2.1.1.	是否为证券交易所或登记结算机构采集客户交易终端信息提供相应的数据接口，并符合国家信息安全标准。	检查客户交易终端信息数据采集接口功能设计和验收文档，确认为证券交易所或登记结算机构采集客户交易终端信息提供相应的数据接口。	是□ 否□ 不适用□	
2.1.2.	是否提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的数据格式或长度符合系统设定要求。	a)检查设计或验收文档，查看是否有对人机接口输入或通信接口输入的数据进行有效性检验； b)测试主要应用系统，查看应用系统是否能明确拒绝不符合格式要求数据。	是□ 否□ 不适用□	
2.1.3.	是否提供自动保护功能，当故障发生时自动保护当前所有状态，保证系统能够进行恢复。	a)检查设计或验收文档，查看是否在故障发生时自动保护当前所有状态保证系统能够进行恢复的描述； b)测试主要应用系统，验证是否提供自动保护功能，当故障发生时自动保护当前所有状态，保证系统能够进行恢复。	是□ 否□ 不适用□	
2.2.	**系统建设**			
2.2.1.	在开展信息系统新建、升级、变更、换代等建设项目时，是否进行充分论证和测试，论证材料包括需求分析、立项报告等。	a)访谈信息技术负责人，询问是否在开展信息系统新建、升级、变更、换代等建设项目时，进行充分论证和测试，以及确保落实的机制； b)检查是否具有相关测试报告、论证材料（包括需求分析、立项报告等）。	是□ 否□ 不适用□	

表 J.2　重要信息系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.2.2.	是否制定详细的工程实施方案控制实施过程，并要求工程实施单位能正式地执行安全工程过程。	a)检查系统建设方面的管理制度，查看其是否包括工程实施过程的控制方法、实施参与人员的行为准则等方面内容； b)检查工程实施方案，查看其是否包括工程时间限制、进度控制和质量控制等方面内容，是否按照工程实施方面的管理制度进行各类控制、产生阶段性文档等。	是□ 否□ 不适用□	
2.2.3.	是否向用户提供系统建设文档和运行维护所需文档。	检查系统交付提交的文档，查看是否有指导用户进行系统运维的文档等，提交的文档是否符合管理规定的要求。	是□ 否□ 不适用□	
2.2.4.	是否书面规定系统交付的控制方法和人员行为准则。	检查系统建设方面的管理制度，查看其是否包括系统交付的控制方法和人员行为准则的规定。	是□ 否□ 不适用□	
2.2.5.	是否指定专门部门管理系统交付，并按照要求完成交付工作。	访谈系统建设负责人，询问是否有专门的部门负责系统交接工作，系统交接工作是否根据交付清单对所交接的设备、文档、软件等进行清点。	是□ 否□ 不适用□	
2.2.6.	是否建立交付流程，对建成的信息系统交付运行维护的活动进行规范。	检查交付管理制度，查看交付流程是否对建成的信息系统交付运行维护的活动进行规范。	是□ 否□ 不适用□	
2.2.7.	是否制定交付工作清单，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。	检查是否具有系统交付清单，查看交付清单是否说明系统交付的各类设备、软件、文档等。	是□ 否□ 不适用□	
2.2.8.	是否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。	a)访谈系统建设负责人，询问系统正式运行前是否对运行维护人员进行过培训，针对哪些方面进行过培训； b)检查是否有系统交付技术培训记录，查看是否包括培训内容、培训时间和参与人员等。	是□ 否□ 不适用□	
2.2.9.	是否制定交付实施计划，划定交付双方的职责，交付的步骤，并对交付过程留存记录。	检查是否具有交付实施计划，查看交付实施计划是否划定交付双方的职责，交付的步骤，并对交付过程留存记录。	是□ 否□ 不适用□	
2.2.10.	是否制定信息系统备份能力建设工作计划。	检查信息技术部门是否编制了信息系统备份能力建设工作计划。	是□ 否□ 不适用□	

表 J.2　重要信息系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.3.	**测试验收**			
2.3.1.	是否建立完整、规范的系统测试操作流程，对测试工作的计划、实施及总结做出详细的规定。对于在生产系统上进行的测试工作，必须制定详细的系统及数据备份、测试环境搭建、测试后系统及数据恢复、生产系统审核等计划，确保生产系统的安全。	检查系统测试操作流程，是否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。	是□ 否□ 不适用□	
2.3.2.	测试验收前是否根据设计方案或合同要求等制订测试验收方案，在测试验收过程中详细记录测试验收结果，并形成测试验收报告。	a)访谈系统建设负责人，询问是否根据设计方案或合同要求组织相关部门和人员制定工程测试验收方案，并对系统测试验收报告进行审定； b)检查是否具有工程测试验收方案，查看其是否明确说明参与测试的部门、人员、测试验收内容、现场操作过程等内容，过程控制是否符合管理规定的要求.	是□ 否□ 不适用□	
2.3.3.	是否组织相关部门和相关人员对系统测试验收报告进行审定，并签字确认。	检查是否具有系统测试验收报告，是否有相关部门和人员对系统测试验收报告进行审定的意见。	是□ 否□ 不适用□	
2.3.4.	是否委托第三方测试单位测试系统安全性，并出具安全性测试报告。	检查是否具有系统测试验收报告，是否有第三方测试机构的签字或盖章。	是□ 否□ 不适用□	
2.3.5.	是否书面规定系统测试验收的控制方法和人员行为准则。	检查系统建设方面的管理制度，查看其是否包括对系统测试验收的控制方法和人员行为准则规定。	是□ 否□ 不适用□	
2.3.6.	是否指定或授权专门的部门负责系统测试验收的管理，并按照管理规定的要求完成系统测试验收工作。	访谈系统建设负责人，询问是否有专门的部门负责测试验收工作，由何部门负责；是否委托第三方测试机构对信息系统进行独立的安全性测试。	是□ 否□ 不适用□	
2.3.7.	是否为系统测试配备必要的人员和设备资源，需要时协调关联单位配合测试。	访谈开发负责人，询问是否为系统测试配备必要的人员和设备资源，需要时协调关联单位配合测试。	是□ 否□ 不适用□	

表 J.2　重要信息系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.3.8.	是否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覆盖功能、性能、容量、安全性、稳定性等方面。测试完成后对测试结果进行分析评估，并给出测试报告。	a)访谈开发负责人，询问是否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； b)检查是否具有测试方案，是否包括覆盖功能、性能、容量、安全性、稳定性等方面； c)检查近期上线系统的测试报告。	是□ 否□ 不适用□	
2.3.9.	是否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。模拟环境是否与生产环境进行有效隔离，不得对生产环境进行干扰。	检查“表 0.3-网络边界防护情况-交易业务网与模拟环境测试网络”，检查系统模拟环境逻辑架构，查看系统模拟环境在逻辑架构上是否与生产环境一致，是否与生产环境有效隔离。	是□ 否□ 不适用□	
2.3.10.	是否根据测试方案的设计，合理配置模拟环境测试所需的设备，识别设备不同可能带来的测试结果正确性风险。	a)访谈开发负责人，询问是否根据测试方案的设计，合理配置模拟环境测试所需的设备，识别设备不同可能带来的测试结果正确性风险； b)检查系统测试方案、测试报告，查看是否有设备不同可能带来的测试结果正确性风险的说明。	是□ 否□ 不适用□	
2.3.11.	是否根据需要，要求生产系统运维人员和业务部门组织业务人员参与模拟环境测试。	a)访谈开发负责人，询问是否根据需要，要求生产系统运维人员和业务部门组织业务人员参与模拟环境测试； b)查看测试通知或记录，是否有生产系统运维人员和业务部门组织业务人员参与。	是□ 否□ 不适用□	
2.3.12.	模拟环境使用的密码是否与生产系统严格区分，系统管理员宜由不同的人员担任。	访谈开发负责人，询问模拟环境使用的密码是否与生产系统严格区分，系统管理员由不同的人员担任。	是□ 否□ 不适用□	
2.3.13.	生产环境测试前是否备份当前系统的数据和配置。	a)检查系统测试管理制度和操作流程，查看数据和配置备份要求； b)抽查在生产系统上进行测试的工作记录，检查是否做好数据备份。	是□ 否□ 不适用□	
2.3.14.	是否提前发布生产环境测试的系统测试公告。	a)访谈开发负责人，询问是否提前发布生产环境测试系统测试公告； b)查看一次使用生产环境测试的测试公告。	是□ 否□ 不适用□	

表 J.2　重要信息系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.3.15.	是否由生产系统运维人员在生产环境下组织完成生产环境测试。	a)访谈开发负责人，询问是否由生产系统运维人员在生产环境下组织完成生产环境测试； b)查看一次生产环境测试的测试方案、测试记录，是否由生产系统运维人员在生产环境下组织完成生产环境测试。	是□ 否□ 不适用□	
2.3.16.	是否根据需要，要求业务部门组织业务人员参与生产环境测试。	a)访谈开发负责人，询问是否根据需要，要求业务部门组织业务人员参与生产环境测试； b)查看一次生产环境测试的测试方案、测试记录，是否根据需要，要求业务部门组织业务人员参与生产环境测试。	是□ 否□ 不适用□	
2.3.17.	是否根据生产环境测试的结果设计系统升级过程及应急预案。	a)访谈开发负责人，询问是否根据生产环境测试的结果设计系统升级过程及应急预案； b)抽查一次生产环境测试报告和系统变更方案。	是□ 否□ 不适用□	
2.3.18.	如果生产环境测试内容涉及其他相关系统，是否协调其他系统用户参与测试。	a)访谈开发负责人，询问如果生产环境测试内容涉及其他相关系统，是否协调其他系统用户参与测试； b)抽查测试方案、测试记录，是否体现其他系统用户。	是□ 否□ 不适用□	
2.3.19.	涉及核心交易业务系统的上线测试，是否组织全市场或全公司各相关部门测试。	a)访谈开发负责人，询问涉及核心交易业务系统的上线测试，是否组织全市场或全公司各相关部门测试； b)抽查核心系统上线测试方案、测试记录，是否体现参测机构及部门。	是□ 否□ 不适用□	
2.3.20.	测试后是否恢复生产环境并验证恢复的有效性。	a)访谈开发负责人，询问测试后是否恢复生产环境并验证恢复的有效性； b)抽查测试方案、恢复验证记录。	是□ 否□ 不适用□	
2.3.21.	是否禁止交易时段使用生产环境进行测试。	a)访谈开发负责人，询问是否交易时段不得使用生产环境进行测试； b)抽查测试方案、测试记录、测试报告，查看是否在交易时段测试。	是□ 否□ 不适用□	
2.3.22.	是否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。	查看测试记录，是否在设备和软件投入使用前进行必要的验证性测试。	是□ 否□ 不适用□	

表 J.2　重要信息系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.4.	**系统运维**			
2.4.1.	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。	a)检查运维管理制度，是否包括机房管理、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； b)检查运维操作流程，是否包括日常操作、事件处理、问题处理、系统变更、应急处置等。	是□ 否□ 不适用□	
2.4.2.	交易业务系统的操作规程是否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。	检查交易业务系统的操作规程，是否包括操作的对象、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。	是□ 否□ 不适用□	
2.4.3.	是否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进行记录留痕，记录的保存时间不少于一年。	检查一年内对交易业务系统的操作记录，是否严格按照操作手册执行运维操作。	是□ 否□ 不适用□	
2.4.4.	特殊操作、临时操作是否经批准后方可双岗执行。操作过程是否进行记录留痕，记录的保存时间是否不少于一年。	抽查公司一年内特殊操作和临时操作的记录，检查相关操作是否经过审批，是否有操作人员和复核人员签名确认。	是□ 否□ 不适用□	
2.4.5.	是否依据业务、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。	抽查修订记录，确认业务或信息系统发生重大变更时，是否对相关系统操作手册及规程进行修订并经过审批。	是□ 否□ 不适用□	
2.4.6.	是否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，是否开启自动监控系统和自动报警系统。	a)访谈运维负责人，询问是否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； b)检查巡检记录，是否包括报单数、成交数、委托数、CPU 使用率、内存使用率等指标。	是□ 否□ 不适用□	
2.4.7.	是否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。	a)访谈运维负责人，询问是否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； b)检查定期检查、评估的记录或报告，确定是否设定了预警阈值。	是□ 否□ 不适用□	

表 J.2　重要信息系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.4.8.	主机监控指标是否包括：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。	a)检查“表 0.4-系统监控情况”，检查系统设计和验收文档，服务器监控指标是否包括设备运行状态、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； b)现场检查主机监控情况。	是□ 否□ 不适用□	
2.4.9.	存储监控指标是否包括：设备运行状态、数据交换延时、存储电池状态等。	a)检查“表 0.4-系统监控情况”，检查系统设计和验收文档，存储监控指标是否包括设备运行状态、数据交换延时、存储电池状态等； b)现场检查存储监控情况。	是□ 否□ 不适用□	
2.4.10.	数据库监控指标是否包括日志信息、表空间使用率、连接数等。	a)检查“表 0.4-系统监控情况”，检查系统设计和验收文档，数据库监控指标是否包括日志信息、表空间使用率、连接数等； b)现场检查数据库监控情况。	是□ 否□ 不适用□	
2.4.11.	核心交易业务相关的应用系统监控指标是否包括进程的活动状态、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。	a)检查“表 0.4-系统监控情况”，检查系统设计和验收文档，检查相关的应用系统监控指标，是否包括进程的活动状态、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； b)现场检查应用系统监控情况。	是□ 否□ 不适用□	
2.4.12.	是否针对不同系统设置合理的监测频度。	a)访谈运维负责人，询问是否针对不同系统设置合理的监测频度； b)查阅相关系统设置文档，是否有监测频度的说明； c)根据监测频度说明，检查相关参数设置情况。	是□ 否□ 不适用□	
2.4.13.	持续跟踪厂商提供的系统升级更新情况，是否在经过充分的测试评估后对必要的补丁进行及时更新，并在安装系统补丁前对现有的重要文件进行备份。	a)访谈系统管理员，了解系统补丁更新程序和评估方法； b)查看系统补丁更新记录，确认持续跟踪厂商提供的系统升级更新情况，确认在对重要文件进行备份后，才实施系统补丁程序的安装。	是□ 否□ 不适用□	

表 J.2　重要信息系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.4.14.	是否依据操作手册对系统进行维护，详细记录操作日志，包括重要的日常操作、运行维护记录、参数的设置和修改等内容，严禁进行未经授权的操作。	a)访谈信息技术部门负责人和操作人员，了解对系统进行维护审批和操作步骤； b)检查运维操作手册和操作日志，确认是否包括重要的日常操作、运行维护记录、参数的设置和修改等内容，确认按照授权进行操作。	是□ 否□ 不适用□	
2.4.15.	是否保持系统的可用性，及时维修、更换故障设备和更新软件。	检查运维操作手册,是否包括保持系统的可用性，及时维修、更换故障设备和更新软件。	是□ 否□ 不适用□	
2.4.16.	是否负责应用系统的参数配置、调优，编制文档并保持更新。	检查运维操作手册,是否包括对应用系统、操作系统的参数进行配置、调优，编制文档并保持更新。	是□ 否□ 不适用□	
2.4.17.	是否定期对系统容量进行检查和评估，形成评估报告。	检查系统容量评估报告，是否定期对系统容量进行检查和评估。	是□ 否□ 不适用□	
2.4.18.	是否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。	检查运维操作手册,是否包括管理系统和应用程序服务进程，并关闭与业务无关的服务。	是□ 否□ 不适用□	
2.4.19.	是否对新上线的设备在接入运行网络前进行全面的安全检查。	a)访谈安全管理员，了解设备上线前的安全检查流程； b)查看设备上线前的漏洞扫描、渗透测试、病毒扫描、木马检测等扫描报告。	是□ 否□ 不适用□	
2.5.	**变更管理**			
2.5.1.	是否确认系统中要发生的变更，并制定相应的变更方案；重要系统变更前是否制定详细的变更方案、失败恢复方案、专项应急预案。	a)访谈系统运维负责人，询问系统变更机制或流程，是否针对系统的重大变更制定变更方案、失败恢复方案、专项应急预案； b)现场检查变更方案，抽查重要系统变更是否制定详细的变更方案、失败恢复方案、专项应急预案。	是□ 否□ 不适用□	
2.5.2.	是否建立变更控制的申报和审批文件化程序，对变更影响进行分析并文档化，记录变更实施过程，并妥善保存所有文档和记录。	检查是否有变更管理制度，查看其是否覆盖变更前审批、变更过程记录、变更后通报等方面内容，是否包括变更申报、审批程序，是否规定需要申报的变更类型、申报流程、审批部门、批准人等方面内容。	是□ 否□ 不适用□	

表 J.2　重要信息系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.5.3.	是否建立中止变更并从失败变更中恢复的文件化程序，明确过程控制方法和人员职责，必要时对恢复过程进行演练。	检查系统变更方案，查看其是否覆盖变更类型、变更原因、变更过程、变更前评估、变更失败恢复程序等方面内容，查看其是否有主管领导的批准签字。	是□ 否□ 不适用□	
2.5.4.	是否建立系统变更流程，对信息系统的变更活动进行规范。	检查变更管理流程。	是□ 否□ 不适用□	
2.5.5.	是否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。	检查系统变更记录，系统变更中的角色是否包括申请人、审批人、实施人、复核人。	是□ 否□ 不适用□	
2.5.6.	变更申请人是否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。	检查系统变更申请，申请中是否有明确的变更方案，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。	是□ 否□ 不适用□	
2.5.7.	变更审批人是否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。	a)检查变更风险评估报告，判断变更审批人是否充分评估变更的技术风险和业务风险； b)检查变更审批记录，是否审批记录留痕并满足审计需要。	是□ 否□ 不适用□	
2.5.8.	变更审批人是否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。	检查变更审批记录，变更审批人是否确定了变更实施时间窗口，做到了除紧急变更外，不得在交易时段进行变更实施。	是□ 否□ 不适用□	
2.5.9.	是否按照测试方案，组织变更前后的测试，测试后是否提交测试记录或报告。	检查变更测试记录或报告，是否按照测试方案，组织变更前后的测试。	是□ 否□ 不适用□	
2.5.10.	变更实施人是否按照变更实施方案进行变更，并及时更新配置库。	a)检查系统变更记录，变更实施人是否按照变更实施方案进行变更； b)检查系统配置库，是否变更后及时更新配置库。	是□ 否□ 不适用□	
2.5.11.	变更复核人是否对变更记录和变更结果进行评估，评估内容是否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。	检查变更复核记录，变更复核人是否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。	是□ 否□ 不适用□	

表 J.2　重要信息系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.6.	**安全管理**			
2.6.1.	是否建立至少每季度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。	a)访谈系统管理员，询问是否定期对系统进行漏洞扫描，扫描周期多长，发现漏洞是否及时修补，在安装系统补丁前是否对重要文件进行备份，是否先在测试环境中测试通过再安装； b)检查是否至少每季进行一次漏洞扫描，并对漏洞风险持续跟踪，在经过充分的验证测试后，对必要的漏洞开展修补工作。	是□ 否□ 不适用□	
2.7.	**身份鉴别**			
2.7.1.	是否提供专用的登录控制模块对登录用户进行身份标识和鉴别。	检查主要应用系统设计和验收文档，查看是否提供身份标识和鉴别功能。	是□ 否□ 不适用□	
2.7.2.	是否提供用户身份标识唯一和鉴别信息复杂度检查功能，保证应用系统中不存在重复用户身份标识，身份鉴别信息不易被冒用。	检查主要应用系统设计和验收文档，查看是否采用了措施保证身份标识具有唯一性，是否对登录用户的口令最小长度、复杂度和更换周期等进行了要求和限制，保证身份鉴别信息不易被冒用。	是□ 否□ 不适用□	
2.7.3.	是否提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施。	检查主要应用系统设计和验收文档，查看是否提供登录失败处理功能，是否根据安全策略设置了登录失败次数等参数。	是□ 否□ 不适用□	
2.7.4.	是否启用身份鉴别、用户身份标识唯一性检查、用户身份鉴别信息复杂度检查以及登录失败处理功能，并根据安全策略配置相关参数。	a)测试主要应用系统，可通过试图以合法和非法用户分别登录系统，验证身份标识和鉴别功能是否有效； b)测试主要应用系统，可通过多次输入错误的密码，验证登录失败处理功能是否有效； c)渗透测试主要应用系统，如多次猜测用户口令，验证应用系统身份标识和鉴别功能是否不存在明显的弱点。应当从互联网向被测试对象进行渗透测试。	是□ 否□ 不适用□	
2.7.5.	管理用户通过受控本地控制台管理应用系统时，是否采用一种或一种以上身份鉴别技术。	检查应用系统设计和验收文档，当管理用户通过受控本地控制台管理应用系统时，是否采用了一种或一种以上身份鉴别技术。	是□ 否□ 不适用□	

表 J.2　重要信息系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.7.6.	管理用户以远程方式登录应用系统，是否采用两种或两种以上组合的鉴别技术进行身份鉴别。	检查应用系统设计和验收文档，当管理用户以远程方式登录应用系统，是否采用了两种或两种以上组合的鉴别技术进行身份鉴别。	是□ 否□ 不适用□	
2.7.7.	面向互联网服务的系统是否提供两种或两种以上组合的鉴别技术供用户选择。	检查应用系统设计和验收文档，面向互联网服务的系统是否向用户提供两种或两种以上组合的鉴别技术供用户选择。	是□ 否□ 不适用□	
2.7.8.	是否禁止设置弱口令，若系统条件允许，口令是否采用数字、字母、符号混排且无规律的方式。	检查口令管理制度，是否规定口令应采用数字、字母、符号混排且无规律的方式。	是□ 否□ 不适用□	
2.7.9.	是否禁止设置弱口令，若系统条件允许，管理员口令长度原则上不低于 12 位。	检查口令管理制度，是否规定管理员用户口令的长度至少为 12 位。	是□ 否□ 不适用□	
2.7.10.	核心交易业务系统是否提示并阻止用户使用弱口令登录。	检查核心交易业务系统设计和验收文档，确定核心交易业务系统是否提示并阻止用户使用弱口令登录。	是□ 否□ 不适用□	
2.7.11.	是否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。	检查口令管理制度，是否规定管理员用户口令至少每季度更换 1 次，更新的口令至少 5 次内不能重复。	是□ 否□ 不适用□	
2.7.12.	应用系统的账户及口令是否采用加密方式存储、传输，加密产品的使用是否符合国家有关规定。	检查口令管理制度，是否规定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。	是□ 否□ 不适用□	
2.7.13.	是否重点加强对匿名/默认用户的管理，防止被非法使用。	a)检查账户列表，是否没有匿名/默认用户； b)若有匿名/默认用户，测试是否不能被非法使用。	是□ 否□ 不适用□	
2.7.14.	是否及时注销不再使用的账户。	检查在岗人员名单和账户列表，确定没有未注销的不再使用的账户。	是□ 否□ 不适用□	
2.7.15.	是否设置抵御连续猜测等对客户账户恶意攻击行为的策略。	a)检查连续猜测等对客户账户恶意攻击行为的策略； b)现场测试系统抵御连续猜测客户账户的攻击行为。	是□ 否□ 不适用□	

表 J.2　重要信息系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.8.	**访问控制**			
2.8.1.	是否提供访问控制和权限管理机制，依据安全策略控制用户对文件等客体的访问，防止客户的授权被恶意提升或转授，防止客户使用未经授权的功能，防止客户进行访问未经授权的数据等非法访问活动。	a)检查应用系统设计和验收文档，查看是否依据安全策略控制用户对文件等客体的访问； b)测试主要应用系统，可通过以不同权限的用户登录系统，查看其拥有的权限是否与系统赋予的权限一致，验证应用系统访问控制功能是否有效。	是□ 否□ 不适用□	
2.8.2.	访问控制的覆盖范围是否包括与资源访问相关的主体、客体及它们之间的操作。	检查应用系统设计和验收文档，查看其访问控制的覆盖范围是否包括与信息安全直接相关的主体、客体及它们之间的操作。	是□ 否□ 不适用□	
2.8.3.	是否由授权主体配置访问控制策略，并严格限制默认账户的访问权限。	a)检查应用系统设计和验收文档，查看其访问控制的覆盖范围是否包括与信息安全直接相关的主体、客体及它们之间的操作； b)测试主要应用系统，可通过以默认用户登录系统，并进行一些合法和非法操作，验证系统是否严格限制了默认帐户的访问权限。	是□ 否□ 不适用□	
2.8.4.	是否授予不同账户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系。	a)检查应用系统的用户角色或权限的分配情况，查看是否仅授予不同帐户为完成各自承担任务所需的最小权限，特权用户的权限是否分离，权限之间是否相互制约，如系统管理员不能进行审计操作、审计员不能进行系统管理操作等； b)渗透测试主要应用系统，进行试图绕过访问控制的操作，验证应用系统的访问控制功能是否不存在明显的弱点。	是□ 否□ 不适用□	
2.8.5.	是否根据业务需求和系统安全分析确定系统的访问控制策略。	a)访谈系统运维负责人，询问是否指定专门的部门或人员负责系统管理，如根据业务需求和系统安全分析制定系统的访问控制策略，控制分配文件及服务的访问权限； b)查看访问控制策略文档，判断是否根据业务需求和系统安全分析制定了系统的访问控制策略。	是□ 否□ 不适用□	

表 J.2　重要信息系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.8.6.	是否指定专人对系统进行管理，划分系统管理员角色，明确各个角色的权限、责任和风险，权限设定是否遵循最小授权原则。	访谈系统运维负责人，询问是否对系统管理员用户进行分类，明确各个角色的权限、责任和风险，权限设定是否遵循最小授权原则。	是□ 否□ 不适用□	
2.9.	**资源控制**			
2.9.1.	用户登录应用系统后在规定的时间内未执行任何操作，是否自动退出系统。	测试主要应用系统，当应用系统的通信双方中的一方在一段时间内未作任何响应，查看另一方是否能够自动结束会话。	是□ 否□ 不适用□	
2.9.2.	是否能够对系统的最大并发会话连接数进行限制。	检查主要应用系统的配置参数，查看是否提供对最大并发会话连接数进行限制。	是□ 否□ 不适用□	
2.9.3.	是否能够对单个账户的多重并发会话进行限制。	测试主要应用系统，可通过对系统进行超过规定的单个帐户的多重并发会话数进行连接，验证系统是否能够正确地限制单个帐户的多重并发会话数。	是□ 否□ 不适用□	
2.9.4.	是否能够对一个时间段内可能的并发会话连接数进行限制。	检查主要应用系统的配置参数，查看是否提供对最大并发会话连接数进行限制。	是□ 否□ 不适用□	
2.9.5.	是否能够对一个访问账户或一个请求进程占用的资源分配最大限额和最小限额。	检查主要应用系统设计和验收文档，查看是否对一个访问帐户或一个请求进程占用的资源分配最大限额和最小限额。	是□ 否□ 不适用□	
2.9.6.	是否能够对系统服务水平降低到预先规定的最小值进行检测和报警。	a)检查主要应用系统设计和验收文档，查看是否有服务水平最小值的设定，当系统的服务水平降低到预先设定的最小值时，系统报警； b)测试主要应用系统，可试图使服务水平降低到预先规定的最小值，验证系统是否能够正确检测并报警。	是□ 否□ 不适用□	
2.9.7.	是否提供服务优先级设定功能，并在安装后根据安全策略设定访问账户或请求进程的优先级，根据优先级分配系统资源。	检查主要应用系统设计和验收文档，查看是否能根据安全策略设定主体的服务优先级，根据优先级分配系统资源。	是□ 否□ 不适用□	

表 J.2　重要信息系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.10.	**数据安全**			
2.10.1.	通过互联网、卫星网进行通信时，是否采用密码技术保证通信过程中数据的完整性。	a)检查设计、验收文档或源代码，查看其是否有关于保护通信完整性的说明，如果有则查看是否有根据校验码判断对方数据有效性，以及散列（Hash）密码计算报文校验码的描述； b)对于通过互联网、卫星网进行通信的系统，通过截包分析，检查通信报文是否经过加密保护。	是□ 否□ 不适用□	
2.10.2.	是否能够检测到系统管理数据、鉴别信息和重要业务数据在传输过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施。	如果主要主机操作系统能够进行远程管理，则应查看应用系统的设计、验收文档或源代码，查看是否有关于能检测系统管理数据、鉴别信息和重要业务数据传输过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施的描述。	是□ 否□ 不适用□	
2.10.3.	是否采用加密或其他保护措施实现系统管理数据、鉴别信息和重要业务数据存储保密性。	检查主要应用系统设计文档，查看鉴别信息是否采用加密或其他有效措施实现存储保密性。	是□ 否□ 不适用□	
2.11.	**备份能力**			
2.11.1.	灾难应对能力是否达到《证券期货经营机构信息系统备份能力标准》第五级或重大灾难应对能力达到第六级要求。	检查“表0.8-系统备份能力”、“表0.8-数据备份情况”，查看灾难应对能力达标证明材料（包括：灾备系统建设情况、备份策略、应急演练记录等），确认灾难应对能力达到《证券期货经营机构信息系统备份能力标准》第五级或重大灾难应对能力达到第六级要求。	是□ 否□ 不适用□	
2.11.2.	重大灾难应对能力是否达到《证券期货经营机构信息系统备份能力标准》第六级要求。	检查“表0.8-系统备份能力”、“表0.8-数据备份情况”，查看灾难应对能力达标证明材料（包括：灾备系统建设情况、备份策略、应急演练记录等），确认重大灾难应对能力达到《证券期货经营机构信息系统备份能力标准》第六级要求。	是□ 否□ 不适用□	
2.11.3.	实时信息系统是否达到《证券期货经营机构信息系统备份能力标准》中故障应对能力的第四级要求。	检查“表0.8-系统备份能力”、“表0.8-数据备份情况”，检查公司实时信息系统故障应对能力达标证明材料（包括：备份系统建设情况、备份策略、应急演练记录等），确认故障应对能力达到《证券期货经营机构信息系统备份能力标准》中第四级要求。	是□ 否□ 不适用□	

表 J.2　重要信息系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.11.4.	法人清算系统、门户网站系统等非实时信息系统是否满足《证券期货经营机构信息系统备份能力标准》中故障应对能力的第二级要求。	检查“表0.8-系统备份能力”、“表0.8-数据备份情况”，检查公司非实时信息系统故障应对能力达标证明材料（包括：备份系统建设情况、备份策略、应急演练记录等），确认法人清算系统、门户网站系统等非实时信息系统的故障应对能力达到《证券期货经营机构信息系统备份能力标准》中故障应对能力的第二级要求。	是□ 否□ 不适用□	
2.12.	**安全审计**			
2.12.1.	应用系统是否能够对每个业务用户的关键操作进行记录，例如用户登录、用户退出、增加用户、修改用户权限等操作。	a)检查主要应用系统，查看审计范围是否覆盖到每个用户，审计策略是否覆盖系统内重要的安全相关事件，例如，用户标识与鉴别、访问控制的所有操作记录、重要用户行为、系统资源的异常使用、重要系统命令的使用等； b)测试主要应用系统，在应用系统上试图产生一些重要的安全相关事件（如进行用户登录、修改用户权限等操作），查看应用系统是否对其进行了审计，验证应用系统安全审计的覆盖情况是否覆盖到每个用户；如果进行了审计则查看审计记录内容是否包含事件的日期、时间、发起者信息、类型、描述和结果等。	是□ 否□ 不适用□	
2.12.2.	审计记录的内容是否包括事件日期、时间、发起者信息、类型、描述和结果等。审计记录是否至少保存6个月。	检查主要应用系统的审计记录，查看是否包括事件发生的日期与时间、触发事件的主体与客体、事件的类型、事件成功或失败、身份鉴别事件中请求的来源、事件的结果等内容；检查是否保存了6个月以上的审计记录。	是□ 否□ 不适用□	
2.12.3.	是否采取有效措施防止单独中断审计进程；审计进程应作为应用系统整体进程中的一部分，并且不能单独中断。	测试主要应用系统，试图非授权终止审计进程或审计功能，删除、修改或覆盖审计记录，查看安全审计进程和记录的保护情况。	是□ 否□ 不适用□	
2.12.4.	是否提供对审计记录数据进行统计、查询、分析及生成审计报表的功能。	检查主要应用系统，查看是否为授权用户浏览和分析审计数据提供专门的审计分析功能，并能根据需要生成审计报表。	是□ 否□ 不适用□	

表 J.2　重要信息系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.12.5.	是否保证信息系统日志的完备性，确保所有重大修改被完整地记录，确保开启审计留痕功能。证券公司信息系统日志是否至少保存 15 年。	a)检查运维管理制度，是否规定保证信息系统日志的完备性，确保所有重大修改被完整地记录，信息系统日志是否至少保存 15 年； b)检查系统设计和验收文档，是否开启审计留痕功能。	是□ 否□ 不适用□	
2.12.6.	是否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。	查看每日检查记录，是否指定人员按照运维管理制度和操作流程，对日常操作执行情况进行每日检查。	是□ 否□ 不适用□	
2.12.7.	是否每季组织开展内部检查，形成检查报告。	审阅内部检查报告，检查是否每季度一次。	是□ 否□ 不适用□	
2.12.8.	是否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。	a)审阅公司年度审计计划，是否包含信息系统运维管理工作审计项目； b)检查公司年度审计报告，是否包含信息系统运维管理工作审计项目。	是□ 否□ 不适用□	
2.12.9.	检查和审计范围是否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。	检查信息系统运维管理工作审计报告，确定信息系统运维管理工作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。	是□ 否□ 不适用□	
2.12.10.	是否对检查和审计的结果采取纠正性和预防性的措施。	审阅信息系统运维管理工作审计整改报告，确定是否对检查和审计的结果采取纠正性和预防性的措施。	是□ 否□ 不适用□	
2.12.11.	是否定期检查安全隔离情况，确保各安全域之间有效隔离。	a)查看包括自建和托管机房的网络拓扑图、安全域划分情况，检查各安全域之间是否采用了防火墙或安全网关等有效隔离方式和隔离手段； b)审阅最近的网络隔离情况检查报告，判断是否定期对上述事项进行了检查。	是□ 否□ 不适用□	

表 J.2　重要信息系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.12.12.	是否组织相关人员定期对监测和报警记录进行分析、评审，发现可疑行为，形成分析报告，并采取必要的应对措施。	a)访谈系统运维负责人，询问其是否组织人员定期对监测记录进行分析、评审，是否发现可疑行为并对其采取必要的措施，是否形成分析报告； b)检查监测记录，查看是否记录监控对象、监控内容、监控的异常现象处理等方面，查看是否对异常现象及处理措施形成分析报告。	是□ 否□ 不适用□	
2.12.13.	是否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。	检查是否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，以满足审计的需要。	是□ 否□ 不适用□	
2.12.14.	是否保存监控产生的日志，保存时间不少于一年。	检查监控日志，保存时间是否不少于一年。	是□ 否□ 不适用□	
2.12.15.	是否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。	查看评估记录，是否每日分析核心交易业务系统监控日志及巡检记录，并跟踪处理日志分析中发现的异常事件。	是□ 否□ 不适用□	
2.12.16.	是否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。	查看评估报告，是否至少每季度全面评估监控日志和操作记录，分析异常情况。	是□ 否□ 不适用□	
2.12.17.	是否至少每月对运行日志和审计数据进行分析。	检查是否每月对运行日志和审计数据进行分析。	是□ 否□ 不适用□	
3.	**数据库管理**			
3.1.	**安全审计**			
3.1.1.	审计内容是否至少包括：用户的添加和删除、审计功能的启动和关闭、审计策略的调整、权限变更、系统资源的异常使用、重要的系统操作（如用户登录、退出）等。	审阅主机审计记录，检查审计内容是否包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件；审计内容至少包括：用户的添加和删除、审计功能的启动和关闭、审计策略的调整、权限变更、系统资源的异常使用、重要的系统操作（如用户登录、退出）等。	是□ 否□ 不适用□	
3.1.2.	审计记录是否包括事件的日期、时间、类型、主体标识、客体标识和结果等。	审阅主机运行日志，检查审计记录是否包括事件的日期、时间、类型、主体标识、客体标识和结果等。	是□ 否□ 不适用□	

表 J.2　重要信息系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
3.1.3.	是否保护审计记录，避免受到未预期的删除、修改或覆盖等。审计记录是否至少保存6个月。	检查审计记录是否至少保存 6 个月。	是□ 否□ 不适用□	
3.1.4.	审计范围是否覆盖到服务器和重要客户端上的每个数据库用户；应在保证系统运行安全和效率的前提下，启用系统审计或采用第三方安全审计产品实现审计要求。	a)通过访谈，了解是否在保证系统运行安全和效率的前提下，启用了系统审计或采用第三方安全审计产品实现审计要求，保证产生、有效记录和存储了审计日志； b)通过访谈，审阅主机和客户端审计记录，判断是否覆盖到服务器和重要客户端上的每个操作系统用户和数据库用户。	是□ 否□ 不适用□	
3.1.5.	是否能够根据记录数据进行分析，并生成审计报表。	检查主要服务器操作系统、重要终端操作系统和主要数据库管理系统的安全审计策略，查看是否为授权用户提供浏览和分析审计记录的功能，是否可以根据需要自动生成不同格式的审计报表。	是□ 否□ 不适用□	
3.1.6.	是否保护审计进程，避免受到未预期的中断。	测试主要服务器操作系统、重要终端操作系统和主要数据库管理系统，可通过非审计员的其他帐户试图中断审计进程，验证审计进程是否受到保护。	是□ 否□ 不适用□	
3.2.	**访问控制**			
3.2.1.	是否严格限制人工对数据库操作的账户权限，并分别使用不同权限的账户执行查询、插入、更新、删除等操作。	a)查看数据库账户权限管理制度，是否规定分别使用不同权限的账户执行查询、插入、更新、删除等操作； b)检查对数据库进行人工操作的记录，确认使用不同权限的账户执行查询、插入、更新、删除等操作。	是□ 否□ 不适用□	
3.3.	**身份鉴别**			
3.3.1.	口令是否符合以下条件：数字、字母、符号混排，无规律的方式。	检查口令管理制度，是否规定口令符合以下条件：数字、字母、符号混排，无规律的方式。	是□ 否□ 不适用□	
3.3.2.	口令的长度是否至少为 12 位。	检查口令管理制度，是否规定管理员用户口令的长度至少为 12 位。	是□ 否□ 不适用□	
3.3.3.	口令是否至少每季度更换1次，更新的口令至少 5 次内不能重复。	检查口令管理制度，是否规定管理员用户口令至少每季度更换 1 次，更新的口令至少 5 次内不能重复。	是□ 否□ 不适用□	

表 J.2　重要信息系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
3.3.4.	如果设备口令长度不支持12位或其他复杂度要求，口令是否使用所支持的最长长度并适当缩小更换周期；也可以使用动态密码卡等一次性口令认证方式。	检查口令管理制度，是否规定口令应使用所支持的最长长度并适当缩小更换周期，也可以使用动态密码卡等一次性口令认证方式。	是□ 否□ 不适用□	
3.3.5.	是否为数据库系统的不同用户分配不同的用户名，确保用户名具有唯一性。	检查数据库系统的用户列表，标识是否唯一。	是□ 否□ 不适用□	
3.4.	**数据库运维**			
3.4.1.	是否保持数据库的可用性，及时维护、更新软件。	a)查看数据库软件、数据库监控软件的采购合同，以及维护、更新记录； b)查看数据库监控日志，判断表空间使用率、连接数等是否保持在合理范围。	是□ 否□ 不适用□	
3.4.2.	是否对数据库的参数进行配置、调优，编制文档并保持更新。	a)访谈数据库管理员,询问是否依照数据库配置文档进行安装、配置及调优； b)查看数据库配置文档和维护记录，确认对数据库系统进行了配置、调优。	是□ 否□ 不适用□	
3.4.3.	是否定期对数据库容量进行检查和评估，形成评估报告。	a)查看公司数据库容量管理制度，是否明确要求定期对数据库系统容量进行检查和评估，并形成评估报告； b)访谈数据库管理员，查看数据库容量评估报告，确认定期对数据库容量进行了检查和评估。	是□ 否□ 不适用□	
3.4.4.	是否管理数据库、表、索引、存储过程，数据库的升级、优化、扩容、迁移。	a)查看公司数据库容量管理制度，是否明确数据库管理员应负责管理数据库、表、索引、存储过程，数据库的升级、优化、扩容、迁移； b)访谈数据库管理员，查看数据库维护记录，确认数据库管理员按照要求管理数据库、表、索引、存储过程，对数据库进行了升级、优化、扩容、迁移等维护工作。	是□ 否□ 不适用□	
3.4.5.	是否定期检查数据库的用户、口令及权限设置的正确性。	访谈数据库管理员，查看数据库维护记录，确认是否定期检查数据库的用户、口令及权限设置的正确性。	是□ 否□ 不适用□	

表 J.2　重要信息系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
3.5	**系统托管**			
3.5.1	二级系统托管是否满足《证券期货业信息系统托管基本要求》（JR/T 0133-2015)的相关要求。	检查托管服务合同和相关文档，确认按照信息安全等级保护二级要求进行定级的系统选购了二级系统托管服务。	是□ 否□ 不适用□	
3.5.2	三级系统托管是否满足《证券期货业信息系统托管基本要求》（JR/T 0133-2015)的相关要求。	检查托管服务合同和相关文档，确认按照信息安全等级保护三级要求进行定级的系统选购了三级系统托管服务。	是□ 否□ 不适用□	
3.5.3	未定级系统托管是否满足《证券期货业信息系统托管基本要求》（JR/T 0133-2015)的相关要求。	检查托管服务合同和相关文档，确认未进行信息安全等级保护定级备案的信息系统选购了二级系统托管服务。	是□ 否□ 不适用□	

附 录 K
（规范性附录）
A 型营业部审计底稿

表K.1至表K.2给出了A型营业部审计的程序、内容及相关记录要求。

表K.1 A 型营业部审计底稿

被审计部门：	索引号：YYB-A-XXX
审计主题： A 型营业部	审计年度：
审计结论、意见及建议： 编制人： 年 月 日 （部门盖章）	
复核意见： 复核人： 年 月 日 （部门盖章）	
被审计部门意见： 年 月 日 （部门盖章）	

表 K.1　A 型营业部审计底稿（续）

审计证据列表：

表K.2　A型营业部审计底稿

序号	审计项	审计程序	审计结论	备注
1.	**安全管理**			
1.1.	是否确保证券营业部局域网与公司广域网、互联网实现有效隔离。	a)检查“表0.15-A型营业部-网络边界防护情况”，审阅网络拓扑图，查看防火墙、入侵检测等安全设备的配备情况； b)查看安全设备是否配置接口参数、过滤规则，网络设备的安全规则是否配置允许访问规则，控制粒度为网段级，对没有明确定义的数据包缺省拒绝； c)检查安全测试记录或第三方安全测试报告，确认网络和安全设备运行的有效性。	是□ 否□ 不适用□	
1.2.	是否确保证券营业部及时更新系统补丁、升级系统安全防护软件，定期进行全面的病毒和木马检测，发现病毒和木马立即处理并报告。移动存储、外来电子文档、软件系统使用前应进行病毒和木马查杀。	a)查看营业部信息技术管理制度，确认有关于证券营业部及时更新系统补丁、升级系统安全防护软件，定期进行全面的病毒和木马检测，发现病毒和木马立即处理并报告等规定； b)查看病毒和木马查杀记录，确认及时更新系统补丁、升级系统安全防护软件，定期进行全面的病毒和木马检测，发现病毒和木马立即处理并报告。移动存储、外来电子文档、软件系统使用前应进行病毒和木马查杀。	是□ 否□ 不适用□	
1.3.	是否证券营业部部署防病毒、防木马、防恶意代码等系统安全防护软件，保护证券营业部信息系统安全。	检查“表0.15-A型营业部-安全防护情况”，查看防护软件安装记录，抽查实际安装情况，确认证券营业部部署防病毒、防木马、防恶意代码等系统安全防护软件。	是□ 否□ 不适用□	
1.4.	证券公司是否加强证券营业部网络安全管理，确保证券营业部不得擅自对外互联或设立网站。如确有必要，证券公司应对网站的设立和维护进行统一管理。	a)查看证券公司发布的证券营业部对外互联、设立网站相关规定，规定是否包含证券营业部不得擅自对外互联或设立网站的相关内容。 b)查看证券公司对营业部对外互联或设立网站的审批记录，确认证券营业部禁止擅自对外互联或设立网站。如确有必要，证券公司应对网站的设立和维护进行统一管理。	是□ 否□ 不适用□	

表 K.2 A 型营业部审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.	**系统建设**			
2.1.	与证券营业部之间是否采用至少2条不同运营商或不同介质的通信线路，建立安全、可靠通信连接，且线路带宽能够满足证券营业部业务需要并留有冗余。	a)检查“表 0.15-A 型营业部-内部通信连接情况”，检查网络设计文档或验收文档，判断与证券营业部之间是否采用至少 2 条不同运营商或不同介质的通信线路，且线路带宽能够满足证券营业部业务需要。 b)检查网络设备清单，判断网络通信设备是否有冗余备份。	是□ 否□ 不适用□	
2.2.	A型证券营业部的通信线路中是否有一条为地面数据专线。	检查“表 0.15-A 型营业部-内部通信连接情况”，检查网络设计文档或验收文档，判断通信线路中是否有一条为地面数据专线。	是□ 否□ 不适用□	
2.3.	是否确保A型证券营业部提供至少2种相互独立的行情揭示系统、委托方式。	检查“表 0.15-A 型营业部-行情揭示软件情况”，检查行情委托系统验收文档，是否提供至少 2 种相互独立的行情揭示系统、委托方式。	是□ 否□ 不适用□	
2.4.	是否选择具备可靠供电的场所。	a)检查“表 0.15-A 型营业部-电力情况-供电方式”，检查相关材料或者询问楼宇物业、机房管理员等人员，确认最近两年内所在楼宇区域是否工作时间段内每年停电不超过 2 次，每次停电时间不超过 2 小时； b)检查相关材料或者询问楼宇物业、机房管理员等人员，供电电压是否稳定。	是□ 否□ 不适用□	
2.5.	是否远离强震源、强磁场源和强噪声源，远离电磁干扰源或实施有效电磁干扰防护。	检查楼宇物业或者机房建设的相关材料，实地检查机房环境，是否远离强震源、强磁场源和强噪声源，远离电磁干扰源或实施有效电磁干扰防护。	是□ 否□ 不适用□	
2.6.	证券营业部机房选址是否远离产生粉尘、油烟、有害气体以及具有腐蚀性、易燃、易爆物品的工厂、仓库等场所。	检查楼宇物业或者机房建设的相关材料，实地检查机房环境，是否远离产生粉尘、油烟、有害气体以及具有腐蚀性、易燃、易爆物品的工厂、仓库等场所。	是□ 否□ 不适用□	
2.7.	是否符合当地抗震强度要求。	检查楼宇物业或者机房建设的相关材料，实地检查机房环境，是否符合当地抗震强度要求。	是□ 否□ 不适用□	
2.8.	是否符合当地消防主管部门的消防安全要求。	检查“表 0.15-A 型营业部-消防情况”，检查机房建设或者机房消防的相关材料，确认机房符合当地消防主管部门的消防安全要求。	是□ 否□ 不适用□	

表K.2 A型营业部审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.9.	证券营业部机房是否具备独立空调系统，使机房温度保持在23℃±5℃范围内。	a)检查营业部机房内是否配备了独立空调系统，是否能够正常运行； b)检查营业部机房温度记录，是否控制在23℃±5℃范围内。	是□ 否□ 不适用□	
2.10.	机房供电是否具有独立于一般照明电的专用供电线路。	检查机房电路设计及验收文档，判断机房供电是否具有独立于一般照明电的专用供电线路。	是□ 否□ 不适用□	
2.11.	机房供电是否设有独立的配电柜或配电箱。	现场检查是否设有独立的配电柜或配电箱。	是□ 否□ 不适用□	
2.12.	机房供电是否相关电器设备、电线应与机柜用电负载相适应，并留有余量。	检查机房电路设计及验收文档、机柜用电负载说明文档，确认相关电器设备、电线是否与机柜用电负载相适应，并留有余量。	是□ 否□ 不适用□	
2.13.	机房是否配置UPS电源。	检查“表 0.15-A 型营业部-UPS”，现场检查是否配置 UPS 电源，并且 UPS 电源处于工作状态。	是□ 否□ 不适用□	
2.14.	机房供电是否禁止将与业务无关的设备接入UPS电源。	a)检查是否配置 UPS 电源； b)检查是否禁止将与业务无关的设备接入 UPS 电源。	是□ 否□ 不适用□	
2.15.	机房供电是否市电插座与UPS插座应严格区分，插座面板应有提示性的标识或标签。	a)检查是否配置 UPS 电源； b)检查市电插座与UPS插座是否严格区分，插座面板是否有提示性的标识或标签。	是□ 否□ 不适用□	
2.16.	A型证券营业部是否至少配备一种持续供电方式，在市电中断情况下，保证不低于25%的现场交易终端或同等支持能力的其他交易终端在交易时间内持续工作，满足证券营业部客户现场交易需要。	a)检查“表 0.15-A 型营业部-UPS”、“表 0.15-A 型营业部-发电机”，检查是否具有双路市电供电，应当说明双路供电的来源； b)如果没有双路市电供电，检查则 UPS 和后备发电设施的供电时间在市电中断情况下，是否可以保证不低于 25%的现场交易终端或同等支持能力的其他交易终端在交易时间内持续工作，满足证券营业部客户现场交易需要。	是□ 否□ 不适用□	
2.17.	证券营业部配备或租用发电机的，发电机是否安装在具有良好通风的场地内，并远离易燃易爆物品。	a)检查机房设备管理清单，确认包括配备或租用发电机； b)实地检查发动机，确认安装在具有良好通风的场地内，并远离易燃易爆物品。	是□ 否□ 不适用□	
2.18.	是否配备防火防盗门等有效安保设施。	实地检查机房入口，确认配备防火防盗门等有效安保设施。	是□ 否□ 不适用□	

表 K.2　A 型营业部审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.19.	证券公司与证券营业部之间网络通信设备是否具有冗余备份，保证发生故障时实现及时切换。	a)检查网络设计文档或验收文档，判断与证券营业部之间是否采用至少 2 条不同运营商或不同介质的通信线路，且线路带宽能够满足证券营业部业务需要； b)检查网络设备清单，判断网络通信设备是否有冗余备份。	是□ 否□ 不适用□	
2.20.	证券公司是否根据业务需要，合理划分证券营业部局域网安全域，确定各安全域的功能定位，在各安全域之间采取安全措施实现有效隔离。	查看包括自建和托管机房的网络拓扑图、安全域划分情况，检查各安全域之间是否根据业务需要，合理划分局域网安全域，是否采用了防火墙或安全网关等有效隔离方式和隔离手段。	是□ 否□ 不适用□	
2.21.	证券公司是否制定证券营业部局域网、公司广域网、互联网接入以及安全防护的网络建设规范，并统一规划管理证券营业部网络配置参数和IP地址段。	a)查看证券公司发布的证券营业部网络互联与接入、安全防护建设规范，规定是否包含证券营业部局域网、公司广域网、互联网接入以及安全防护的网络建设规范的相关内容； b)查看证券公司给营业部的网络配置参数和 IP 地址段分配表，确认统一规划管理证券营业部网络配置参数和 IP 地址段。	是□ 否□ 不适用□	
2.22.	证券公司是否对证券营业部与客户建立的网络连接进行审批，对连接方式进行统一规划和管理，并采取安全措施，实现有效隔离。	a)查看证券公司发布的证券营业部与客户建立网络连接的规定，规定是否包含连接方式进行统一规划和管理，并采取安全措施，实现有效隔离的相关内容； b)查看证券公司审批、检查营业部与客户建立网络连接的记录，确认相关规定的有效执行。	是□ 否□ 不适用□	
2.23.	证券公司是否确保证券营业部提供行情、开户、交易、资讯等客户服务的信息系统，具备足够的健壮性，系统处理能力具有一定的冗余度，并采用热备或冷备等手段，避免单点故障，提高系统可用性。	a)检查“表 0.15-A 型营业部-行情资讯软件情况”、“表 0.15-A 型营业部-行情接收情况”，查看证券公司发布的证券营业部信息系统建设的相关规定，规定是否包含证券营业部提供行情、开户、交易、资讯等客户服务的信息系统，具备足够的健壮性，系统处理能力具有一定的冗余度，并采用热备或冷备等手段，避免单点故障，提高系统可用性的相关内容； b)查看证券公司审批、检查营业部信息系统建设的记录，确认相关规定的有效执行。	是□ 否□ 不适用□	

表K.2 A型营业部审计底稿（续）

序号	审计项	审计程序	审计结论	备注
3.	**运维管理**			
3.1.	A型证券营业部是否至少配备一名专职技术人员。	检查“表 0.15-A 型营业部-IT 人员情况”，检查证券营业部类型和信息技术人员名单，判断 A 型证券营业部是否至少配备一名专职技术人员。	是□ 否□ 不适用□	
3.2.	证券营业部专职技术人员和兼职技术人员是否具有计算机相关专业学历或从事信息技术工作1年以上。	a)检查营业部信息技术人员简历，判断专职技术人员和兼职技术人员是否具有计算机相关专业学历或从事信息技术工作 1 年以上； b)检查营业部信息技术人员简历，判断专职技术人员和兼职技术人员是否具有计算机相关专业学历或从事信息技术工作 1 年以上。	是□ 否□ 不适用□	
3.3.	营业部是否制定顶岗、备岗等相关制度，确保在交易时间内有技术人员值守。	查看营业部顶岗、备岗等相关制度，检查操作记录，访谈营业部技术人员，判断是否在交易时间内有技术人员值守。	是□ 否□ 不适用□	
3.4.	是否加强证券营业部网络配置、访问控制、安全审计等网络管理，确保证券营业部的网络设备按最小安全访问原则设置访问控制权限，每一次变更后及时更新备份网络设备的配置信息。	a)检查营业部访问控制策略，访谈网络管理员，判断营业部的网络设备是否按最小安全访问原则设置访问控制权限； b)检查变更记录，判断每一次变更后是否及时更新备份网络设备的配置信息。	是□ 否□ 不适用□	
3.5.	证券营业部是否加强计算机终端的管理，记录网卡地址，防止非法使用。未经许可，不得将客户和员工的自备计算机接入证券营业部网络。	a)是否营业部有终端接入管理记录、记录网卡地址； b)是否有效防止非法使用。	是□ 否□ 不适用□	
3.6.	证券营业部提供无线网络服务的，证券公司是否统一制定证券营业部无线网络使用规范，采取有效的无线网络准入控制措施，登记并记录无线接入设备的信息。	a)证券公司是否统一制定证券营业部无线网络使用规范； b)查看营业部终端接入管理记录、营业部无线网络准入记录，检查营业部终端接入管理措施是否有效、无线网络使用规范是否落实。	是□ 否□ 不适用□	

表 K.2 A 型营业部审计底稿（续）

序号	审计项	审计程序	审计结论	备注
3.7.	是否加强证券营业部技术文档的收集、更新、保管、借阅等管理，确保证券营业部根据信息系统的变更情况及时更新技术文档。证券营业部技术文档包括但不限于机房平面图、供配电图、网络拓扑图、信息点对照表、系统手册、应急预案、运维日志、设备维护档案等资料。	a)检查文档管理制度，是否对营业部技术文档加强管理，包括收集、更新、保管、借阅等； b)检查证券营业部技术文档，是否包括但不限于机房平面图、供配电图、网络拓扑图、信息点对照表、系统手册、应急预案、运维日志、设备维护档案等资料。	是□ 否□ 不适用□	
3.8.	是否加强证券营业部数据备份、存放、保密、调阅、销毁等数据管理，确保证券营业部指定专人负责数据管理，数据调阅须经审批，且不得对外泄露。	a)检查数据管理制度，是否加强证券营业部数据备份、存放、保密、调阅、销毁等数据管理； b)访谈数据管理人员，判断是否指定专人负责数据管理，数据调阅须经审批，且不得对外泄露。	是□ 否□ 不适用□	
3.9.	证券营业部是否在关键系统和关键设备的用户管理上遵循权限最小化原则，建立用户和权限的清单，定期进行检查核对。用户和权限变更应执行相关审批流程，并保留完整的变更记录。	a)检查关键系统和关键设备用户和权限清单，确认用户管理上遵循权限最小化原则； b)检查关键系统和关键设备用户和权限定期检查记录，确认定期检查核对相关内容； c)检查用户和权限变更审批记录、变更记录，确认用户和权限变更应执行相关审批流程，并保留完整的变更记录。	是□ 否□ 不适用□	
3.10.	是否证券营业部关键系统和关键设备的管理员用户密码实行专人管理，采用不低于8位的复合密码，每半年至少更换一次。发生人员变动时应及时更新密码。	a)检查口令管理办法，确认关键系统和关键设备的管理员用户密码实行专人管理，采用不低于 8 位的复合密码，每半年至少更换一次。发生人员变动时应及时更新密码； b)检查密码变动记录，确认是否至少每半年更新一次密码，确认管理人变动时及时更新密码。	是□ 否□ 不适用□	
3.11.	证券营业部是否至少每半年检查一次电力、机房空调、消防等设施，每季度选择非交易时间进行UPS电池的充放电测试，并详细记录。	检查机房基础设施定期检查记录，确认是否每半年检查一次电力、机房空调、消防等设施，每季度选择非交易时间进行 UPS 电池的充放电测试的记录。	是□ 否□ 不适用□	

表K.2 A型营业部审计底稿（续）

序号	审计项	审计程序	审计结论	备注
3.12.	是否A型证券营业部具备完善的监控体系，对信息系统的运行环境、运行状况等进行定时监控和事后分析。	a)检查“表0.15-A型营业部-机房监控”、“表 0.15-A 型营业部-系统监控情况”，检查监控系统设计文档、监控系统日志，确认是否具备完善的监控体系，对信息系统的运行环境、运行状况等进行监控； b)检查监控系统日志和监控日志分析报告，是否对信息系统的运行环境、运行状况等进行定时监控和事后分析。	是□ 否□ 不适用□	
3.13.	是否A型证券营业部对系统运维日志进行规范管理，日常操作及异常事件处理应在系统运维日志中详细记录。运维日志可采用电子文档或纸质件记录，并妥善保管，保留期限不少于2年。	a)检查系统运维日志管理办法，确认对系统运维日志进行规范管理； b)抽查近 2 年的运维日志，判断日常操作及异常事件处理是否在系统运维日志中详细记录。	是□ 否□ 不适用□	
3.14.	是否对证券营业部安装使用的应用软件进行统一管理，证券营业部不得擅自安装与业务及技术维护无关的应用软件。	a)如果有应用软件统一管理平台，检查应用软件统一管理平台的采购合同、日志记录和分析报告，确认有效阻止擅自安装与业务及技术维护无关的应用软件； b)如果没有应用软件统一管理平台，检查应用软件统一管理制度和检查记录，确认阻止擅自安装与业务及技术维护无关的应用软件。	是□ 否□ 不适用□	
3.15.	是否配备应急照明装置。	a)检查应急物资资产记录、盘点更新记录，确认配备一定数量的应急照明装置； b)实地检查确认应急照明装置。	是□ 否□ 不适用□	
3.16.	是否证券营业部每年至少进行两次应急演练，并留存演练记录。	a)检查应急管理制度，是否要求每年至少进行二次演练； b)检查应急演练记录，确认每年至少进行两次应急演练。	是□ 否□ 不适用□	
3.17.	营业部发生影响交易业务的技术故障时，证券公司是否立即启动应急预案，尽快恢复交易业务，并按有关要求及时上报公司和证券营业部所在地证监局。应急事件处理完成后，应以书面形式上报公司和证券营业部所在地证监局。	a)检查应急处理记录，确认营业部发生影响交易业务的技术故障时，证券公司是否立即启动应急预案，尽快恢复交易业务； b)检查故障上报记录，确认营业部发生影响交易业务的技术故障时，是否按有关要求及时上报公司和证券营业部所在地证监局； c)查看故障报告等相关上报记录，确认应急事件处理完成后，以书面形式上报公司和证券营业部所在地证监局。	是□ 否□ 不适用□	

表 K.2 A 型营业部审计底稿（续）

序号	审计项	审计程序	审计结论	备注
3.18.	证券公司是否加强证券营业部设备选型、购置、登记、保养、维修、报废等设备管理，确保对关键设备建立维护档案。	a)查看证券公司发布的证券营业部设备管理的相关规定，规定是否包含设备选型、购置、登记、保养、维修、报废等设备管理要求，并要求对关键设备建立维护档案； b)查看证券公司检查营业部设备管理的记录，确认相关规定的有效执行。	是□ 否□ 不适用□	
3.19.	证券公司是否统一管理和指导证券营业部进行生产环境下的测试工作，制定详细的测试计划，并确保做好系统、数据和应用程序测试前的备份工作。测试完成后做好系统的恢复和验证等工作。	a)查看证券公司发布的证券营业部信息系统测试的相关规定，规定是否包含进行生产环境下测试工作时，制定详细的测试计划，并确保做好系统、数据和应用程序测试前的备份工作，测试完成后做好系统的恢复和验证等工作的相关内容； b)查看证券公司指导和检查营业部设备管理的记录，确认相关规定的有效执行。	是□ 否□ 不适用□	
3.20.	证券公司是否确保证券营业部在供电、网络通信、服务器、现场交易服务相关系统等关键设备或系统变更时经过严格的测试。	a)查看证券公司发布的证券营业部系统关键设备与系统变更测试的相关规定，规定是否包含在供电、网络通信、服务器、现场交易服务相关系统等关键设备或系统变更时经过严格的测试的相关内容； b)查看证券公司检查营业部系统关键设备与系统变更的记录，确认相关规定的有效执行。	是□ 否□ 不适用□	
3.21.	证券公司是否确保证券营业部在信息系统变更前制定详细的变更方案和变更应急预案，并做好系统和数据的备份。	a)查看证券公司发布的证券营业部系统变更的相关规定，规定是否包含在信息系统变更前制定详细的变更方案和变更应急预案，并做好系统和数据的备份的相关内容； b)查看证券公司检查营业部系统变更情况的记录，确认相关规定的有效执行。	是□ 否□ 不适用□	
3.22.	证券公司是否统一制定证券营业部信息系统故障应急处理流程，并确保证券营业部建立信息系统应急预案并及时更新。	a)查看证券公司发布的证券营业部应急预案和应急处理的相关规定，规定是否包含统一制定证券营业部信息系统故障应急处理流程，并要求证券营业部建立信息系统应急预案并及时更新的相关内容； b)查看证券公司检查营业部应急预案和应急处理更新情况的记录，确认相关规定的有效执行。	是□ 否□ 不适用□	

附 录 L
（规范性附录）
B 型营业部审计底稿

表L.1至表L.2给出了B型营业部审计的程序、内容及相关记录要求。

表L.1 B 型营业部审计底稿

被审计部门：	索引号： YYB-B-XXX
审计主题：B 型营业部	审计年度：
审计结论、意见及建议： 编制人： 年 月 日 （部门盖章）	
复核意见： 复核人： 年 月 日 （部门盖章）	
被审计部门意见： 年 月 日 （部门盖章）	

表 L.1　B 型营业部审计底稿（续）

审计证据列表：

表L.2　B型营业部审计底稿

序号	审计项	审计程序	审计结论	备注
1.	**安全管理**			
1.1.	是否确保证券营业部局域网与公司广域网、互联网实现有效隔离。	a)检查“表0.16-B型营业部-网络边界防护情况”，审阅网络拓扑图，查看防火墙、入侵检测等安全设备的配备情况； b)查看安全设备是否配置接口参数、过滤规则，网络设备的安全规则是否配置允许访问规则，控制粒度为网段级，对没有明确定义的数据包缺省拒绝； c)检查安全测试记录或第三方安全测试报告，确认网络和安全设备运行的有效性。	是□ 否□ 不适用□	
1.2.	是否确保证券营业部及时更新系统补丁、升级系统安全防护软件，定期进行全面的病毒和木马检测，发现病毒和木马立即处理并报告。移动存储、外来电子文档、软件系统使用前应进行病毒和木马查杀。	a)查看营业部信息技术管理制度，确认有关于证券营业部及时更新系统补丁、升级系统安全防护软件，定期进行全面的病毒和木马检测，发现病毒和木马立即处理并报告等规定； b)查看病毒和木马查杀记录，确认及时更新系统补丁、升级系统安全防护软件，定期进行全面的病毒和木马检测，发现病毒和木马立即处理并报告。移动存储、外来电子文档、软件系统使用前应进行病毒和木马查杀。	是□ 否□ 不适用□	
1.3.	是否证券营业部部署防病毒、防木马、防恶意代码等系统安全防护软件，保护证券营业部信息系统安全。	检查“表0.16-B型营业部-安全防护情况”，查看防护软件安装记录，抽查实际安装情况，确认证券营业部部署防病毒、防木马、防恶意代码等系统安全防护软件。	是□ 否□ 不适用□	
1.4.	证券公司是否加强证券营业部网络安全管理，确保证券营业部不得擅自对外互联或设立网站。如确有必要，证券公司应对网站的设立和维护进行统一管理。	a)查看证券公司发布的证券营业部对外互联、设立网站相关规定，规定是否包含证券营业部不得擅自对外互联或设立网站的相关内容； b)查看证券公司对营业部对外互联或设立网站的审批记录，确认证券营业部禁止擅自对外互联或设立网站。如确有必要，证券公司应对网站的设立和维护进行统一管理。	是□ 否□ 不适用□	
2.	**系统建设**			
2.1.	与证券营业部之间是否采用至少2条不同运营商或不同介质的通信线路，建立安全、可靠通信连接，且线路带宽能够满足证券营业部业务需要并留有冗余。	a)检查“表0.16-B型营业部-内部通信连接情况”，检查网络设计文档或验收文档，判断与证券营业部之间是否采用至少2条不同运营商或不同介质的通信线路，且线路带宽能够满足证券营业部业务需要； b)检查网络设备清单，判断网络通信设备是否有冗余备份。	是□ 否□ 不适用□	

表 L.2　B 型营业部审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.2.	B型证券营业部的通信线路中是否有一条为地面数据专线。	检查“表 0.16-B 型营业部-内部通信连接情况”，检查网络设计文档或验收文档，判断通信线路中是否有一条为地面数据专线。	是□ 否□ 不适用□	
2.3.	是否确保B型证券营业部提供至少2种相互独立的行情揭示系统、委托方式。	检查“表 0.16-B 型营业部--行情揭示软件情况”，检查行情委托系统验收文档，是否提供至少 2 种相互独立的行情揭示系统、委托方式。	是□ 否□ 不适用□	
2.4.	是否选择具备可靠供电的场所。	a)检查“表 0.16-B 型营业部-电力情况-供电方式”，检查相关材料或者询问楼宇物业、机房管理员等人员，确认最近两年内所在楼宇区域是否工作时间段内每年停电不超过 2 次，每次停电时间不超过 2 小时； b)检查相关材料或者询问楼宇物业、机房管理员等人员，供电电压是否稳定。	是□ 否□ 不适用□	
2.5.	是否远离强震源、强磁场源和强噪声源，远离电磁干扰源或实施有效电磁干扰防护。	检查楼宇物业或者机房建设的相关材料，实地检查机房环境，是否远离强震源、强磁场源和强噪声源，远离电磁干扰源或实施有效电磁干扰防护。	是□ 否□ 不适用□	
2.6.	证券营业部机房选址是否远离产生粉尘、油烟、有害气体以及具有腐蚀性、易燃、易爆物品的工厂、仓库等场所。	检查楼宇物业或者机房建设的相关材料，实地检查机房环境，是否远离产生粉尘、油烟、有害气体以及具有腐蚀性、易燃、易爆物品的工厂、仓库等场所。	是□ 否□ 不适用□	
2.7.	是否符合当地抗震强度要求。	检查楼宇物业或者机房建设的相关材料，实地检查机房环境，是否符合当地抗震强度要求。	是□ 否□ 不适用□	
2.8.	是否符合当地消防主管部门的消防安全要求。	检查“表 0.16-B 型营业部-消防情况”，检查机房建设或者机房消防的相关材料，确认机房符合当地消防主管部门的消防安全要求。	是□ 否□ 不适用□	
2.9.	证券营业部机房是否具备独立空调系统，使机房温度保持在23℃±5℃范围内。	a)检查营业部机房内是否配备了独立空调系统，是否能够正常运行； b)检查营业部机房温度记录，是否控制在23℃±5℃范围内。	是□ 否□ 不适用□	
2.10.	机房供电是否具有独立于一般照明电的专用供电线路。	检查机房电路设计及验收文档，判断机房供电是否具有独立于一般照明电的专用供电线路。	是□ 否□ 不适用□	
2.11.	机房供电是否设有独立的配电柜或配电箱。	现场确认设有独立的配电柜或配电箱。	是□ 否□ 不适用□	

表 L.2　B 型营业部审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.12.	机房供电是否相关电器设备、电线应与机柜用电负载相适应，并留有余量。	检查机房电路设计及验收文档、机柜用电负载说明文档，确认相关电器设备、电线是否与机柜用电负载相适应，并留有余量。	是□ 否□ 不适用□	
2.13.	机房是否配置UPS电源。	检查“表 0.16-B 型营业部-UPS”，现场检查是否配置 UPS 电源，并且 UPS 电源处于工作状态。	是□ 否□ 不适用□	
2.14.	机房供电是否禁止将与业务无关的设备接入UPS电源。	a)检查是否配置 UPS 电源； b)检查是否禁止将与业务无关的设备接入 UPS 电源。	是□ 否□ 不适用□	
2.15.	机房供电是否市电插座与UPS插座应严格区分，插座面板应有提示性的标识或标签。	a)检查是否配置 UPS 电源； b)检查市电插座与 UPS 插座是否严格区分，插座面板是否有提示性的标识或标签。	是□ 否□ 不适用□	
2.16.	B型证券营业部是否至少配备一种持续供电方式，在市电中断情况下，保证不低于25%的现场交易终端或同等支持能力的其他交易终端在交易时间内持续工作，满足证券营业部客户现场交易需要。	a)检查“表 0.16-B 型营业部-UPS”、“表 0.16-B 型营业部-发电机”，检查是否具有双路市电供电，应当说明双路供电的来源； b)如果没有双路市电供电，检查则 UPS 和后备发电设施的供电时间在市电中断情况下，是否可以保证不低于 25%的现场交易终端或同等支持能力的其他交易终端在交易时间内持续工作，满足证券营业部客户现场交易需要。	是□ 否□ 不适用□	
2.17.	证券营业部配备或租用发电机的，发电机是否安装在具有良好通风的场地内，并远离易燃易爆物品。	a)检查机房设备管理清单，确认包括配备或租用发电机； b)实地检查发动机，确认安装在具有良好通风的场地内，并远离易燃易爆物品。	是□ 否□ 不适用□	
2.18.	是否配备防火防盗门等有效安保设施。	实地检查机房入口，确认配备防火防盗门等有效安保设施。	是□ 否□ 不适用□	
2.19.	证券公司与证券营业部之间网络通信设备是否具有冗余备份，保证发生故障时实现及时切换。	a)检查网络设计文档或验收文档，判断与证券营业部之间是否采用至少 2 条不同运营商或不同介质的通信线路，且线路带宽能够满足证券营业部业务需要。 b)检查网络设备清单，判断网络通信设备是否有冗余备份。	是□ 否□ 不适用□	

表 L.2 B 型营业部审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.20.	证券公司是否根据业务需要，合理划分证券营业部局域网安全域，确定各安全域的功能定位，在各安全域之间采取安全措施实现有效隔离。	查看包括自建和托管机房的网络拓扑图、安全域划分情况，检查各安全域之间是否根据业务需要，合理划分局域网安全域，是否采用了防火墙或安全网关等有效隔离方式和隔离手段。	是□ 否□ 不适用□	
2.21.	证券公司是否制定证券营业部局域网、公司广域网、互联网接入以及安全防护的网络建设规范，并统一规划管理证券营业部网络配置参数和IP地址段。	a)查看证券公司发布的证券营业部网络互联与接入、安全防护建设规范，规定是否包含证券营业部局域网、公司广域网、互联网接入以及安全防护的网络建设规范的相关内容； b)查看证券公司给营业部的网络配置参数和 IP 地址段分配表，确认统一规划管理证券营业部网络配置参数和 IP 地址段。	是□ 否□ 不适用□	
2.22.	证券公司是否对证券营业部与客户建立的网络连接进行审批，对连接方式进行统一规划和管理，并采取安全措施，实现有效隔离。	a)查看证券公司发布的证券营业部与客户建立网络连接的规定，规定是否包含连接方式进行统一规划和管理，并采取安全措施，实现有效隔离的相关内容； b)查看证券公司审批、检查营业部与客户建立网络连接的记录，确认相关规定的有效执行。	是□ 否□ 不适用□	
2.23.	证券公司是否确保证券营业部提供行情、开户、交易、资讯等客户服务的信息系统，具备足够的健壮性，系统处理能力具有一定的冗余度，并采用热备或冷备等手段，避免单点故障，提高系统可用性。	a)检查“表 0.16-B 型营业部-行情资讯软件情况”、“表 0.16-B 型营业部-行情接收情况”，，查看证券公司发布的证券营业部信息系统建设的相关规定，规定是否包含证券营业部提供行情、开户、交易、资讯等客户服务的信息系统，具备足够的健壮性，系统处理能力具有一定的冗余度，并采用热备或冷备等手段，避免单点故障，提高系统可用性的相关内容； b)查看证券公司审批、检查营业部信息系统建设的记录，确认相关规定的有效执行。	是□ 否□ 不适用□	
3.	**运维管理**			
3.1.	B型证券营业部是否至少配备一名兼职技术人员。	检查“表 0.16-B 型营业部-IT 人员情况”，检查证券营业部类型和信息技术人员名单，判断 B 型证券营业部是否至少配备一名兼职技术人员。	是□ 否□ 不适用□	

表 L.2　B 型营业部审计底稿（续）

序号	审计项	审计程序	审计结论	备注
3.2.	证券营业部专职技术人员和兼职技术人员是否具有计算机相关专业学历或从事信息技术工作1年以上。	a)检查营业部信息技术人员简历，判断专职技术人员和兼职技术人员是否具有计算机相关专业学历或从事信息技术工作 1 年以上； b)检查营业部信息技术人员简历，判断专职技术人员和兼职技术人员是否具有计算机相关专业学历或从事信息技术工作 1 年以上。	是□ 否□ 不适用□	
3.3.	营业部是否制定顶岗、备岗等相关制度，确保在交易时间内有技术人员值守。	查看营业部顶岗、备岗等相关制度，检查操作记录，访谈营业部技术人员，判断是否在交易时间内有技术人员值守。	是□ 否□ 不适用□	
3.4.	B型证券营业部外包的信息系统运维工作，是否与外包服务提供单位签订外包合同与保密协议，确保信息系统安全运行、风险可控。	a)检查是否存在证券营业部与外包服务提供单位签订外包合同与保密协议； b)检查外包合同与保密协议中是否存在确保信息系统安全运行、风险可控条款。	是□ 否□ 不适用□	
3.5.	B型证券营业部外包的信息系统运维工作，是否禁止授予外包人员业务系统操作权限。	a)检查权限分配表，确认权限分配表中没有外包人员操作权限； b)检查系统账户与权限是否与权限分配表一致。	是□ 否□ 不适用□	
3.6.	是否加强证券营业部网络配置、访问控制、安全审计等网络管理，确保证券营业部的网络设备按最小安全访问原则设置访问控制权限，每一次变更后及时更新备份网络设备的配置信息。	a)检查营业部访问控制策略，访谈网络管理员，判断营业部的网络设备是否按最小安全访问原则设置访问控制权限； b)检查变更记录，判断每一次变更后是否及时更新备份网络设备的配置信息。	是□ 否□ 不适用□	
3.7.	证券营业部是否加强计算机终端的管理，记录网卡地址，防止非法使用。未经许可，不得将客户和员工的自备计算机接入证券营业部网络。	a)是否营业部有终端接入管理记录、记录网卡地址； b)是否有效防止非法使用。	是□ 否□ 不适用□	
3.8.	证券营业部提供无线网络服务的，证券公司是否统一制定证券营业部无线网络使用规范，采取有效的无线网络准入控制措施，登记并记录无线接入设备的信息。	a)证券公司是否统一制定证券营业部无线网络使用规范； b)查看营业部终端接入管理记录、营业部无线网络准入记录，检查营业部终端接入管理措施是否有效、无线网络使用规范是否落实。	是□ 否□ 不适用□	

表 L.2　B 型营业部审计底稿（续）

序号	审计项	审计程序	审计结论	备注
3.9.	是否加强证券营业部技术文档的收集、更新、保管、借阅等管理，确保证券营业部根据信息系统的变更情况及时更新技术文档。证券营业部技术文档包括但不限于机房平面图、供配电图、网络拓扑图、信息点对照表、系统手册、应急预案、运维日志、设备维护档案等资料。	a)检查文档管理制度，是否对营业部技术文档加强管理，包括收集、更新、保管、借阅等； b)检查证券营业部技术文档，是否包括但不限于机房平面图、供配电图、网络拓扑图、信息点对照表、系统手册、应急预案、运维日志、设备维护档案等资料。	是□ 否□ 不适用□	
3.10.	是否加强证券营业部数据备份、存放、保密、调阅、销毁等数据管理，确保证券营业部指定专人负责数据管理，数据调阅须经审批，且不得对外泄露。	a)检查数据管理制度，是否加强证券营业部数据备份、存放、保密、调阅、销毁等数据管理； b)访谈数据管理人员，判断是否指定专人负责数据管理，数据调阅须经审批，且不得对外泄露。	是□ 否□ 不适用□	
3.11.	证券营业部是否在关键系统和关键设备的用户管理上遵循权限最小化原则，建立用户和权限的清单，定期进行检查核对。用户和权限变更应执行相关审批流程，并保留完整的变更记录。	a)检查关键系统和关键设备用户和权限清单，确认用户管理上遵循权限最小化原则； b)检查关键系统和关键设备用户和权限定期检查记录，确认定期检查核对相关内容； c)检查用户和权限变更审批记录、变更记录，确认用户和权限变更应执行相关审批流程，并保留完整的变更记录。	是□ 否□ 不适用□	
3.12.	是否证券营业部关键系统和关键设备的管理员用户密码实行专人管理，采用不低于8位的复合密码，每半年至少更换一次。发生人员变动时应及时更新密码。	a)检查口令管理办法，确认关键系统和关键设备的管理员用户密码实行专人管理，采用不低于 8 位的复合密码，每半年至少更换一次。发生人员变动时应及时更新密码； b)检查密码变动记录，确认是否至少每半年更新一次密码，确认管理人变动时及时更新密码。	是□ 否□ 不适用□	
3.13.	证券营业部是否至少每半年检查一次电力、机房空调、消防等设施，每季度选择非交易时间进行UPS电池的充放电测试，并详细记录。	检查机房基础设施定期检查记录，确认是否每半年检查一次电力、机房空调、消防等设施，每季度选择非交易时间进行 UPS 电池的充放电测试的记录。	是□ 否□ 不适用□	

表 L.2　B 型营业部审计底稿（续）

序号	审计项	审计程序	审计结论	备注
3.14.	是否B型证券营业部对系统运维日志进行规范管理，日常操作及异常事件处理应在系统运维日志中详细记录。运维日志可采用电子文档或纸质件记录，并妥善保管，保留期限不少于2年。	a)检查系统运维日志管理办法，确认对系统运维日志进行规范管理； b)抽查近 2 年的运维日志，判断日常操作及异常事件处理是否在系统运维日志中详细记录。	是□ 否□ 不适用□	
3.15.	是否对证券营业部安装使用的应用软件进行统一管理，证券营业部不得擅自安装与业务及技术维护无关的应用软件。	a)如果有应用软件统一管理平台，检查应用软件统一管理平台的采购合同、日志记录和分析报告，确认有效阻止擅自安装与业务及技术维护无关的应用软件； b)如果没有应用软件统一管理平台，检查应用软件统一管理制度和检查记录，确认阻止擅自安装与业务及技术维护无关的应用软件。	是□ 否□ 不适用□	
3.16.	是否配备应急照明装置。	a)检查应急物资资产记录、盘点更新记录，确认配备一定数量的应急照明装置； b)实地检查确认应急照明装置。	是□ 否□ 不适用□	
3.17.	是否证券营业部每年至少进行两次应急演练，并留存演练记录。	a)检查应急管理制度，是否要求每年至少进行二次演练； b)检查应急演练记录，确认每年至少进行两次应急演练。	是□ 否□ 不适用□	
3.18.	营业部发生影响交易业务的技术故障时，证券公司是否立即启动应急预案，尽快恢复交易业务，并按有关要求及时上报公司和证券营业部所在地证监局。应急事件处理完成后，应以书面形式上报公司和证券营业部所在地证监局。	a)检查应急处理记录，确认营业部发生影响交易业务的技术故障时，证券公司是否立即启动应急预案，尽快恢复交易业务； b)检查故障上报记录，确认营业部发生影响交易业务的技术故障时，是否按有关要求及时上报公司和证券营业部所在地证监局； c)查看故障报告等相关上报记录，确认应急事件处理完成后，以书面形式上报公司和证券营业部所在地证监局。	是□ 否□ 不适用□	
3.19.	证券公司是否加强证券营业部设备选型、购置、登记、保养、维修、报废等设备管理，确保对关键设备建立维护档案。	a)查看证券公司发布的证券营业部设备管理的相关规定，规定是否包含设备选型、购置、登记、保养、维修、报废等设备管理要求，并要求对关键设备建立维护档案； b)查看证券公司检查营业部设备管理的记录，确认相关规定的有效执行。	是□ 否□ 不适用□	

表 L.2 B 型营业部审计底稿（续）

序号	审计项	审计程序	审计结论	备注
3.20.	证券公司是否统一管理和指导证券营业部进行生产环境下的测试工作，制定详细的测试计划，并确保做好系统、数据和应用程序测试前的备份工作。测试完成后做好系统的恢复和验证等工作。	a)查看证券公司发布的证券营业部信息系统测试的相关规定，规定是否包含进行生产环境下测试工作时，制定详细的测试计划，并确保做好系统、数据和应用程序测试前的备份工作，测试完成后做好系统的恢复和验证等工作的相关内容； b)查看证券公司指导和检查营业部设备管理的记录，确认相关规定的有效执行。	是□ 否□ 不适用□	
3.21.	证券公司是否确保证券营业部在供电、网络通信、服务器、现场交易服务相关系统等关键设备或系统变更时经过严格的测试。	a)查看证券公司发布的证券营业部系统关键设备与系统变更测试的相关规定，规定是否包含在供电、网络通信、服务器、现场交易服务相关系统等关键设备或系统变更时经过严格的测试的相关内容； b)查看证券公司检查营业部系统关键设备与系统变更的记录，确认相关规定的有效执行。	是□ 否□ 不适用□	
3.22.	证券公司是否确保证券营业部在信息系统变更前制定详细的变更方案和变更应急预案，并做好系统和数据的备份。	a)查看证券公司发布的证券营业部系统变更的相关规定，规定是否包含在信息系统变更前制定详细的变更方案和变更应急预案，并做好系统和数据的备份的相关内容； b)查看证券公司检查营业部系统变更情况的记录，确认相关规定的有效执行。	是□ 否□ 不适用□	
3.23.	证券公司是否统一制定证券营业部信息系统故障应急处理流程，并确保证券营业部建立信息系统应急预案并及时更新。	a)查看证券公司发布的证券营业部应急预案和应急处理的相关规定，规定是否包含统一制定证券营业部信息系统故障应急处理流程，并要求证券营业部建立信息系统应急预案并及时更新的相关内容； b)查看证券公司检查营业部应急预案和应急处理更新情况的记录，确认相关规定的有效执行。	是□ 否□ 不适用□	

附 录 M
（规范性附录）
C 型营业部审计底稿

表M.1至表M.2给出了C型营业部审计的程序、内容及相关记录要求。

表M.1 C 型营业部审计底稿

被审计部门：	索引号：YYB-C-XXX
审计主题：C 型营业部	审计年度：
审计结论、意见及建议： 编制人： 年 月 日 （部门盖章）	
复核意见： 复核人： 年 月 日 （部门盖章）	
被审计部门意见： 年 月 日 （部门盖章）	

表 M.1　C 型营业部审计底稿（续）

审计证据列表： 、

表M.2　C型营业部审计底稿

序号	审计项	审计程序	审计结论	备注
1.	**安全管理**			
1.1.	是否确保证券营业部及时更新系统补丁、升级系统安全防护软件，定期进行全面的病毒和木马检测，发现病毒和木马立即处理并报告。移动存储、外来电子文档、软件系统使用前应进行病毒和木马查杀。	a)查看营业部信息技术管理制度，确认有关于证券营业部及时更新系统补丁、升级系统安全防护软件，定期进行全面的病毒和木马检测，发现病毒和木马立即处理并报告等规定； b)查看病毒和木马查杀记录，确认及时更新系统补丁、升级系统安全防护软件，定期进行全面的病毒和木马检测，发现病毒和木马立即处理并报告。移动存储、外来电子文档、软件系统使用前应进行病毒和木马查杀。	是□ 否□ 不适用□	
1.2.	是否证券营业部部署防病毒、防木马、防恶意代码等系统安全防护软件，保护证券营业部信息系统安全。	检查“表0.12-C型营业部-安全防护情况”，查看防护软件安装记录，抽查实际安装情况，确认证券营业部部署防病毒、防木马、防恶意代码等系统安全防护软件。	是□ 否□ 不适用□	
1.3.	证券公司是否加强证券营业部网络安全管理，确保证券营业部不得擅自对外互联或设立网站。如确有必要，证券公司应对网站的设立和维护进行统一管理。	a)查看证券公司发布的证券营业部对外互联、设立网站相关规定，规定是否包含证券营业部不得擅自对外互联或设立网站的相关内容。 b)查看证券公司对营业部对外互联或设立网站的审批记录，确认证券营业部禁止擅自对外互联或设立网站。如确有必要，证券公司应对网站的设立和维护进行统一管理。	是□ 否□ 不适用□	
2.	**运维管理**			
2.1.	证券营业部是否加强计算机终端的管理，记录网卡地址，防止非法使用。未经许可，不得将客户和员工的自备计算机接入证券营业部网络。	a)是否营业部有终端接入管理记录、记录网卡地址； b)是否有效防止非法使用。	是□ 否□ 不适用□	
2.2.	是否对证券营业部安装使用的应用软件进行统一管理，证券营业部不得擅自安装与业务及技术维护无关的应用软件。	a)如果有应用软件统一管理平台，检查应用软件统一管理平台的采购合同、日志记录和分析报告，确认有效阻止擅自安装与业务及技术维护无关的应用软件； b)如果没有应用软件统一管理平台，检查应用软件统一管理制度和检查记录，确认阻止擅自安装与业务及技术维护无关的应用软件。	是□ 否□ 不适用□	

附 录 N
（规范性附录）
信息系统托管审计底稿

表N.1至表N.2给出了信息系统托管审计的程序、内容及相关记录要求。

表N.1 信息系统托管审计底稿

被审计部门：	索引号：TGSJ
审计主题：托管审计	审计年度：
审计结论、意见及建议： 编制人： 年 月 日 （部门盖章）	
复核意见： 复核人： 年 月 日 （部门盖章）	
被审计部门意见： 年 月 日 （部门盖章）	

表 N.1　信息系统托管审计底稿(续)

审计证据列表：

表N.2 信息系统托管审计底稿

序号	审计项	审计程序	审计结论	备注
1	**机柜要求**			
1.1	**基础设施要求**			
1.1.1	机柜所在机房是否满足GB 50174中B级机房要求。（本项适用于：二级系统托管）	检查机房满足GB 50174中B级机房的设计验收材料，确认机柜所在机房满足B级机房要求。	是□ 否□ 不适用□	
1.1.2	机柜所在机房是否满足GB 50174中A级机房要求。（本项适用于：三级、三+系统托管）	检查机房满足GB 50174中A级机房的设计验收材料，确认机柜所在机房满足A级机房要求。	是□ 否□ 不适用□	
1.1.3	机柜的结构尺寸、机电接口、机械性能、外观要求、通风散热等技术指标是否满足GB/T 23359和GB/T 22690的要求。	检查机柜的技术指标满足GB/T 23359和GB/T 22690的要求的合格证，确认机柜的技术指标满足GB/T 23359和GB/T 22690的要求。	是□ 否□ 不适用□	
1.1.4	在证券期货交易时段，机柜的电力可用性是否达到99.9%。（本项适用于：二级系统托管）	检查“表O.3-本年度交易时段双路失电的时间”，计算近一年交易时段双路未失电的时间占比，确定是否达到99.9%；或检查近一年交易时段机柜的电力可用性达到99.9%的证明材料，确认电力可用性达到99.9%	是□ 否□ 不适用□	
1.1.5	在证券期货交易时段，机柜的电力可用性是否达到99.99%。（本项适用于：三级、三+系统托管）	检查“表O.3-本年度交易时段双路失电的时间”，计算证券期货近一年交易时段双路未失电的时间占比，确定是否达到99.99%；或检查近一年交易时段机柜的电力可用性达到99.99%的证明材料，确认电力可用性达到99.99%。	是□ 否□ 不适用□	
1.1.6	机柜是否配置两路独立的电源分配模块，并且每个机柜的供电是否由独立开关控制。（本项适用于：三级、三+系统托管）	检查照片或证明材料，确认机柜配置了两路独立的电源分配模块，并且每个机柜的供电由独立开关控制。	是□ 否□ 不适用□	
1.1.7	机柜内强弱电线路是否以不同标识或颜色区分，是否确保线路安置清晰整洁。	检查照片或证明材料，确认机柜内强弱电线路是否以不同标识或颜色区分，线路安置是否清晰整洁。	是□ 否□ 不适用□	
1.1.8	机柜所在机房区域的温湿度是否达到GB 50174中B级的有关要求。（本项适用于：二级系统托管）	检查机柜所在机房区域的温湿度的巡检记录，或达到GB 50174中B级的有关要求的证明材料，确认温湿度达到GB 50174中B级的有关要求。	是□ 否□ 不适用□	

表 N.2　信息系统托管审计底稿（续）

序号	审计项	审计程序	审计结论	备注
1.1.9	机柜所在机房精密空调至少采用 N+1 方式冗余，机柜所在机房区域的温湿度是否达到 GB 50174 中 A 级的有关要求。（本项适用于：三级、三+系统托管）	a)检查机柜所在机房精密空调部署图，确认是否至少采用 N+1 方式冗余； b)检查机柜所在机房区域的温湿度的巡检记录，或达到 GB 50174 中 A 级的有关要求的证明材料，确认温湿度达到 GB 50174 中 A 级的有关要求。	是□ 否□ 不适用□	
1.1.10	机柜所在机房是否配置环境监控系统，能够对机柜所在机房的支路供电、温度、湿度等关键指标进行自动实时监控和报警。（本项适用于：三级、三+系统托管）	检查机柜所在机房环境监控系统，确认是否能够对机柜所在机房的支路供电、温度、湿度等关键指标进行自动实时监控和报警。	是□ 否□ 不适用□	
1.1.11	机柜所在区域消防系统是否采用高效灭火系统和火灾自动报警系统，并通过当地消防部门验收。	检查机柜所在区域消防系统通过当地消防部门验收证明，确认消防系统通过当地消防部门验收。	是□ 否□ 不适用□	
1.1.12	受托方是否做好机柜所在机房基础设施的日常巡检工作，每日巡检次数不少于三次。（本项适用于：二级系统托管）	检查机房基础设施的日常巡检相关制度和记录，确认每日巡检次数不少于三次。	是□ 否□ 不适用□	
1.1.13	受托方是否做好机柜所在机房基础设施的日常巡检工作，每日巡检次数不少于六次。（本项适用于：三级、三+系统托管）	检查机房基础设施的日常巡检相关制度和记录，确认每日巡检次数不少于六次。	是□ 否□ 不适用□	
1.1.14	受托方是否配备7×24小时值班基础设施管理员，负责机柜所在机房及机柜基础设施的日常维护、事件应急、故障处置等工作。	检查基础设施值班相关制度、排班表及管理员职责说明，确认配备了7×24小时值班基础设施管理员，负责机柜所在机房及机柜基础设施的日常维护、事件应急、故障处置等工作。	是□ 否□ 不适用□	
1.2	**网络通信要求**			
1.2.1	受托方是否提供网络线路接入条件，满足委托方交易专网、互联网、数据专线等网络通信需求。	检查“表 0.6-卫星通信情况”、“表 0.6-地面通信情况”，确认受托方提供了多个运营商的网络线路接入条件。	是□ 否□ 不适用□	

表 N.2　信息系统托管审计底稿（续）

序号	审计项	审计程序	审计结论	备注
1.2.2	受托方是否提供至少两家基础通信运营商的线路接入资源，且每家基础通信运营商至少采用两种不同的物理路由接入局端机房。（本项适用于：三级、三+系统托管）	检查“表 0.6-卫星通信情况”、“表 0.6-地面通信情况”，确认是否提供两家基础通信运营商的线路接入资源，且每家基础通信运营商至少采用两种不同的物理路由接入局端机房。	是□ 否□ 不适用□	
1.2.3	机柜网络接入集中网络前是否采取有效的安全防护措施，实现机柜网络环境与其它区域网络环境的有效隔离。	a)检查“表 0.3-网络边界防护情况”、网络设计文档或网络验收文档及网络拓扑图，查看重要网段的部署方式； b)检查边界和主要网络设备，查看重要网段是否采取了技术隔离手段与其他网段隔离。	是□ 否□ 不适用□	
1.2.4	受托方是否 7×24 小时对机房公共网络运行情况进行实时监控，受托方未经委托方授权，禁止监听、获取、复制、利用通过网络传输的信息系统数据信息。	a）检查机房公共网络运行维护手册和监控记录，确认受托方 7×24 小时对机房公共网络运行情况进行实时监控； b）检查保密承诺书，确认未经委托方授权，禁止监听、获取、复制、利用通过网络传输的信息系统数据信息。〞	是□ 否□ 不适用□	
1.2.5	受托方是否配备 7×24 小时网络支持人员，负责其提供的机柜公共网络的日常维护、事件应急、故障处置等工作。	检查网络值班制度、岗位职责说明、值班记录，确认受托方配备 7×24 小时网络支持人员，负责其提供的机柜公共网络的日常维护、事件应急、故障处置等工作。	是□ 否□ 不适用□	
1.3	**安全保卫要求**			
1.3.1	受托方是否为机柜提供电子锁或机械锁。受托方可留有备用钥匙以备应急使用，但是否提前获得委托方同意，并记录使用情况。	检查机柜锁照片、应急相关制度和记录，确认受托方为机柜提供电子锁或机械锁。受托方可留有备用钥匙以备应急使用，但应提前获得委托方同意，并记录使用情况。	是□ 否□ 不适用□	
1.3.2	受托方是否对机柜所在机房设置视频监控设备，监控范围覆盖机柜操作面、机柜所在机房出入口等关键区域。连续视频监控记录是否保存至少90天。	a)检查机房运行维护手册，确认受托方对机柜所在机房设置视频监控设备，监控范围覆盖机柜操作面、机柜所在机房出入口等关键区域； b)抽查视频监控记录，确认连续视频监控记录保存至少 90 天。	是□ 否□ 不适用□	

表 N.2　信息系统托管审计底稿（续）

序号	审计项	审计程序	审计结论	备注
1.3.3	受托方是否在机柜所在建筑物入口处安装出入控制和安全防护装置，包括闸机、防爆桶、X射线安全检查设备等，并对出入人员和所带物品是否进行安全检查。（本项适用于：三级、三+系统托管）	a)检查机房运行维护手册，确认受托方在机柜所在建筑物入口处安装出入控制和安全防护装置，包括闸机、防爆桶、X 射线安全检查设备等，并对出入人员和所带物品应进行安全检查； b)现场检查机柜所在建筑物入口处安装出入控制和安全防护装置，包括闸机、防爆桶、X 射线安全检查设备等，确认对出入人员和所带物品进行安全检查。	是□ 否□ 不适用□	
1.3.4	受托方是否对机柜所在区域出入人员身份执行审批审核流程，并记录出入人员信息、进出时间、工作内容等，相关记录是否保存至少 360 天。	检查人员出入审批审核流程和进出记录，确认包括人员信息、进出时间、工作内容等，相关记录应保存至少 360 天。	是□ 否□ 不适用□	
1.3.5	受托方是否配备 7×24 小时值班保安人员，负责机柜所在机房的安全保卫工作。	检查日常值班表 日常值班制度，确认受托方配备 7×24 小时值班保安人员，负责机柜所在机房的安全保卫工作。	是□ 否□ 不适用□	
1.4	**运维保障**			
1.4.1	受托方是否制定并完善对机柜的运维管理相关制度，包括对机柜所在机房、机柜本身、网络通信、安全保卫等运维操作流程、操作手册、故障处理、应急预案、应急联络人联络方式等，并提供给委托方。	检查委托方是否有受托方的运维管理制度，包括对机柜所在机房、机柜本身、网络通信、安全保卫等运维操作流程、操作手册、故障处理、应急预案、应急联络人联络方式。	是□ 否□ 不适用□	
1.4.2	受托方是否为委托方提供信息系统运维和监控的场地条件，根据委托方要求，提供公共监控工位，满足委托方运维和监控需要。（本项适用于：二级系统托管）	查看场地租赁合同，访谈现场办公人员，确认受托方为委托方提供了信息系统运维和监控的场地条件，根据委托方要求，提供公共监控工位，满足委托方运维和监控需要。	是□ 否□ 不适用□	

表 N.2　信息系统托管审计底稿（续）

序号	审计项	审计程序	审计结论	备注
1.4.3	受托方是否为委托方提供信息系统运维和监控的场地条件，根据委托方要求，提供专用监控工位或监控室，满足委托方运维和监控需要。（本项适用于：三级、三+系统托管）	查看场地租赁合同，访谈现场办公人员，确认受托方为委托方提供了信息系统运维和监控的场地条件，根据委托方要求，提供专用监控工位或监控室，满足委托方运维和监控需要。	是□ 否□ 不适用□	
1.4.4	受托方是否向委托方告知值班基础设施管理员、网络管理员、保安人员的职责，并公布值班电话。	查看基础设施管理员、网管、保安职责和值班电话，确认受托方向委托方告知值班基础设施管理员、网络管理员、保安人员的职责、值班电话等信息。	是□ 否□ 不适用□	
1.4.5	受托方在进行重大变更时，是否提前至少 10 个工作日通过书面方式通知可能受到影响的委托方。（本项适用于：二级系统托管）	查看变更管理制度和变更通知，确认受托方在进行重大变更时，至少提前 10 个工作日通过书面方式通知可能受到影响的委托方。	是□ 否□ 不适用□	
1.4.6	受托方在进行重大变更时，是否提前至少 20 个工作日通过书面方式通知可能受到影响的委托方。（本项适用于：三级系统托管）	查看变更管理制度和变更通知，确认受托方在进行重大变更时，至少提前 20 个工作日通过书面方式通知可能受到影响的委托方。	是□ 否□ 不适用□	
1.4.7	受托方在进行重大变更时，是否提前至少 30 个工作日通过书面方式通知可能受到影响的委托方。（本项适用于：三+系统托管）	查看变更管理制度和变更通知，确认受托方在进行重大变更时，至少提前 30 个工作日通过书面方式通知可能受到影响的委托方。	是□ 否□ 不适用□	
1.4.8	受托方是否为委托方提供 7×24 小时支持服务，是否在 15 分钟内响应委托方提出的服务请求。遇到突发事件，是否积极配合委托方共同开展应急处置工作。（本项适用于：二级系统托管）	查看委托合同和应急记录，确认受托方为委托方提供 7×24 小时支持服务，在 15 分钟内响应委托方提出的服务请求。	是□ 否□ 不适用□	

表 N.2　信息系统托管审计底稿（续）

序号	审计项	审计程序	审计结论	备注
1.4.9	受托方是否为委托方提供7×24 小时支持服务，是否在 10 分钟内响应委托方提出的服务请求。遇到突发事件，是否积极配合委托方共同开展应急处置工作。（本项适用于：三级系统托管）	查看委托合同和应急记录，确认受托方为委托方提供 7×24 小时支持服务，在 10 分钟内响应委托方提出的服务请求。	是□ 否□ 不适用□	
1.4.10	受托方是否为委托方提供7×24 小时支持服务，是否在 5 分钟内响应委托方提出的服务请求。遇到突发事件，是否积极配合委托方共同开展应急处置工作。（本项适用于：三+系统托管）	查看委托合同和应急记录，确认受托方为委托方提供 7×24 小时支持服务，在 5 分钟内响应委托方提出的服务请求。	是□ 否□ 不适用□	
1.4.11	受托方是否至少每年一次向委托方提供服务报告，包括监控及巡检、日常维护、应急处理工作等。（本项适用于：二级系统托管）	检查服务报告，确认受托方至少每年一次向委托方提供服务报告，包括监控及巡检、日常维护、应急处理工作等。	是□ 否□ 不适用□	
1.4.12	受托方是否至少每半年一次向委托方提供服务报告，包括监控及巡检、日常维护、应急处理工作等。（本项适用于：三级、三+系统托管）	检查服务报告，确认受托方至少每半年一次向委托方提供服务报告，包括监控及巡检、日常维护、应急处理工作等。	是□ 否□ 不适用□	
1.4.13	受托方是否做好基础设施演练的年度计划，并按计划予以实施。（本项适用于：三级、三+系统托管）	检查基础设施演练的年度计划、演练报告，确认按计划实施了相关演练工作。	是□ 否□ 不适用□	
2	**机房租赁**			
2.1	**基础设施要求**			
2.1.1	机房是否满足 GB 50174 中 B 级机房要求。（本项适用于：二级系统托管）	检查机房满足 GB 50174 中 B 级机房的设计验收材料，确认机房满足 B 级机房要求。	是□ 否□ 不适用□	
2.1.2	机房是否满足 GB 50174 中 A 级机房要求。（本项适用于：三级、三+系统托管）	检查机房满足 GB 50174 中 A 级机房的设计验收材料，确认机房满足 A 级机房要求。	是□ 否□ 不适用□	

表 N.2　信息系统托管审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.1.3	机房是否有独立的双路电源配电柜，在证券期货交易时段，机房的电力可用性是否达到 99.9%。（本项适用于：二级系统托管）	检查“表 0.3-本年度交易时段双路失电的时间”，计算证券期货近一年交易时段双路未失电的时间占比，确定是否达到 99.9%；或检查近一年交易时段机房的电力可用性达到 99.9%的证明材料，确认电力可用性达到 99.9%。	是□ 否□ 不适用□	
2.1.4	机房是否有独立的双路电源配电柜，在证券期货交易时段，机房的电力可用性是否达到 99.99%。（本项适用于：三级、三+系统托管）	检查“表 0.3-本年度交易时段双路失电的时间”，计算证券期货近一年交易时段双路未失电的时间占比，确定是否达到 99.99%；或检查近一年交易时段机房的电力可用性达到 99.99%的证明材料，确认电力可用性达到 99.99%。	是□ 否□ 不适用□	
2.1.5	机房区域的温湿度是否达到 GB 50174 中 B 级的有关要求。（本项适用于：二级系统托管）	检查机房区域的温湿度的巡检记录，或达到 GB 50174 中 B 级的有关要求的证明材料，确认温湿度达到 GB 50174 中 B 级的有关要求。	是□ 否□ 不适用□	
2.1.6	机房精密空调至少采用 N+1 方式冗余，机房区域的温湿度是否达到 GB 50174 中 A 级的有关要求。（本项适用于：三级、三+系统托管）	a)检查机房精密空调部署图，确认是否至少采用 N+1 方式冗余； b)检查机房区域的温湿度的巡检记录，或达到 GB 50174 中 A 级的有关要求的证明材料，确认温湿度达到 GB 50174 中 A 级的有关要求。	是□ 否□ 不适用□	
2.1.7	机房是否具备集成的环境监控系统、设备监控系统，对环境、供电、空调、给水排水、消防等重要系统进行自动实时监控和报警。（本项适用于：三级、三+系统托管）	检查机房环境监控系统，确认是否能够对环境、供电、空调、给水排水、消防等重要系统进行自动实时监控和报警。	是□ 否□ 不适用□	
2.1.8	机房消防系统是否采用高效灭火系统和火灾自动报警系统，并通过当地消防部门验收。	检查机房消防系统通过当地消防部门验收证明，确认消防系统通过当地消防部门验收。	是□ 否□ 不适用□	
2.1.9	受托方是否做好对机房的基础设施日常巡检工作，每日巡检次数不少于三次。（本项适用于：二级系统托管）	检查机房基础设施的日常巡检相关制度和记录，确认每日巡检次数不少于三次。	是□ 否□ 不适用□	

表 N.2　信息系统托管审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.1.10	受托方是否做好对机房的基础设施日常巡检工作，每日巡检次数不少于六次。(本项适用于:三级、三+系统托管)	检查机房基础设施的日常巡检相关制度和记录，确认每日巡检次数不少于六次。	是□ 否□ 不适用□	
2.1.11	受托方是否配备 7×24 小时值班基础设施管理员，负责机房的日常维护、事件应急、故障处置等工作。	检查基础设施值班相关制度、排班表及管理员职责说明，确认配备了 7×24 小时值班基础设施管理员，负责机房基础设施的日常维护、事件应急、故障处置等工作。	是□ 否□ 不适用□	
2.2	**网络通信**			
2.2.1	受托方是否提供网络线路接入条件，满足委托方交易专网、互联网、数据专线等网络通信需求。	检查“表 0.6-卫星通信情况”、“表 0.6-地面通信情况”，确认受托方提供了多个运营商的网络线路接入条件。	是□ 否□ 不适用□	
2.2.2	受托方是否提供至少两家基础通信运营商的线路接入资源，且每家基础通信运营商至少采用两种不同的物理路由接入局端机房。(本项适用于：三级、三+系统托管)	检查“表 0.6-卫星通信情况”、“表 0.6-地面通信情况”，确认是否提供两家基础通信运营商的线路接入资源，且每家基础通信运营商至少采用两种不同的物理路由接入局端机房。	是□ 否□ 不适用□	
2.2.3	受托方是否 7×24 小时对机房公共网络运行情况进行实时监控，受托方未经委托方授权，禁止监听、获取、复制、利用通过网络传输的信息系统数据信息。	a）检查机房公共网络运行维护手册和监控记录，确认受托方 7×24 小时对机房公共网络运行情况进行实时监控； b）检查保密承诺书，确认未经委托方授权，禁止监听、获取、复制、利用通过网络传输的信息系统数据信息。	是□ 否□ 不适用□	
2.2.4	受托方是否配备 7×24 小时网络支持人员，负责其提供的机房公共网络的日常维护、事件应急、故障处置等工作。	检查网络值班制度、岗位职责说明、值班记录，确认受托方配备 7×24 小时网络支持人员，负责其提供的机柜公共网络的日常维护、事件应急、故障处置等工作。	是□ 否□ 不适用□	
2.3	**安全保卫**			
2.3.1	受托方是否为机房划定单独区域，并进行物理隔离且设有电子门锁。	检查机房平面图、机房出入口电子门锁照片，确认机房间进行物理隔离且设有电子门锁。	是□ 否□ 不适用□	
2.3.2	受托方是否对机房设置视频监控设备，监控范围覆盖机房区域出入口。连续视频监控记录是否保存至少90天。	a)检查机房运行维护手册，确认受托方对机房设置视频监控设备，监控范围覆盖机房出入口等关键区域； b)抽查视频监控记录，确认连续视频监控记录保存至少90天。	是□ 否□ 不适用□	

表 N.2　信息系统托管审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.3.3	机房所在建筑物是否设置周界区域，建筑物群体周界是否设置围墙，是否安装入侵报警系统、安全防护系统、防车辆撞击设施等。各安全防范子系统是否满足GB 50348规定的集成式安全防范系统设计要求以及各子系统的设计要求。（本项适用于：三级、三+系统托管）	查看机房建筑物平面图、建筑物群体周界照片、各安全防范子系统说明，确认机房所在建筑物满足GB 50348规定的集成式安全防范系统设计要求以及各子系统的设计要求。	是□ 否□ 不适用□	
2.3.4	受托方是否在机房所在建筑物入口处安装出入控制和安全防护装置，包括闸机、防爆桶、X射线安全检查设备等，并对出入人员和所带物品是否进行安全检查。（本项适用于：三级、三+系统托管）	a)检查机房运行维护手册，确认受托方在建筑物入口处安装出入控制和安全防护装置，包括闸机、防爆桶、X射线安全检查设备等，并对出入人员和所带物品应进行安全检查； b)现场检查建筑物入口处安装出入控制和安全防护装置，包括闸机、防爆桶、X射线安全检查设备等，确认对出入人员和所带物品进行安全检查。	是□ 否□ 不适用□	
2.3.5	受托方是否对机房所在区域出入人员身份执行审批审核流程，并记录出入人员信息、进出时间、工作内容等，相关记录是否保存至少360天。	检查人员出入审批审核流程和进出记录，确认包括人员信息、进出时间、工作内容等，相关记录应保存至少360天。	是□ 否□ 不适用□	
2.3.6	受托方是否配备7×24小时值班保安人员，负责机房的安全保卫工作。	检查日常值班表 日常值班制度，确认受托方配备7×24小时值班保安人员，负责机房的安全保卫工作。	是□ 否□ 不适用□	
2.4	**运维保障**			
2.4.1	受托方是否制定并完善对机房的运维管理相关制度，包括对机房基础设施、网络通信、安全保卫等运维操作流程、操作手册、故障处理、应急预案、应急联络人联络方式等，并提供给委托方。	检查委托方是否有受托方的运维管理制度,包括对机房基础设施、、网络通信、安全保卫等运维操作流程、操作手册、故障处理、应急预案、应急联络人联络方式。	是□ 否□ 不适用□	

表 N.2　信息系统托管审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.4.2	受托方是否为委托方提供信息系统运维和监控的场地条件，至少提供公共监控工位，满足委托方运维和监控需要。（本项适用于：二级系统托管）	查看场地租赁合同，访谈现场办公人员，确认受托方为委托方提供了信息系统运维和监控的场地条件，根据委托方要求，提供公共监控工位，满足委托方运维和监控需要。	是□ 否□ 不适用□	
2.4.3	受托方是否为委托方提供信息系统运维和监控的场地条件，至少提供专用的监控工位或专用监控室，满足委托方运维和监控需要。（本项适用于：三级、三+系统托管）	查看场地租赁合同，访谈现场办公人员，确认受托方为委托方提供了信息系统运维和监控的场地条件，根据委托方要求，提供专用监控工位或监控室，满足委托方运维和监控需要。	是□ 否□ 不适用□	
2.4.4	受托方是否向委托方告知值班基础设施管理员、网络管理员、保安人员的职责，并公布值班电话。	查看基础设施管理员、网管、保安职责和值班电话，确认受托方向委托方告知值班基础设施管理员、网络管理员、保安人员的职责、值班电话等信息。	是□ 否□ 不适用□	
2.4.5	受托方在进行重大变更时，是否提前至少10个工作日通过书面方式通知可能受到影响的委托方。（本项适用于：二级系统托管）	查看变更管理制度和变更通知，确认受托方在进行重大变更时，至少提前10个工作日通过书面方式通知可能受到影响的委托方。	是□ 否□ 不适用□	
2.4.6	受托方在进行重大变更时，是否提前至少20个工作日通过书面方式通知可能受到影响的委托方。（本项适用于：三级系统托管）	查看变更管理制度和变更通知，确认受托方在进行重大变更时，至少提前20个工作日通过书面方式通知可能受到影响的委托方。	是□ 否□ 不适用□	
2.4.7	受托方在进行重大变更时，是否提前至少30个工作日通过书面方式通知可能受到影响的委托方。（本项适用于：三+系统托管）	查看变更管理制度和变更通知，确认受托方在进行重大变更时，至少提前30个工作日通过书面方式通知可能受到影响的委托方。	是□ 否□ 不适用□	
2.4.8	受托方是否为委托方提供7×24小时支持服务，是否在15分钟内响应委托方提出的服务请求。遇到突发事件，是否积极配合委托方共同开展应急处置工作。（本项适用于：二级系统托管）	查看委托合同和应急记录，确认受托方为委托方提供7×24小时支持服务，在15分钟内响应委托方提出的服务请求。	是□ 否□ 不适用□	

表 N.2　信息系统托管审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.4.9	受托方是否为委托方提供7×24小时支持服务，是否在10分钟内响应委托方提出的服务请求。遇到突发事件，是否积极配合委托方共同开展应急处置工作。（本项适用于：三级系统托管）	查看委托合同和应急记录，确认受托方为委托方提供7×24小时支持服务，在10分钟内响应委托方提出的服务请求。	是□ 否□ 不适用□	
2.4.10	受托方是否为委托方提供7×24小时支持服务，是否在5分钟内响应委托方提出的服务请求。遇到突发事件，是否积极配合委托方共同开展应急处置工作。（本项适用于：三+系统托管）	查看委托合同和应急记录，确认受托方为委托方提供7×24小时支持服务，在5分钟内响应委托方提出的服务请求。	是□ 否□ 不适用□	
2.4.11	受托方是否至少每年一次向委托方提供服务报告，包括监控及巡检、日常维护、应急处理工作等。（本项适用于：二级系统托管）	检查服务报告，确认受托方至少每年一次向委托方提供服务报告，包括监控及巡检、日常维护、应急处理工作等。	是□ 否□ 不适用□	
2.4.12	受托方是否至少每半年一次向委托方提供服务报告，包括监控及巡检、日常维护、应急处理工作等。（本项适用于：三级、三+系统托管）	检查服务报告，确认受托方至少每半年一次向委托方提供服务报告，包括监控及巡检、日常维护、应急处理工作等。	是□ 否□ 不适用□	
2.4.13	受托方是否做好基础设施演练的年度计划，并按计划予以实施。（本项适用于：三级、三+系统托管）	检查基础设施演练的年度计划、演练报告，确认按计划实施了相关演练工作。	是□ 否□ 不适用□	
3.	**基础资源租赁**			
3.1	**基础设施要求**			
3.1.1	机房是否满足GB 50174中B级机房要求。（本项适用于：二级系统托管）	检查机房满足 GB 50174 中 B 级机房的设计验收材料，确认机柜所在机房满足 B 级机房要求。	是□ 否□ 不适用□	
3.1.2	机房是否满足GB 50174中A级机房要求。（本项适用于：三级、三+系统托管）	检查机房满足 GB 50174 中 A 级机房的设计验收材料，确认机柜所在机房满足 A 级机房要求。	是□ 否□ 不适用□	

表 N.2　信息系统托管审计底稿（续）

序号	审计项	审计程序	审计结论	备注
3.1.3	机房是否有独立的双路电源配电柜，在证券期货交易时段，机房的电力可用性是否达到99.9%。（本项适用于：二级系统托管）	检查“表 0.3-本年度交易时段双路失电的时间”，计算证券期货近一年交易时段双路未失电的时间占比，确定是否达到 99.9%；或检查近一年交易时段机房的电力可用性达到 99.9%的证明材料，确认电力可用性达到 99.9%。	是□ 否□ 不适用□	
3.1.4	机房是否有独立的双路电源配电柜，在证券期货交易时段，机房的电力可用性是否达到99.99%。（本项适用于：三级、三+系统托管）	检查“表 0.3-本年度交易时段双路失电的时间”，计算证券期货近一年交易时段双路未失电的时间占比，确定是否达到 99.99%；或检查近一年交易时段机房的电力可用性达到 99.99%的证明材料，确认电力可用性达到 99.99%。	是□ 否□ 不适用□	
3.1.5	机房区域的温湿度是否达到GB 50174中B级的有关要求。（本项适用于：二级系统托管）	检查机房区域的温湿度的巡检记录，或达到GB 50174 中 B 级的有关要求的证明材料，确认温湿度达到 GB 50174 中 B 级的有关要求。	是□ 否□ 不适用□	
3.1.6	机房精密空调至少采用N+1方式冗余，机房区域的温湿度是否达到GB 50174中A级的有关要求。（本项适用于：三级、三+系统托管）	a)检查机房精密空调部署图，确认是否至少采用 N+1 方式冗余； b)检查机房区域的温湿度的巡检记录，或达到 GB 50174 中 A 级的有关要求的证明材料，确认温湿度达到 GB 50174 中 A 级的有关要求。	是□ 否□ 不适用□	
3.1.7	机房是否具备集成的环境监控系统、设备监控系统，对环境、供电、空调、给水排水、消防等重要系统进行自动实时监控和报警。（本项适用于：三级、三+系统托管）	检查机房环境监控系统，确认是否能够对环境、供电、空调、给水排水、消防等重要系统进行自动实时监控和报警。	是□ 否□ 不适用□	
3.1.8	机房消防系统是否采用高效灭火系统和火灾自动报警系统，并通过当地消防部门验收。	检查机房消防系统通过当地消防部门验收证明，确认消防系统通过当地消防部门验收。	是□ 否□ 不适用□	
3.1.9	受托方是否做好对机房的基础设施日常巡检工作，每日巡检次数不少于三次。（本项适用于：二级系统托管）	检查机房基础设施的日常巡检相关制度和记录，确认每日巡检次数不少于三次。	是□ 否□ 不适用□	

表 N.2　信息系统托管审计底稿（续）

序号	审计项	审计程序	审计结论	备注
3.1.10	受托方是否做好对机房的基础设施日常巡检工作，每日巡检次数不少于六次。（本项适用于：三级、三+系统托管）	检查机房基础设施的日常巡检相关制度和记录，确认每日巡检次数不少于六次。	是□ 否□ 不适用□	
3.1.11	受托方是否配备7×24小时值班基础设施管理员，负责机房的日常维护、事件应急、故障处置等工作。	检查基础设施值班相关制度、排班表及管理员职责说明，确认配备了 7×24 小时值班基础设施管理员，负责机房基础设施的日常维护、事件应急、故障处置等工作。	是□ 否□ 不适用□	
3.2	**网络通信**			
3.2.1	受托方是否提供网络线路接入条件，满足委托方交易专网、互联网、数据专线等网络通信需求。	检查“表0.6-卫星通信情况”、“表0.6-地面通信情况”，确认受托方提供了多个运营商的网络线路接入条件。	是□ 否□ 不适用□	
3.2.2	受托方是否提供至少两家基础通信运营商的线路接入资源，且每家基础通信运营商至少采用两种不同的物理路由接入局端机房。（本项适用于：三级、三+系统托管）	检查“表0.6-卫星通信情况”、“表0.6-地面通信情况”，确认是否提供两家基础通信运营商的线路接入资源，且每家基础通信运营商至少采用两种不同的物理路由接入局端机房。	是□ 否□ 不适用□	
3.2.3	受托方是否7×24小时对机房公共网络运行情况进行实时监控，受托方未经委托方授权，禁止监听、获取、复制、利用通过网络传输的信息系统数据信息。	a）检查机房公共网络运行维护手册和监控记录，确认受托方7×24小时对机房公共网络运行情况进行实时监控； b）检查保密承诺书，确认未经委托方授权，禁止监听、获取、复制、利用通过网络传输的信息系统数据信息。	是□ 否□ 不适用□	
3.2.4	受托方是否配备7×24小时网络支持人员，负责其提供的机房公共网络的日常维护、事件应急、故障处置等工作。	检查网络值班制度、岗位职责说明、值班记录，确认受托方配备7×24小时网络支持人员，负责其提供的机柜公共网络的日常维护、事件应急、故障处置等工作。	是□ 否□ 不适用□	
3.2.5	受托方是否为委托方提供冗余通道，访问委托方租赁的基础资源。（本项适用于：三级、三+系统托管）	检查网络拓扑图，确认存在冗余通道。	是□ 否□ 不适用□	
3.3	**安全保卫**			
3.3.1	受托方是否为机房划定单独区域，并进行物理隔离且设有电子门锁。	检查机房平面图、机房出入口电子门锁照片，确认机房间进行物理隔离且设有电子门锁。	是□ 否□ 不适用□	

表 N.2　信息系统托管审计底稿（续）

序号	审计项	审计程序	审计结论	备注
3.3.2	受托方是否对机房设置视频监控设备，监控范围覆盖机房区域出入口。连续视频监控记录是否保存至少90天。	a)检查机房运行维护手册，确认受托方对机房设置视频监控设备，监控范围覆盖机房出入口等关键区域； b)抽查视频监控记录，确认连续视频监控记录保存至少90天。	是□ 否□ 不适用□	
3.3.3	机房所在建筑物是否设置周界区域，建筑物群体周界是否设置围墙，是否安装入侵报警系统、安全防护系统、防车辆撞击设施等。各安全防范子系统是否满足GB 50348规定的集成式安全防范系统设计要求以及各子系统的设计要求。（本项适用于：三级、三+系统托管）	查看机房建筑物平面图、建筑物群体周界照片、各安全防范子系统说明，确认机房所在建筑物满足GB 50348规定的集成式安全防范系统设计要求以及各子系统的设计要求。	是□ 否□ 不适用□	
3.3.4	受托方是否在机房所在建筑物入口处安装出入控制和安全防护装置，包括闸机、防爆桶、X射线安全检查设备等，并对出入人员和所带物品是否进行安全检查。（本项适用于：三级、三+系统托管）	a)检查机房运行维护手册，确认受托方在建筑物入口处安装出入控制和安全防护装置，包括闸机、防爆桶、X射线安全检查设备等，并对出入人员和所带物品应进行安全检查； b)现场检查建筑物入口处安装出入控制和安全防护装置，包括闸机、防爆桶、X射线安全检查设备等，确认对出入人员和所带物品进行安全检查。	是□ 否□ 不适用□	
3.3.5	受托方是否对机房所在区域出入人员身份执行审批审核流程，并记录出入人员信息、进出时间、工作内容等，相关记录是否保存至少360天。	检查人员出入审批审核流程和进出记录，确认包括人员信息、进出时间、工作内容等，相关记录应保存至少360天。	是□ 否□ 不适用□	
3.3.6	受托方是否配备7×24小时值班保安人员，负责机房的安全保卫工作。	检查日常值班表 日常值班制度，确认受托方配备7×24小时值班保安人员，负责机房的安全保卫工作。	是□ 否□ 不适用□	

表 N.2　信息系统托管审计底稿（续）

序号	审计项	审计程序	审计结论	备注
3.4	**基础资源租赁产品要求**			
3.4.1	**基础硬件产品**			
3.4.1.1	受托方提供的服务器设备、网络设备、安全设备、存储设备等基础硬件产品是否为冗余架构，性能和可用性是否满足委托方需求。	a)检查网络拓扑图、系统部署架构图，确定受托方提供的服务器设备、网络设备、安全设备、存储设备等基础硬件产品是否为冗余架构； b)检查服务器设备、网络设备、安全设备、存储设备性能说明材料及委托方与受托方签订的相关合同或协议等材料，确定受托方提供设备性能和可用性是否满足委托方需求。	是□ 否□ 不适用□	
3.4.1.2	受托方是否按照流程为提供的服务器设备、网络设备、安全设备、存储设备等基础硬件产品进行设备信息登记（供货日期，保修日期，序列号，厂家信息等）。	a)检查受托方是否有资产管理的相关制度，是否有相关流程规定对提供的服务器设备、网络设备、安全设备、存储设备等基础硬件产品进行设备信息登记（供货日期，保修日期，序列号，厂家信息等）； b)抽查受托方的设备资产登记表等材料，确定是否对提供的服务器设备、网络设备、安全设备、存储设备等基础硬件产品进行设备信息登记（供货日期，保修日期，序列号，厂家信息等）。	是□ 否□ 不适用□	
3.4.1.3	受托方是否提供独立的区域，部署服务器设备、网络设备、安全设备、存储设备等基础硬件产品。（本项适用于：三级、三+系统托管）	检查机房平面图，确定是否提供独立的区域，部署服务器设备、网络设备、安全设备、存储设备等基础硬件产品。	是□ 否□ 不适用□	
3.4.1.4	受托方是否为提供的服务器设备、网络设备、安全设备、存储设备等基础硬件产品提供备机、备件服务，或原厂维保服务。（本项适用于：三+系统托管）	检查委托方与受托方签订的相关合同或协议等材料，确定受托方是否承诺对为委托方提供服务器设备、网络设备、安全设备、存储设备等基础硬件产品提供备机、备件服务，或原厂维保服务。	是□ 否□ 不适用□	
3.4.2	**基础软件产品**			
3.4.2.1	受托方是否提供合法正版的系统软件等基础软件产品，并及时更新软件许可。	检查委托方与受托方签订的相关合同或协议等材料，确定受托方是否承诺提供合法正版的系统软件等基础软件产品，并及时更新软件许可。	是□ 否□ 不适用□	

表 N.2　信息系统托管审计底稿（续）

序号	审计项	审计程序	审计结论	备注
3.4.2.2	受托方是否负责对提供的系统软件等基础软件产品的安装、测试、升级和故障处理。	a)检查相关服务说明或合同等材料，是否明确规定受托方应负责对提供的系统软件等基础软件产品的安装、测试、升级和故障处理； b)检查软件安装、测试、升级及故障处理的记录，确定受托方是否按照规定执行。	是□ 否□ 不适用□	
3.4.2.3	受托方是否提供系统软件等基础软件产品的升级手册和升级包，且在提供升级补丁前，配合委托方进行可用性和风险评估。（本项适用于：三级、三+系统托管）	a)检查相关服务说明或合同等材料，是否明确规定受托方应提供系统软件等基础软件产品的升级手册和升级包，且在提供升级补丁前，配合委托方进行可用性和风险评估； b)如实施过可用性和风险评估，应有相关记录。	是□ 否□ 不适用□	
3.4.2.4	受托方是否提供针对系统软件等基础软件产品的培训。（本项适用于：三级、三+系统托管）	a)检查相关服务说明或合同等材料，是否规定受托方应提供针对系统软件等基础软件产品的培训； b)检查相关培训记录，确定是否按照规定开展培训。	是□ 否□ 不适用□	
3.4.3	**基础平台**			
3.4.3.1	受托方是否为虚拟机平台、存储平台等基础平台，提供安装、调试、培训、运行、升级等维护服务。	a)检查相关服务说明或合同等材料，确定是否明确规定受托方应为虚拟机平台、存储平台等基础平台，提供安装、调试、培训、运行、升级等维护服务； b)检查安装、调试、培训、运行、升级等维护服务相关记录，确定是否按照规定执行。	是□ 否□ 不适用□	
3.4.3.2	受托方提供的虚拟机平台、存储平台等基础平台的可用性是否不低于99.9%。（本项适用于：三级系统托管）	a)检查相关服务说明或合同等材料，确定是否明确规定受托方提供的虚拟机平台、存储平台等基础平台的可用性应不低于99.9%； b)计算虚拟机平台、存储平台近一年可用的时间占比，确定是否达到99.9%；或检查近一年可用性达到99.9%的证明材料，确认可用性达到99.9%。	是□ 否□ 不适用□	

表 N.2　信息系统托管审计底稿（续）

序号	审计项	审计程序	审计结论	备注
3.4.3.3	受托方提供的虚拟机平台、存储平台等基础平台的可用性是否不低于99.95%。（本项适用于：三+系统托管）	a)检查相关服务说明或合同等材料，确定是否明确规定受托方提供的虚拟机平台、存储平台等基础平台的可用性应不低于99.95%； b)计算虚拟机平台、存储平台近一年可用的时间占比，确定是否达到99.95%；或检查近一年可用性达到99.95%的证明材料，确认可用性达到99.95%。	是□ 否□ 不适用□	
3.4.3.4	受托方是否保证委托方数据在虚拟机平台、存储平台等基础平台上的安全、可靠传输，并保留数据传输日志记录，时间不得少于一年。	a)检查相关服务说明或合同等材料，确定是否明确规定受托方应保证委托方数据在虚拟机平台、存储平台等基础平台上的安全、可靠传输，并保留数据传输日志记录，时间不得少于一年； b)检查数据传输的相关日志记录，确定近一年内数据传输日志记录存在。	是□ 否□ 不适用□	
3.4.3.5	受托方是否做好虚拟机平台、存储平台等基础平台的数据备份工作。	a)检查受托方是否有数据备份相关制度； b)检查受托方是否按照制度要求对虚拟机平台、存储平台等基础平台进行数据备份，并存在数据备份记录。	是□ 否□ 不适用□	
3.4.3.6	受托方是否为虚拟机平台、存储平台等基础平台建立灾备系统，并制定应急方案。委托方是否配合受托方进行切换演练。（本项适用于：三级、三+系统托管）	a)检查系统设计方案、应急预案等材料，确定受托方是否为虚拟机平台、存储平台等基础平台建立灾备系统，并制定应急方案； b)检查相关服务说明或合同等材料，确定是否明确规定委托方应配合受托方进行切换演练； c)检查演练记录，确定按照规定执行。	是□ 否□ 不适用□	
3.4.3.7	受托方是否做好虚拟机平台、存储平台等基础平台的容量管理工作。（本项适用于：二级系统托管）	a)检查容量管理相关制度，确定受托方是否明确规定要对虚拟机平台、存储平台等基础平台开展容量管理工作； b)检查容量监控报告或评估报告等材料是否存在。	是□ 否□ 不适用□	
3.4.3.8	受托方是否做好虚拟机平台、存储平台等基础平台的容量管理工作，并定期提供容量监控报告。（本项适用于：三级系统托管）	a)检查容量管理相关制度，确定受托方是否明确规定要对虚拟机平台、存储平台等基础平台开展容量管理工作； b)检查是否定期形成容量监控报告（或评估报告），间隔周期应不超过一年。	是□ 否□ 不适用□	

表 N.2　信息系统托管审计底稿（续）

序号	审计项	审计程序	审计结论	备注
3.4.3.9	受托方是否做好虚拟机平台、存储平台等基础平台的容量管理工作，设定报警阈值，并定期提供容量监控报告。（本项适用于：三+系统托管）	a)检查容量管理相关制度，确定受托方是否明确规定要对虚拟机平台、存储平台等基础平台开展容量管理工作； b)检查是否按照制度规定对虚拟机平台、存储平台等基础平台设定报警阈值； c)检查是否定期形成容量监控报告（或评估报告），间隔周期应不超过一年。	是□ 否□ 不适用□	
3.4.3.10	受托方是否采取有效的安全隔离措施，防止基础平台内不同客户间的风险传导。（本项适用于：三级、三+系统托管）	检查受托方是否承诺采取有效的安全隔离措施，防止基础平台内不同客户间的风险传导；受托方应向委托方提供安全隔离措施的说明文件、测试报告等，证明其采取了有效隔离措施。	是□ 否□ 不适用□	
3.5	**运维保障**			
3.5.1	受托方是否制定并完善对基础资源的运维管理相关制度，包括对基础资源所在机房基础设施、网络通信、安全保卫、基础资源等运维操作流程、操作手册、故障处理、应急预案、应急联络人联络方式等，并提供给委托方。	检查受托方是否制定并完善对基础资源的运维管理相关制度，包括对基础资源所在机房基础设施、网络通信、安全保卫、基础资源等运维操作流程、操作手册、故障处理、应急预案、应急联络人联络方式等，并提供给委托方。	是□ 否□ 不适用□	
3.5.2	受托方是否为委托方提供信息系统运维和监控条件，满足委托方运维和监控需要。	检查相关服务说明或合同等材料，确定受托方是否为委托方提供信息系统运维和监控条件，满足委托方运维和监控需要。	是□ 否□ 不适用□	
3.5.3	受托方是否提供专业监控工具对基础资源租赁产品进行监控。（本项适用于：二级系统托管）	a)检查相关服务说明或合同等材料，确定受托方是否按照规定提供专业监控工具对基础资源租赁产品进行监控； b)检查监控工具的使用情况。	是□ 否□ 不适用□	
3.5.4	受托方是否提供专业监控工具对基础资源租赁产品进行监控，并定期提供监控报告。（本项适用于：三级、三+系统托管）	a)检查相关服务说明或合同等材料，确定受托方是否按照规定提供专业监控工具对基础资源租赁产品进行监控； b)检查监控工具的使用情况； c) 检查是否定期提供监控报告。	是□ 否□ 不适用□	
3.5.5	受托方是否定期对基础资源租赁产品进行巡检，并记录巡检结果。	a)检查运维制度内是否有定期巡检要求，是否明确内容、频度、人员等； b)抽查巡检记录，确认对基础资源租赁产品进行了巡检。	是□ 否□ 不适用□	

表 N.2　信息系统托管审计底稿（续）

序号	审计项	审计程序	审计结论	备注
3.5.6	受托方是否向委托方告知值班基础设施管理员、网络管理员、保安人员、平台运维人员的职责，并确定明确的排班表。	a)查阅受托方向委托方提供的值班基础设施管理员、网络管理员、保安人员、平台运维人员等岗位职责说明文件； b)查阅受托方提供的排班表。	是□ 否□ 不适用□	
3.5.7	受托方在进行可能涉及基础资源的变更时，是否提前至少 10 个工作日通过书面方式通知可能受到影响的委托方。（本项适用于：二级系统托管）	a)检查基础资源变更维护制度是否要求有提前 10 天告知的相应要求； b)对比做变更时提前告知委托方的通知和变更维护记录，判断是否做到变更前及时通知。	是□ 否□ 不适用□	
3.5.8	受托方在进行可能涉及基础资源的变更时，是否提前至少 20 个工作日通过书面方式通知可能受到影响的委托方。（本项适用于：三级系统托管）	a)检查基础资源变更维护制度是否要求有提前 20 天告知的相应要求； b)对比做变更时提前告知委托方的通知和变更维护记录，判断是否做到变更前及时通知。	是□ 否□ 不适用□	
3.5.9	受托方在进行可能涉及基础资源的变更时，是否提前至少 30 个工作日通过书面方式通知可能受到影响的委托方。（本项适用于：三+系统托管）	a)检查基础资源变更维护制度是否要求有提前 30 天告知的相应要求； b)对比做变更时提前告知委托方的通知和变更维护记录，判断是否做到变更前及时通知。	是□ 否□ 不适用□	
3.5.10	基础资源发生故障时，受托方是否按事件处理流程，积极配合委托方共同开展应急处置工作。	a)检查受托方是否提供应急管理制度或流程文件； b)检查应急管理文件中是否包含基础资源发生故障时，针对联合开展应急处置工作的相关要求。	是□ 否□ 不适用□	
3.5.11	受托方是否采取有效措施限制单个委托方对基础资源的使用限度。	a)检查基础资源控制策略，查看是否设置了单个委托方对基础资源的最大或最小使用限度； b)查看策略验证报告，确认策略是否有效。	是□ 否□ 不适用□	
3.5.12	受托方在进行双方合同中约定的关键操作时，是否按合同约定的程序执行审批手续，确保双人复核，并进行留痕，相关记录是否保存至少一年。	a)检查托管合同，是否明确关键操作规程，是否有“双人复核，并留痕，相关记录保存至少一年”的规定； b)检查关键操作记录，是否实行双人复核、达到至少保存一年的要求。	是□ 否□ 不适用□	

表 N.2　信息系统托管审计底稿（续）

序号	审计项	审计程序	审计结论	备注
3.5.13	受托方是否采取身份识别控制和权限管理，杜绝非授权和越权访问、更改委托方的数据。	a)检查用户权限清单和权限审批记录是否匹配； b)抽查身份识别和权限管理的操作记录，是否没有非授权和越权访问、更改委托方数据的记录。	是□ 否□ 不适用□	
3.5.14	受托方是否持续跟踪厂商提供的系统升级更新情况，检查基础资源系统的补丁是否得到了及时更新。	a)访谈系统管理员，了解系统补丁更新程序和评估方法； b)查看系统补丁更新记录，确认持续跟踪厂商提供的系统升级更新情况，确认在对重要文件进行备份后，才实施系统补丁程序的安装。	是□ 否□ 不适用□	
3.5.15	受托方是否部署防病毒产品和支持防恶意代码软件的统一管理，并定期检查防病毒产品和恶意代码库的版本更新情况。	a)检查是否有防病毒产品列表和防恶意代码软件的部署方案和管理制度； b)检查恶意代码库的升级记录，判断是否定期和及时。	是□ 否□ 不适用□	
3.5.16	受托方是否采取入侵防范措施，及时检测并阻断对平台系统的入侵行为。(本项适用于：二级系统托管)	a)检查入侵防范策略，查看是否对入侵采取防范措施； b)检查入侵防范设备的日志，是否及时检测并阻断对平台系统的入侵行为。	是□ 否□ 不适用□	
3.5.17	受托方是否采取入侵防范措施，及时检测并阻断对平台系统的入侵行为。是否能够检测到对重要服务器进行入侵的行为，能够记录入侵的源 IP、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警。(本项适用于：三级、三+系统托管)	a)检查入侵防范策略，查看是否要求记录对主要服务器攻击的源 IP、攻击类型、攻击目标、攻击时间等，在发生严重入侵事件时是否提供报警； b)检查入侵报警记录，查看记录中是否包括入侵的源 IP、攻击的类型、攻击的目的、攻击的时间等。	是□ 否□ 不适用□	
3.5.18	受托方是否为委托方提供 7×24 小时支持服务，是否在 15 分钟内响应委托方提出的服务请求。遇到突发事件，是否积极配合委托方共同开展应急处置工作。(本项适用于：二级系统托管)	a)查看委托合同和应急预案，是否明确要求 7×24 小时支持服务制度； b)检查应急事件报告书，查看受托方是否在 15 分钟内响应委托方的服务请求。	是□ 否□ 不适用□	

表 N.2　信息系统托管审计底稿（续）

序号	审计项	审计程序	审计结论	备注
3.5.19	受托方是否为委托方提供 7×24 小时支持服务，是否在 10 分钟内响应委托方提出的服务请求，并在 60 分钟内到场服务。遇到突发事件，是否积极配合委托方共同开展应急处置工作。（本项适用于：三级系统托管）	a)查看委托合同和应急预案，是否明确要求 7×24 小时支持服务制度； b)检查应急事件报告书，查看受托方是否在 15 分钟内响应委托方的服务请求，并在 60 分钟内到场服务。	是□ 否□ 不适用□	
3.5.20	受托方是否为委托方提供 7×24 小时支持服务，是否在 5 分钟内响应委托方提出的服务请求，并在 30 分钟内到场服务。遇到突发事件，是否积极配合委托方共同开展应急处置工作。（本项适用于：三+系统托管）	a)查看委托合同和应急预案，是否明确要求 7×24 小时支持服务制度； b)检查应急事件报告书，查看受托方是否在 5 分钟内响应委托方的服务请求，并在 30 分钟内到场服务。	是□ 否□ 不适用□	
3.5.21	受托方是否至少每年一次向委托方提供基础资源服务报告。（本项适用于：二级系统托管）	检查基础资源服务报告，是否至少每年一次。	是□ 否□ 不适用□	
3.5.22	受托方是否至少每半年一次向委托方提供基础资源服务报告，包括监控及巡检、日常维护、应急处理工作等。（本项适用于：三级、三+系统托管）	检查基础资源服务报告，是否至少每半年一次，检查报告是否包括监控及巡检、日常维护、应急处理工作等内容。	是□ 否□ 不适用□	
3.5.23	受托方是否做好数据保密工作，未经授权不得使用、分析、复制委托方数据，不得向第三方透露数据内容。	检查保密协议，确认是否要求受托方未经授权不得使用、分析、复制委托方数据，不得向第三方透露数据内容。	是□ 否□ 不适用□	
3.5.24	双方终止合同，受托方是否协助委托方收回所有数据，并保证系统中全部相关数据被删除，并不可恢复。	a)检查合同中是否明确提出合同终止时对数据的回收和删除相关要求； b)检查数据删除操作记录，确认删除操作记录中包含不可恢复的相关说明。	是□ 否□ 不适用□	

表 N.2　信息系统托管审计底稿（续）

序号	审计项	审计程序	审计结论	备注
4.	**整体外包**			
4.1	**基础设施要求**			
4.1.1	机房是否满足 GB 50174 中 B 级机房要求。（本项适用于：二级系统托管）	检查机房满足 GB 50174 中 B 级机房的设计验收材料，确认机柜所在机房满足 B 级机房要求。	是□ 否□ 不适用□	
4.1.2	机房是否满足 GB 50174 中 A 级机房要求。（本项适用于：三级、三+系统托管）	检查机房满足 GB 50174 中 A 级机房的设计验收材料，确认机柜所在机房满足 A 级机房要求。	是□ 否□ 不适用□	
4.1.3	机房是否有独立的双路电源配电柜，在证券期货交易时段，机房的电力可用性是否达到 99.9%。（本项适用于：二级系统托管）	检查“表 0.3-本年度交易时段双路失电的时间”，计算证券期货近一年交易时段双路未失电的时间占比，确定是否达到 99.9%；或检查近一年交易时段机房的电力可用性达到 99.9%的证明材料，确认电力可用性达到 99.9%。	是□ 否□ 不适用□	
4.1.4	机房是否有独立的双路电源配电柜，在证券期货交易时段，机房的电力可用性是否达到 99.99%。（本项适用于：三级、三+系统托管）	检查“表 0.3-本年度交易时段双路失电的时间”，计算证券期货近一年交易时段双路未失电的时间占比，确定是否达到 99.99%；或检查近一年交易时段机房的电力可用性达到 99.99%的证明材料，确认电力可用性达到 99.99%。	是□ 否□ 不适用□	
4.1.5	机房区域的温湿度是否达到 GB 50174 中 B 级的有关要求。（本项适用于：二级系统托管）	检查机房区域的温湿度的巡检记录，或达到 GB 50174 中 B 级的有关要求的证明材料，确认温湿度达到 GB 50174 中 B 级的有关要求。	是□ 否□ 不适用□	
4.1.6	机房精密空调至少采用 N+1 方式冗余，机房区域的温湿度是否达到 GB 50174 中 A 级的有关要求。（本项适用于：三级、三+系统托管）	a) 检查机房精密空调部署图，确认是否至少采用 N+1 方式冗余； b) 检查机房区域的温湿度的巡检记录，或达到 GB 50174 中 A 级的有关要求的证明材料，确认温湿度达到 GB 50174 中 A 级的有关要求。	是□ 否□ 不适用□	
4.1.7	机房是否具备集成的环境监控系统、设备监控系统，对环境、供电、空调、给水排水、消防等重要系统进行自动实时监控和报警。（本项适用于：三级、三+系统托管）	检查“表 0.3 机房基本情况”环境监控系统、设备监控系统，是否对环境、供电、空调、给水排水、消防等重要系统进行自动实时监控和报警。	是□ 否□ 不适用□	
4.1.8	机房消防系统是否采用高效灭火系统和火灾自动报警系统，并通过当地消防部门验收。	检查“表 0.3 机房基本情况”机房消防系统通过当地消防部门验收证明，确认消防系统通过当地消防部门验收。	是□ 否□ 不适用□	

表 N.2　信息系统托管审计底稿（续）

序号	审计项	审计程序	审计结论	备注
4.1.9	受托方是否做好对机房的基础设施日常巡检工作，每日巡检次数不少于三次。（本项适用于：二级系统托管）	检查机房基础设施的日常巡检相关制度和记录，确认每日巡检次数不少于三次。	是□ 否□ 不适用□	
4.1.10	受托方是否做好对机房的基础设施日常巡检工作，每日巡检次数不少于六次。（本项适用于：三级、三+系统托管）	检查机房基础设施的日常巡检相关制度和记录，确认每日巡检次数不少于六次。	是□ 否□ 不适用□	
4.1.11	受托方是否配备 7×24 小时值班基础设施管理员，负责机房的日常维护、事件应急、故障处置等工作。	检查基础设施值班相关制度、排班表及管理员职责说明，确认配备了 7×24 小时值班基础设施管理员，负责机房基础设施的日常维护、事件应急、故障处置等工作。	是□ 否□ 不适用□	
4.2	**网络通信要求**			
4.2.1	受托方是否提供网络线路接入条件，满足委托方交易专网、互联网、数据专线等网络通信需求。	检查“表 0.6-卫星通信情况”、“表 0.6-地面通信情况”，确认受托方提供了多个运营商的网络线路接入条件。	是□ 否□ 不适用□	
4.2.2	受托方是否提供至少两家基础通信运营商的线路接入资源，且每家基础通信运营商至少采用两种不同的物理路由接入局端机房。（本项适用于：三级、三+系统托管）	检查“表 0.6-卫星通信情况”、“表 0.6-地面通信情况”，确认是否提供两家基础通信运营商的线路接入资源，且每家基础通信运营商至少采用两种不同的物理路由接入局端机房。	是□ 否□ 不适用□	
4.2.3	受托方是否 7×24 小时对机房公共网络运行情况进行实时监控，受托方未经委托方授权，禁止监听、获取、复制、利用通过网络传输的信息系统数据信息。	a）检查机房公共网络运行维护手册和监控记录，确认受托方 7×24 小时对机房公共网络运行情况进行实时监控； b）检查保密承诺书，确认未经委托方授权，禁止监听、获取、复制、利用通过网络传输的信息系统数据信息。	是□ 否□ 不适用□	
4.2.4	受托方是否配备 7×24 小时网络支持人员，负责其提供的机房公共网络的日常维护、事件应急、故障处置等工作。	检查网络值班制度、岗位职责说明、值班记录，确认受托方配备 7×24 小时网络支持人员，负责其提供的机柜公共网络的日常维护、事件应急、故障处置等工作。	是□ 否□ 不适用□	
4.2.5	受托方是否为委托方提供冗余通道，访问委托方租赁的基础资源。（本项适用于：三级、三+系统托管）	检查网络拓扑图，确认存在冗余通道。	是□ 否□ 不适用□	

表 N.2　信息系统托管审计底稿（续）

序号	审计项	审计程序	审计结论	备注
4.3	**安全保卫要求**			
4.3.1	受托方是否为机房划定单独区域，并进行物理隔离且设有电子门锁。	检查机房平面图、机房出入口电子门锁照片，确认机房间进行物理隔离且设有电子门锁。	是□ 否□ 不适用□	
4.3.2	受托方是否对机房设置视频监控设备，监控范围覆盖机房区域出入口。连续视频监控记录是否保存至少 90 天。	a)检查机房运行维护手册，确认受托方对机房设置视频监控设备，监控范围覆盖机房出入口等关键区域； b)抽查视频监控记录，确认连续视频监控记录保存至少 90 天。	是□ 否□ 不适用□	
4.3.3	机房所在建筑物是否设置周界区域，建筑物群体周界是否设置围墙，是否安装入侵报警系统、安全防护系统、防车辆撞击设施等。各安全防范子系统是否满足 GB 50348 规定的集成式安全防范系统设计要求以及各子系统的设计要求。（本项适用于：三级、三+系统托管）	查看机房建筑物平面图、建筑物群体周界照片、各安全防范子系统说明，确认机房所在建筑物满足 GB 50348 规定的集成式安全防范系统设计要求以及各子系统的设计要求。	是□ 否□ 不适用□	
4.3.4	受托方是否在机房所在建筑物入口处安装出入控制和安全防护装置，包括闸机、防爆桶、X 射线安全检查设备等，并对出入人员和所带物品是否进行安全检查。(本项适用于:三级、三+系统托管)	a)检查机房运行维护手册，确认受托方在建筑物入口处安装出入控制和安全防护装置，包括闸机、防爆桶、X 射线安全检查设备等，并对出入人员和所带物品应进行安全检查； b)现场检查建筑物入口处安装出入控制和安全防护装置，包括闸机、防爆桶、X 射线安全检查设备等，确认对出入人员和所带物品进行安全检查。	是□ 否□ 不适用□	
4.3.5	受托方是否对机房所在区域出入人员身份执行审批审核流程，并记录出入人员信息、进出时间、工作内容等，相关记录是否保存至少 360 天。	检查人员出入审批审核流程和进出记录，确认包括人员信息、进出时间、工作内容等，相关记录应保存至少 360 天。	是□ 否□ 不适用□	
4.3.6	受托方是否配备 7×24 小时值班保安人员，负责机房的安全保卫工作。	检查日常值班表 日常值班制度，确认受托方配备 7×24 小时值班保安人员，负责机柜所在机房的安全保卫工作。	是□ 否□ 不适用□	

表 N.2　信息系统托管审计底稿（续）

序号	审计项	审计程序	审计结论	备注
4.4	**基础资源租赁产品要求**			
4.4.1	**基础硬件产品**			
4.4.1.1	受托方提供的服务器设备、网络设备、安全设备、存储设备等基础硬件产品是否为冗余架构，性能和可用性是否满足委托方需求。	a)检查网络拓扑图、系统部署架构图，确定受托方提供的服务器设备、网络设备、安全设备、存储设备等基础硬件产品是否为冗余架构； b)检查服务器设备、网络设备、安全设备、存储设备性能说明材料及委托方与受托方签订的相关合同或协议等材料，确定受托方提供设备性能和可用性是否满足委托方需求。	是□ 否□ 不适用□	
4.4.1.2	受托方是否按照流程为提供的服务器设备、网络设备、安全设备、存储设备等基础硬件产品进行设备信息登记（供货日期，保修日期，序列号，厂家信息等）。	a)检查受托方是否有资产管理的相关制度，是否有相关流程规定对提供的服务器设备、网络设备、安全设备、存储设备等基础硬件产品进行设备信息登记（供货日期，保修日期，序列号，厂家信息等）； b)抽查受托方的设备资产登记表等材料，确定是否对提供的服务器设备、网络设备、安全设备、存储设备等基础硬件产品进行设备信息登记（供货日期，保修日期，序列号，厂家信息等）。	是□ 否□ 不适用□	
4.4.1.3	受托方是否提供独立的区域，部署服务器设备、网络设备、安全设备、存储设备等基础硬件产品。(本项适用于：三级、三+系统托管)	检查机房平面图，确定是否提供独立的区域，部署服务器设备、网络设备、安全设备、存储设备等基础硬件产品。	是□ 否□ 不适用□	
4.4.1.4	受托方是否为提供的服务器设备、网络设备、安全设备、存储设备等基础硬件产品提供备机、备件服务，或原厂维保服务。(本项适用于：三+系统托管)	检查委托方与受托方签订的相关合同或协议等材料，确定受托方是否承诺对为委托方提供服务器设备、网络设备、安全设备、存储设备等基础硬件产品提供备机、备件服务，或原厂维保服务。	是□ 否□ 不适用□	
4.4.2	**基础软件产品**			
4.4.2.1	受托方是否提供合法正版的系统软件等基础软件产品，并及时更新软件许可。	检查委托方与受托方签订的相关合同或协议等材料，确定受托方是否承诺提供合法正版的系统软件等基础软件产品，并及时更新软件许可。	是□ 否□ 不适用□	

表 N.2　信息系统托管审计底稿（续）

序号	审计项	审计程序	审计结论	备注
4.4.2.2	受托方是否负责对提供的系统软件等基础软件产品的安装、测试、升级和故障处理。	a)检查相关服务说明或合同等材料，是否明确规定受托方应负责对提供的系统软件等基础软件产品的安装、测试、升级和故障处理； b)检查软件安装、测试、升级及故障处理的记录，确定受托方是否按照规定制定。	是□ 否□ 不适用□	
4.4.2.3	受托方是否提供系统软件等基础软件产品的升级手册和升级包，且在提供升级补丁前，配合委托方进行可用性和风险评估。（本项适用于：三级、三+系统托管）	a)检查相关服务说明或合同等材料，是否明确规定受托方应提供系统软件等基础软件产品的升级手册和升级包，且在提供升级补丁前，配合委托方进行可用性和风险评估； b)如实施过可用性和风险评估，应有相关记录。	是□ 否□ 不适用□	
4.4.2.4	受托方是否提供针对系统软件等基础软件产品的培训。（本项适用于：三级、三+系统托管）	a)检查相关服务说明或合同等材料，是否规定受托方应提供针对系统软件等基础软件产品的培训； b)检查相关培训记录，确定是否按照规定开展培训。	是□ 否□ 不适用□	
4.4.3	**基础平台**			
4.4.3.1	受托方是否为虚拟机平台、存储平台等基础平台，提供安装、调试、培训、运行、升级等维护服务。	a)检查相关服务说明或合同等材料，确定是否明确规定受托方应为虚拟机平台、存储平台等基础平台，提供安装、调试、培训、运行、升级等维护服务； b)检查安装、调试、培训、运行、升级等维护服务相关记录，确定是否按照规定执行。	是□ 否□ 不适用□	
4.4.3.2	受托方提供的虚拟机平台、存储平台等基础平台的可用性是否不低于 99.9%。（本项适用于：三级系统托管）	a)检查相关服务说明或合同等材料，确定是否明确规定受托方提供的虚拟机平台、存储平台等基础平台的可用性应不低于99.9%； b)计算虚拟机平台、存储平台近一年可用的时间占比，确定是否达到 99.9%；或检查近一年可用性达到 99.9%的证明材料，确认可用性达到 99.9%。	是□ 否□ 不适用□	

表 N.2 信息系统托管审计底稿（续）

序号	审计项	审计程序	审计结论	备注
4.4.3.3	受托方提供的虚拟机平台、存储平台等基础平台的可用性是否不低于 99.95%。（本项适用于：三+系统托管）	a)检查相关服务说明或合同等材料，确定是否明确规定受托方提供的虚拟机平台、存储平台等基础平台的可用性应不低于99.95%； b)计算虚拟机平台、存储平台近一年可用的时间占比，确定是否达到 99.95%；或检查近一年可用性达到 99.95%的证明材料，确认可用性达到99.95%。	是□ 否□ 不适用□	
4.4.3.4	受托方是否保证委托方数据在虚拟机平台、存储平台等基础平台上的安全、可靠传输，并保留数据传输日志记录，时间不得少于一年。	a)检查相关服务说明或合同等材料，确定是否明确规定受托方应保证委托方数据在虚拟机平台、存储平台等基础平台上的安全、可靠传输，并保留数据传输日志记录，时间不得少于一年； b)检查数据传输的相关日志记录，确定近一年内数据传输日志记录存在。	是□ 否□ 不适用□	
4.4.3.5	受托方是否做好虚拟机平台、存储平台等基础平台的数据备份工作。	a)检查受托方是否有数据备份相关制度； b)检查受托方是否按照制度要求对虚拟机平台、存储平台等基础平台进行数据备份，并存在数据备份记录。	是□ 否□ 不适用□	
4.4.3.6	受托方是否做好虚拟机平台、存储平台等基础平台的容量管理工作。（本项适用于：二级系统托管）	a)检查容量管理相关制度，确定受托方是否明确规定要对虚拟机平台、存储平台等基础平台开展容量管理工作； b)检查容量监控报告或评估报告等材料是否存在。	是□ 否□ 不适用□	
4.4.3.7	受托方是否做好虚拟机平台、存储平台等基础平台的容量管理工作，并定期提供容量监控报告。（本项适用于：三级系统托管）	a)检查容量管理相关制度，确定受托方是否明确规定要对虚拟机平台、存储平台等基础平台开展容量管理工作； b)检查是否定期形成容量监控报告（或评估报告），间隔周期应不超过一年。	是□ 否□ 不适用□	
4.4.3.8	受托方是否做好虚拟机平台、存储平台等基础平台的容量管理工作，设定报警阈值，并定期提供容量监控报告。（本项适用于：三+系统托管）	a)检查容量管理相关制度，确定受托方是否明确规定要对虚拟机平台、存储平台等基础平台开展容量管理工作； b)检查是否按照制度规定对虚拟机平台、存储平台等基础平台设定报警阈值； c)检查是否定期形成容量监控报告（或评估报告），间隔周期应不超过一年。	是□ 否□ 不适用□	

表 N.2　信息系统托管审计底稿（续）

序号	审计项	审计程序	审计结论	备注
4.4.3.9	受托方是否为虚拟机平台、存储平台等基础平台建立灾备系统，并制定应急方案。委托方是否配合受托方进行切换演练。（本项适用于：三级、三+系统托管）	a）检查系统设计方案、应急预案等材料，确定受托方是否为虚拟机平台、存储平台等基础平台建立灾备系统，并制定应急方案； b）检查相关服务说明或合同等材料，确定是否明确规定委托方应配合受托方进行切换演练； c）检查演练记录，确定按照规定执行。	是□ 否□ 不适用□	
4.4.3.10	受托方是否采取有效的安全隔离措施，防止基础平台内不同客户间的风险传导。（本项适用于：三级、三+系统托管）	检查受托方是否承诺采取有效的安全隔离措施，防止基础平台内不同客户间的风险传导；受托方应向委托方提供安全隔离措施的说明文件、测试报告等，证明其采取了有效隔离措施。	是□ 否□ 不适用□	
4.5	**应用系统要求**			
4.5.1	受托方是否向委托方提供应用系统的交付文档，包括但不限于系统架构、功能说明和用户手册等。	检查受托方向委托方提供的应用系统交付文档，是否包括系统架构、功能说明和用户手册等。	是□ 否□ 不适用□	
4.5.2	受托方提供的应用系统是否稳定可靠，确保业务的正常运行。	检查日常运行报告和故障报告，判断应用系统是否稳定可靠运行，未影响正常业务运行。	是□ 否□ 不适用□	
4.5.3	受托方提供的应用系统的性能和容量是否满足委托方的要求。	检查应用系统性能和容量情况是否满足委托方要求，是否未影响正常业务运行。	是□ 否□ 不适用□	
4.5.4	受托方提供的应用系统是否具备身份识别和权限控制功能。	检查应用系统功能说明书，并登录应用系统查看，判断应用系统是否具备身份识别和权限控制功能。	是□ 否□ 不适用□	
4.5.5	受托方提供的应用系统在数据传输、备份、存储等过程中，是否具备加密功能。	检查应用系统功能说明书，查看应用系统是否在数据传输、备份、存储等过程中具备加密功能。	是□ 否□ 不适用□	
4.5.6	受托方提供的应用系统是否具备日志记录功能，满足委托方的安全审计要求。	检查应用系统功能说明书，并登录应用系统查看系统日志，判断应用系统是否具备日志记录功能，满足委托方的安全审计要求。	是□ 否□ 不适用□	
4.5.7	受托方提供的应用系统是否满足委托方对于信息系统隔离的要求。（本项适用于：三级、三+系统托管）	检查应用系统清单，并登录要求隔离的信息系统，判断对于有信息系统隔离要求的信息系统，是否进行了隔离。	是□ 否□ 不适用□	

表 N.2 信息系统托管审计底稿（续）

序号	审计项	审计程序	审计结论	备注
4.5.8	受托方提供的应用系统的设计和部署是否满足 JR/T 0059 的要求。（本项适用于：三级、三+系统托管）	检查应用系统的备份能力设计和部署情况，是否满足 JR/T 0059 的要求。	是□ 否□ 不适用□	
4.5.9	受托方提供的应用系统是否为委托方提供监控工具或者接口，满足委托方的监控需要。	检查受托方提供的监控工具或者接口，是否满足委托方监控应用系统的需要。	是□ 否□ 不适用□	
4.6	**运维保障要求**			
4.6.1	受托方是否制定并完善对基础资源的运维管理相关制度，包括对基础资源所在机房基础设施、网络通信、安全保卫、基础资源等运维操作流程、操作手册、故障处理、应急预案、应急联络人联络方式等，并提供给委托方。	检查受托方是否制定并完善对基础资源的运维管理相关制度，包括对基础资源所在机房基础设施、网络通信、安全保卫、基础资源等运维操作流程、操作手册、故障处理、应急预案、应急联络人联络方式等，并提供给委托方。	是□ 否□ 不适用□	
4.6.2	受托方是否为委托方提供信息系统运维和监控条件，满足委托方运维和监控需要。	检查相关服务说明或合同等材料，确定受托方是否为委托方提供信息系统运维和监控条件，满足委托方运维和监控需要。	是□ 否□ 不适用□	
4.6.3	受托方是否提供专业监控工具对基础资源租赁产品进行监控。（本项适用于：二级系统托管）	a)检查相关服务说明或合同等材料，确定受托方是否按照规定提供专业监控工具对基础资源租赁产品进行监控； b)检查监控工具的使用情况。	是□ 否□ 不适用□	
4.6.4	受托方是否提供专业监控工具对基础资源租赁产品进行监控，并定期提供监控报告。（本项适用于：三级、三+系统托管）	a)检查相关服务说明或合同等材料，确定受托方是否按照规定提供专业监控工具对基础资源租赁产品进行监控； b)检查监控工具的使用情况； c) 检查是否定期提供监控报告。	是□ 否□ 不适用□	
4.6.5	受托方是否定期对基础资源租赁产品进行巡检，并记录巡检结果。	a)检查运维制度内是否有定期巡检要求，是否明确内容、频度、人员等； b)抽查巡检记录，确认对基础资源租赁产品进行了巡检。	是□ 否□ 不适用□	
4.6.6	受托方是否向委托方告知值班基础设施管理员、网络管理员、保安人员、平台运维人员的职责，并确定明确的排班表。	a)查阅受托方向委托方提供的值班基础设施管理员、网络管理员、保安人员、平台运维人员等岗位职责说明文件； b)查阅受托方提供的排班表。	是□ 否□ 不适用□	

表 N.2　信息系统托管审计底稿（续）

序号	审计项	审计程序	审计结论	备注
4.6.7	受托方在进行可能涉及基础资源的变更时，是否提前至少 10 个工作日通过书面方式通知可能受到影响的委托方。（本项适用于：二级系统托管）	a)检查基础资源变更维护制度是否要求有提前 10 天告知的相应要求； b)对比做变更时提前告知委托方的通知和变更维护记录，判断是否做到变更前及时通知。	是□ 否□ 不适用□	
4.6.8	受托方在进行可能涉及基础资源的变更时，是否提前至少 20 个工作日通过书面方式通知可能受到影响的委托方。（本项适用于：三级系统托管）	a)检查基础资源变更维护制度是否要求有提前 20 天告知的相应要求； b)对比做变更时提前告知委托方的通知和变更维护记录，判断是否做到变更前及时通知。	是□ 否□ 不适用□	
4.6.9	受托方在进行可能涉及基础资源的变更时，是否提前至少 30 个工作日通过书面方式通知可能受到影响的委托方。（本项适用于：三+系统托管）	a)检查基础资源变更维护制度是否要求有提前 30 天告知的相应要求； b)对比做变更时提前告知委托方的通知和变更维护记录，判断是否做到变更前及时通知。	是□ 否□ 不适用□	
4.6.10	基础资源发生故障时，受托方是否按事件处理流程，积极配合委托方共同开展应急处置工作。	a)检查受托方是否提供应急管理制度或流程文件； b)检查应急管理文件中是否包含基础资源发生故障时，针对联合开展应急处置工作的相关要求。	是□ 否□ 不适用□	
4.6.11	受托方是否采取有效措施限制单个委托方对基础资源的使用限度。	a)检查基础资源控制策略，查看是否设置了单个委托方对基础资源的最大或最小使用限度； b)查看策略验证报告，确认策略是否有效。	是□ 否□ 不适用□	
4.6.12	受托方在进行双方合同中约定的关键操作时，是否按合同约定的程序执行审批手续，确保双人复核，并进行留痕，相关记录是否保存至少一年。	a)检查托管合同，是否明确关键操作规程，是否有“双人复核，并留痕，相关记录保存至少一年”的规定； b)检查关键操作记录，是否实行双人复核、达到至少保存一年的要求。	是□ 否□ 不适用□	
4.6.13	受托方是否采取身份识别控制和权限管理，杜绝非授权和越权访问、更改委托方的数据。	a)检查用户权限清单和权限审批记录是否匹配； b)抽查身份识别和权限管理的操作记录，是否没有非授权和越权访问、更改委托方数据的记录。	是□ 否□ 不适用□	

表 N.2　信息系统托管审计底稿（续）

序号	审计项	审计程序	审计结论	备注
4.6.14	受托方是否持续跟踪厂商提供的系统升级更新情况，检查基础资源系统的补丁是否得到了及时更新。	a)访谈系统管理员，了解系统补丁更新程序和评估方法； b)查看系统补丁更新记录，确认持续跟踪厂商提供的系统升级更新情况，确认在对重要文件进行备份后，才实施系统补丁程序的安装。	是□ 否□ 不适用□	
4.6.15	受托方是否部署防病毒产品和支持防恶意代码软件的统一管理，并定期检查恶意代码库的版本更新情况。	a)检查是否有防病毒产品列表和防恶意代码软件的部署方案和管理制度； b)检查恶意代码库的升级记录，判断是否定期和及时。	是□ 否□ 不适用□	
4.6.16	受托方是否采取入侵防范措施，及时检测并阻断对平台系统的入侵行为。(本项适用于：二系统托管)	a)检查入侵防范策略，查看是否对入侵采取防范措施； b)检查入侵防范设备的日志，是否及时检测并阻断对平台系统的入侵行为。	是□ 否□ 不适用□	
4.6.17	受托方是否采取入侵防范措施，及时检测并阻断对平台系统的入侵行为。是否能够检测到对重要服务器进行入侵的行为，能够记录入侵的源 IP、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警。(本项适用于：三级、三+系统托管)	a)检查入侵防范策略，查看是否要求记录对主要服务器攻击的源 IP、攻击类型、攻击目标、攻击时间等，在发生严重入侵事件时是否提供报警； b)检查入侵报警记录，查看记录中是否包括入侵的源 IP、攻击的类型、攻击的目的、攻击的时间等。	是□ 否□ 不适用□	
4.6.18	受托方是否为委托方提供 7×24 小时支持服务，是否在 15 分钟内响应委托方提出的服务请求。遇到突发事件，是否积极配合委托方共同开展应急处置工作。(本项适用于：二级系统托管)	a)查看委托合同和应急预案，是否明确要求 7×24 小时支持服务制度； b)检查应急事件报告书，查看受托方是否在 15 分钟内响应委托方的服务请求。	是□ 否□ 不适用□	
4.6.19	受托方是否为委托方提供 7×24 小时支持服务，是否在 10 分钟内响应委托方提出的服务请求，并在 60 分钟内到场服务。遇到突发事件，是否积极配合委托方共同开展应急处置工作。(本项适用于：三级系统托管)	a)查看委托合同和应急预案，是否明确要求 7×24 小时支持服务制度； b)检查应急事件报告书，查看受托方是否在 15 分钟内响应委托方的服务请求，并在 60 分钟内到场服务。	是□ 否□ 不适用□	

表 N.2　信息系统托管审计底稿（续）

序号	审计项	审计程序	审计结论	备注
4.6.20	受托方是否为委托方提供 7×24 小时支持服务，是否在 5 分钟内响应委托方提出的服务请求，并在 30 分钟内到场服务。遇到突发事件，是否积极配合委托方共同开展应急处置工作。（本项适用于：三+系统托管）	a)查看委托合同和应急预案，是否明确要求 7×24 小时支持服务制度； b)检查应急事件报告书，查看受托方是否在 5 分钟内响应委托方的服务请求，并在 30 分钟内到场服务。	是□ 否□ 不适用□	
4.6.21	受托方是否至少每年一次向委托方提供基础资源服务报告。（本项适用于：二级系统托管）	检查基础资源服务报告，是否至少每年一次。	是□ 否□ 不适用□	
4.6.22	受托方是否至少每半年一次向委托方提供基础资源服务报告，包括监控及巡检、日常维护、应急处理工作等。（本项适用于：三级、三+系统托管）	检查基础资源服务报告，是否至少每半年一次，检查报告是否包括监控及巡检、日常维护、应急处理工作等内容。	是□ 否□ 不适用□	
4.6.23	受托方是否做好数据保密工作，未经授权不得使用、分析、复制委托方数据，不得向第三方透露数据内容。	检查保密协议，确认是否要求受托方未经授权不得使用、分析、复制委托方数据，不得向第三方透露数据内容。	是□ 否□ 不适用□	
4.6.24	双方终止合同，受托方是否协助委托方收回所有数据，并保证系统中全部相关数据被删除，并不可恢复。	a)检查合同中是否明确提出合同终止时对数据的回收和删除相关要求； b)检查数据删除操作记录，确认删除操作记录中包含不可恢复的相关说明。	是□ 否□ 不适用□	
4.6.25	受托方对受托应用系统的运维工作，是否当按照 JR/T 0099 的各项要求开展。	检查受托方运维管理制度、或相关运维评估说明文件，确认其满足 JR/T 0099 的各项要求标准。	是□ 否□ 不适用□	
4.6.26	受托方是否配合委托方进行应用系统必要的业务测试。	a)检查受托方测试管理制度或流程。确认其针对配合委托方应用系统必要的业务测试有明确要求； b)抽出测试记录，确保其按照要求执行。	是□ 否□ 不适用□	
4.6.27	受托方在进行可能影响应用系统的变更时，是否提前至少 10 个工作日通过书面方式通知可能受到影响的委托方。（本项适用于：二级系统托管）	查看受托方提供的变更管理制度和变更通知，确认受托方在进行可能影响应用系统的变更时，至少提前 10 个工作日通过书面方式通知可能受到影响的委托方。	是□ 否□ 不适用□	

表 N.2　信息系统托管审计底稿（续）

序号	审计项	审计程序	审计结论	备注
4.6.28	受托方在进行可能影响应用系统的变更时，是否提前至少 20 个工作日通过书面方式通知可能受到影响的委托方。(本项适用于：三级系统托管)	查看受托方提供的变更管理制度和变更通知，确认受托方在进行可能影响应用系统的变更时，至少提前 20 个工作日通过书面方式通知可能受到影响的委托方。	是□ 否□ 不适用□	
4.6.29	受托方在进行可能影响应用系统的变更时，是否提前至少 30 个工作日通过书面方式通知可能受到影响的委托方。(本项适用于：三+系统托管)	查看受托方提供的变更管理制度和变更通知，确认受托方在进行可能影响应用系统的变更时，至少提前 30 个工作日通过书面方式通知可能受到影响的委托方。	是□ 否□ 不适用□	
4.6.30	受托方是否至少每年对应用系统进行检查，并形成相关检查记录和评估报告。(本项适用于：二级系统托管)	查看受托方提供的应用系统检查记录和评估报告，确认其满足至少每年一次的要求。	是□ 否□ 不适用□	
4.6.31	受托方是否至少每半年对应用系统进行检查，包括应用系统可用性、参数配置、系统性能容量、权限设置、系统版本等，并形成相关检查记录和评估报告。(本项适用于：三级系统托管)	查看受托方提供的应用系统检查记录和评估报告，确认其满足至少每半年一次的要求，并涵盖应用系统可用性、参数配置、系统性能容量、权限设置、系统版本等方面内容。	是□ 否□ 不适用□	
4.6.32	受托方是否至少每季度对应用系统进行检查，包括应用系统可用性、参数配置、系统性能容量、权限设置、系统版本等，并形成相关检查记录和评估报告。(本项适用于：三+系统托管)	查看受托方提供的应用系统检查记录和评估报告，确认其满足至少每半年一次的要求，并涵盖应用系统可用性、参数配置、系统性能容量、权限设置、系统版本等方面内容。	是□ 否□ 不适用□	
4.6.33	受托方是否至少每年一次向委托方提供应用系统服务报告。(本项适用于：二级系统托管)	查看受托方向委托方提供的应用系统服务报告，确认其满足至少每年一次的要求。	是□ 否□ 不适用□	
4.6.34	受托方是否至少每半年一次向委托方提供应用系统服务报告，包括监控及巡检、日常维护、应急处理工作等。(本项适用于：三级系统托管)	查看受托方向委托方提供的应用系统服务报告，确认其满足至少每半年一次的要求，并涵盖监控及巡检、日常维护、应急处理工作等方面内容。	是□ 否□ 不适用□	

表 N.2　信息系统托管审计底稿（续）

序号	审计项	审计程序	审计结论	备注
4.6.35	受托方是否至少每季度一次向委托方提供应用系统服务报告，包括监控及巡检、日常维护、应急处理工作等。（本项适用于：三+系统托管）	查看受托方向委托方提供的应用系统服务报告，确认其满足至少每季度一次的要求，并涵盖监控及巡检、日常维护、应急处理工作等方面内容。	是□ 否□ 不适用□	
4.6.36	受托方在进行双方合同中约定的应用系统关键数据操作时，是否按合同规定的程序执行审批手续，确保双人复核，并进行留痕，相关记录是否保存至少两年。(本项适用于：三+系统托管）	a)检查托管合同，是否明确应用系统关键数据操作规程，是否有“双人复核，并留痕，相关记录保存至少两年”的规定； b)检查关键数据操作记录，确认其实行双人复核、达到至少保存两年的要求。	是□ 否□ 不适用□	
4.6.37	受托方是否提供应用系统的应急预案，当故障发生时，能恢复原来的工作状态。组织用户至少每年进行一次故障应急演练。（本项适用于：三级、三+系统托管）	a)检查受托方提供的应用系统应急预案、部署说明，确认其故障发生时，能够恢复原来的工作状态； b)抽查故障应急演练记录，确认其满足至少每年进行一次的要求。	是□ 否□ 不适用□	

附 录 0
（规范性附录）
信息系统调查表

表0.1至表0.16约定了信息系统调查的内容和要求

表0.1 IT治理-人员与岗位情况

人员基本情况					
正式员工总数（人）		IT员工总数（人）			
分管信息技术的公司领导					
姓名	工作电话	手机	电子邮箱	职务	分管部门
信息技术相关部门负责人（含副职）					
姓名	工作电话	手机	电子邮箱	职务	所在部门
信息系统审计相关部门的负责人（含副职）					
姓名	工作电话	手机	电子邮箱	职务	所在部门
IT治理委员会或类似机构组成人员					
姓名	工作电话	手机	电子邮箱	职务	所在部门
按岗位人员情况					

岗位设置	**主岗人员数**	**备岗人员数**
总部机房管理员人员数（人）		
总部网络管理员人员数（人）		
总部系统管理员人员数（人）		
总部数据库管理员人员数（人）		
总部安全管理员人员数（人）		
其中总部安全管理专岗人员数（人）		

表0.2　IT治理-经营与IT投入情况

经营情况							
		N-2年度		N-1年度		N年度（本年度）	
营业收入（万元）							
净利润（万元）							
信息技术投入情况							
		N-2年度		N-1年度		N年度（本年度）	
		预算	核算	预算	核算	预算	核算
机房物理环境建设费用（万元）							
信息系统硬件费用（万元）							
软件投入（万元）	软件采购费用						
	应用系统开发费用						
系统运维费用（万元）	机房物理环境维护费用（万元）						
	信息系统硬件维护费用（万元）						
	信息系统软件维护费用（万元）						
	技术服务费用（万元）						
	应急保障费用（万元）						
	其它运维费用（万元）						
网络与通信设施的使用费（万元）							
网络与通信设施的维护费（万元）							
信息技术培训费用（万元）							
其它费用（万元）							
合计（万元）							

表0.3　机房基本情况

基本情况			
机房名称		所在城市	
机房详细地址		机房类别	自建机房 □　　托管机房□
消防情况			
是否通过当地消防部门的验收	是□　否□	是否已向当地消防部门备案	是□否□
消防类型（可多选）	自动喷水灭火□　自动气体灭火□　手动气体灭火□ 自动泡沫灭火□　手动泡沫灭火□　干粉灭火□		
电力情况			
供电方式（可多选）	三变电站三路供电 □　双变电站双路供电□　单变电站双路供电 □ 单路供电□　UPS 设备□　备用发电机□		
供电站名称（供电来源）		大楼物业是否提供发电车连接装置	是□否□
总电力容量（KVA）		当前电力容量（KVA）	
本年度交易时段双路失电的时间			

UPS（不同品牌和功率应增加表格分别填写）						
该机房 UPS 总功率(KVA)		平均满载运行时间（小时）		平均负载率（%）		
UPS 品牌	单台功率（KVA）	数量（台）	联机方式	满载运行时间（小时）	当前负载率（%）	已使用年限（年）
			并机□　串机□ 未联接□			

发电机（不同品牌和功率应增加表格分别填写）					
发电机品牌	功率（KVA）	储油量维持供电时间（小时）	配备方式	启用所需时间(分钟)	已使用年限（年）
			购买□租赁发电车□租赁物业发电机□		
			购买□租赁发电车□租赁物业发电机□		

空调（不同品牌和制冷量应增加表格分别填写）					
品牌	单台制冷量（KW）	数量（台）	空调能否由发电机供电	是否精密空调	已使用年限（年）
			是□ 否□	是□ 否□	

表 0.3　机房基本情况(续)

机房监控情况						
软件名称及版本	软件厂商	监控对象	监控内容	监控方式	日志保存时间（天）	报警手段
		机　房环境	电力状态□　空调□ 新风机□　温湿度□ 配电柜□　UPS□ UPS 电池（整组）□ UPS 电池（单个）□ 漏水检测□　机房进出□ 消防设施□	交易时间人工监控□ 交易时间软件监控□ 非交易时间人工监控□ 非交易时间软件监控□		声光报警□ 自动拨号语音报警□ 短信报警□ 电子邮件报警□ 其他□
		安全设备	运行状况□ cpu 使用率□ 内存利用率□ 端口状态□ 数据流量□ 并发连接数□ 并发处理量□ 安全事件记录□	同上		同上
		网络通信	运行状况□ cpu 使用率□ 通信连接状态□ 网络流量□ 核心节点网络延时□ 丢包率□	同上		同上

网络边界防护情况（可根据该机房划分安全域增加）		
重要安全域隔离情况	隔离方式	隔离手段
交易业务网与可上互联网的内部办公网	物理隔离□ 逻辑隔离□ 未隔离□ 无此项□	防火墙□ 网闸□　数据网关□ 路由器□ 交换机□ 协议隔离□　Vlan□ 其它□
核心交易业务网与非核心交易业务网	同上	同上
核心交易业务网与分支机构交易业务网	同上	同上
网上信息系统与互联网	同上	同上
门户网站与网上交易系统	同上	同上
网上交易下单网页与网上交易后台数据库	同上	同上
交易业务网与开发测试网络	同上	同上
交易业务网与模拟环境测试网络	同上	同上

表 0.3　机房基本情况(续)

该机房的病毒木马防护软件情况（表格不够可增加）				
软件名称	软件厂商	软件类型（网络版/单机版）	部署目标	病毒木马库更新周期（天）
			服务器□ 网络设备□ 终端设备□ 其他□	

该机房的网络安全检查情况（如有请填写，表格不够请增加）			
安全检查方式	检查频率	检查软件名称	安全服务商
漏洞扫描			
渗透测试			
病毒扫描			
木马检测			

该机房的攻击防护措施（如有请填写，表格不够请增加）				
	品牌	型号	厂商	数量（台）
防 DDOS 专用设备				
入侵防护设备				
入侵检测设备				
负载均衡设备				
防火墙				
其它防护措施（请填写）				

表0.4　集中交易系统情况

基本情况				
主用系统所在机房名称				
系统处理能力				
压力测试系统支持最大客户数（万户）		系统实际有效客户数（万户）		
压力测试峰值每秒最大委托处理笔数（笔）		本年度峰值交易日峰值每秒处理笔数（笔）		
		历史峰值交易日峰值每秒处理笔数（笔）		
扩展系统处理能力所需时间（自然日）		本年度交易中断、严重缓慢总时长（分钟）		
备份系统情况				
系统备份方式	热备□　温备□　冷备□	是否建立灾备系统	同城灾备□　异地灾备□	
同城备份系统所在机房名称（如有）				
与主机房直线距离（km）				
异地备份系统所在机房名称（如有）				
与主机房直线距离（km）				
备份系统处理能力				
	备份系统	同城备份系统	异地备份系统	
相对于主用信息系统的处理能力（%）				
系统备份能力				
	故障应对能力	灾难应对能力	重大灾难应对能力	
信息系统恢复时间目标 RTO	分钟	小时	天	
信息系统恢复点目标 RPO	秒	分钟	小时	

表 0.4 集中交易系统情况(续)

集中交易软件情况			
源代码所有权	有□ 无□	源代码审查	是 □ 否 □
源代码保存机制	外包开发商保存□ 自主保存□ 第三方托管□		

审计软件情况					
软件名称		软件版本		软件开发商	
开发方式	完全自主开发 □ 引进后自主开发 □ 联合开发□ 外包开发 □ 直接购买 □ 上级下发□				

客户信息及交易数据备份情况（不同备份内容请逐一填写）										
备份内容	备份方式	备份周期	备份介质	是否压缩	备份数据量（GB）	是否本地存放	同城存放地与主中心直线距离（km）	异地存放地与主中心直线距离（km）	有效性验证方式	验证周期
				是□ 否□		是□ 否□				

系统监控情况（不同监控软件请逐一填写）							
软件名称及版本	软件厂商	监控对象	监控内容	监控方式	日志保存时间（天）	监控范围	报警手段
		交易软件	进程状态□ 日志信息□ cpu 使用率□ 内存利用率□ 并发线程数□ 并发处理量□ 关键业务指标□	交易时间人工监控□ 交易时间软件监控□ 非交易时间人工监控□ 非交易时间软件监控□		主用系统□ 备份系统□ 同城备份系统□ 异地备份系统□	声光报警□ 自动拨号语音报警□ 短信报警□ 电子邮件报警□ 其他□
		数据库	日志信息□ 表空间使用率□ 连接数□ 日志记录□	同上		同上	
		服务器	运行状况□ cpu 使用率□ 内存利用率□ 磁盘空间□ 通信端口□ 日志记录□	同上		同上	
		存储	运行状况□ 数据交换延时□ 存储电池□ 日志记录□	同上		同上	

表 0.4 集中交易系统情况(续)

<table>
<tr><td colspan="10">卫星通信情况</td></tr>
<tr><td colspan="10">基本情况</td></tr>
<tr><td></td><td colspan="2">上海单向宽带广播卫星小站数（个）</td><td colspan="2">上海宽带双向小站数（个）</td><td colspan="2">深圳多媒体高速单向小站数（个）</td><td colspan="2">深圳双向卫星小站数（个）</td></tr>
<tr><td>总部</td><td colspan="2"></td><td colspan="2"></td><td colspan="2"></td><td colspan="2"></td></tr>
<tr><td colspan="10">地面通信情况</td></tr>
<tr><td colspan="10">外联通信情况</td></tr>
<tr><td colspan="10">1.与上交所和上证通地面专线连接情况通信情况（如有请填写，空不够可增加）</td></tr>
<tr><td>序号</td><td>通信本端</td><td>通信本端机房类型</td><td>通信对端</td><td>主备方式</td><td>运营商</td><td>连接类型</td><td>线路类型</td><td>带宽</td><td>流量负载率（%）</td><td>线路用途</td></tr>
<tr><td>1</td><td></td><td>主机房□
同城备份机房□
异地备份机房□
其它□</td><td></td><td>主□
备□</td><td></td><td>DDN□
SDH□
MSTP□
ATM□
局域网□
裸光纤□
互联网 VPN□
3G□
电话拨号□
其它□</td><td>局域网□
本市□
本省□
跨省□
跨境□</td><td></td><td></td><td>交易□
行情□
结算□
融资融券□
开户□
会员服务□
资讯信息□
证监会及证监局数据报送□
保证金监控数据报送□
资本市场监测数据□
人民银行反洗钱数据报送□
上市公司数据报送□
数据备份□
银证数据交换□
中国债券登记公司数据□
信托保险业务数据交换□
场外市场数据传输□
外汇交易中心数据□
境外市场接入□
交易仿真测试□
联合测试□
视频会议□
应急指挥□
办公□
身份认证□
其他□</td></tr>
</table>

表 0.4 集中交易系统情况(续)

2.与深交所和深证通的地面专线连接情况（如有请填写，空不够可增加）										
序号	通信本端	通信本端机房类型	通信对端	主备方式	运营商	连接类型	线路类型	带宽	流量负载率（%）	线路用途
1		同上		同上		同上	同上			同上
3. 中证登公司、中证登（上海）公司和中证登（深圳）公司的地面专线连接情况（如有请填写，空不够可增加）										
序号	通信本端	通信本端机房类型	通信对端	主备方式	运营商	连接类型	线路类型	带宽	流量负载率（%）	线路用途
1		同上		同上		同上	同上			同上
内部通信情况										
a)总部主备机房之间地面专线连接情况（如有请填写，空不够可增加）										
序号	通信本端	通信本端机房类型	通信对端	主备方式	运营商	连接类型	线路类型	带宽	流量负载率（%）	线路用途
1		同上		同上		同上	同上			同上

表0.5　第三方存管系统情况

基本情况			
主用系统所在机房名称			
系统处理能力			
压力测试系统支持最大客户数（万）		开通第三方存管业务的客户数（万）	
转账类交易压力测试处理性能（笔/秒，每百万客户）		本年度转账类交易平均处理笔数（笔/秒，每百万客户）	
查询类交易压力测试处理性能（笔/秒，每百万客户）		本年度查询类交易平均处理笔数（笔/秒，每百万客户）	
压力测试日处理最大银证转账笔数(万笔)		本年度最大日处理银证转账笔数（万笔）	
压力测试日处理最大银证查询笔数（万笔）		本年度最大日处理银证查询笔数（万笔）	
本年度交易中断、严重缓慢总时长（分钟）			
备份系统情况			
系统备份方式	热备□　温备□　冷备□	是否建立灾备系统	同城灾备□　异地灾备□
同城备份系统所在机房名称（如有）			
与主机房直线距离（km）			
异地备份系统所在机房名称（如有）			
与主机房直线距离（km）			

备份系统处理能力			
	备份系统	同城备份系统	异地备份系统
相对于主用信息系统的处理能力（%）			

本单位切换备份系统，银证业务情况（如有，请按照银行逐一填写）							
序号	存管银行名称	切换至备份系统		切换至同城系统		切换至异地系统	
		银证业务是否正常	信息系统恢复时间目标RTO(分)	银证业务是否正常	信息系统恢复时间目标RTO(小时)	银证业务是否正常	信息系统恢复时间目标RTO(天)
1		是□否□		是□否□		是□否□	

表 0.5　第三方存管系统情况(续)

转账日志备份情况									
备份方式	备份周期	备份介质	是否压缩	备份数据量（GB）	是否本地存放	同城存放地与主中心直线距离（km）	异地存放地与主中心直线距离（km）	有效性验证方式	验证周期
			是□ 否□		是□ 否□				

审计软件情况					
软件名称		软件版本		软件开发商	
开发方式	完全自主开发 □ 引进后自主开发 □ 联合开发□ 外包开发 □ 直接购买 □ 上级下发□				

系统监控情况（不同监控软件请逐一填写）							
软件名称及版本	软件厂商	监控对象	监控内容	监控方式	日志保存时间（天）	监控范围	报警手段
		第三方存管业务处理情况	进程状态□ 日志信息□ cpu 使用率□ 内存利用率□ 并发线程数□ 并发处理量□ 关键业务指标□	交易时间人工监控□ 交易时间软件监控□ 非交易时间人工监控□ 非交易时间软件监控□		主用系统□ 备份系统□ 同城备份系统□ 异地备份系统□	声光报警□ 自动拨号语音报警□ 短信报警□ 电子邮件报警□ 其他□
		服务器	运行状况□ cpu 使用率□ 内存利用率□ 磁盘空间□ 通信端口□ 日志记录□	同上		同上	

表0.6　网上信息系统情况

网上信息系统基本情况			
承载网上信息系统机房数（个）		网上委托站点数量（个）	
网上行情站点数量（个）		手机证券站点数量（个）	
下单网页站点数量（个）		门户网站站点数量（个）	
自建电子商务站点数量（个）		依托的第三方电子商务平台数量（个）	

网上信息系统站点分布信息情况（请逐一列出，表格不够可增加）							
序号	所在机房名称	网上委托站点数量	网上行情站点数量	下单网页站点数量	手机证券站点数量	门户网站站点数量	自建电子商务站点数量
1							
2							
3							

网上信息系统客户端软件使用情况						
a)网上交易行情客户端软件（计算机）						
序号	软件名称	功能（多选）	版本	交易功能软件开发商	行情功能软件开发商	存储客户交易终端信息（多选）
1		交易□ 行情□				IP 地址□ MAC 地址□ 其它
2		同上				同上

b)网页交易下单				
序号	软件名称	版本	软件开发商	存储客户交易终端信息
1				IP 地址□ MAC 地址□ 电话号码□ 其它
2				同上

表 0.6　网上信息系统情况(续)

c)移动证券									
序号	软件名称	版本	软件开发商	适用的操作系统名称	最低操作系统版本要求	客户端提供渠道（多选）	存储客户交易终端信息	软件具备的安全保护措施（多选）	运行平台
1				Android□ 苹果 iOS□ Windows phone□ Symbian□ 其他		官网下载□ Google play□ iTune store□ 微软 Marketplace□ 360□ 安卓网□ 其它	IP 地址□ IMEI□ WIFI MAC 地址□ 电话号码□ 其它	安装与卸载时检测程序被篡改□ 限制登陆密码尝试次数□ 含弱口令检查机制□ 防止软件被动态调试□ 防止程序被代码注入□ 防止程序被反编译□ 防止密码、账号等敏感信息被截屏泄露□ 禁止在客户端本地存储密码等敏感信息□ 禁止在客户端本地日志记录密码等敏感信息□ 自带病毒木马扫描□ 生成委托订单令牌□ 其他	自建□ 云平台□

网上信息系统身份认证方式			
	专用客户端	网页下单	手机终端
账号+静态密码	□	□	□
随机验证码	□	□	□
通讯码	□	□	□
密码图形键盘（软键盘）	□	□	□
客户端电脑或手机特征码绑定	□	□	□
软件数字证书	□	□	□
手机短信口令	□	□	□
硬件数字证书（第 1 代）	□	□	□
硬件数字证书（第 2 代）	□	□	□
动态密码（口令）卡	□	□	□

表 0.6　网上信息系统情况(续)

身份认证方式	厂商	已发放数量（张、个）	占有效客户总数比例（%）	资产总额占全部客户资产比例（%）
硬件数字证书（第 1 代）				
硬件数字证书（第 2 代）				
动态密码(口令)卡				

软件数字证书建设情况（如有请填写）						
根证书管理方式	根证书提供厂商或第三方 CA 中心名称	证书系统建设情况	证书系统厂商名称	已发放数量(张、个)	占有效客户总数比例（%）	资产总额占全部客户资产比例（%）
本机构自主生成□ 采用中登公司的根证书□ 采用 CFCA 根证书□ 采用其他第三方 CA 中心根证书□		自建根证书系统□ 建设第三方 CA 中心或中登公司数字证书中心的分中心系统□ 无系统□				

表0.7为表0.6的附表，表0.7需以机房为单位分别填写。

表0.7　附表

该机房的网上信息系统详细情况			
所在机房名称		互联网线路总带宽（Mbps）	

该机房的网上信息系统互联网通信情况（请逐一列出，表格不够可增加）						
序号	运营商	带宽	独享/共享	流量负载率（%）	是否购买流量清洗服务	清洗流量带宽
1					是□　否□	
2					是□　否□	

该机房的网上委托站点基本情况（如有请填写）			
	压力测试值	历史峰值	本年度峰值
客户同时在线最大支持数（万人）			
峰值每秒处理笔数（笔）			
日处理最大委托笔数（万笔）			
扩展系统处理能力所需时间（自然日）			

该机房的网上委托站点详细情况（请逐一列出，表格不够可增加）										
序号	互联网IP地址	所属运营商	软件开发商	软件名称及版本	主机数量(台)	最大客户支持数（万人）	日处理最大委托笔数(万笔)	是否采用线路负载均衡	客户认证信息传输情况	客户网络地址记录情况
1								是□ 否□	明文传输□ 加密传输□	客户端源 IP 地址、MAC 地址□ 代理服务器 IP 地址、MAC 地址□
2								同上	同上	同上

表 0.7　附表（续）

该机房的网上行情站点基本情况（如有请填写）									
压力测试最大客户支持数（万人）				当前平均每日同时在线客户数（万人）					
历史峰值同时在线最大客户数（万人）				本年度峰值同时在线最大客户数（万人）					
扩展系统处理能力所需时间（自然日）									
行情来源（可多选）	总部□　营业部□　其它□								
该机房的网上行情站点详细情况（请逐一列出，表格不够可增加）									
序号	互联网IP地址	所属运营商	软件开发商	软件名称及版本	主机数量（台）	最大客户支持数（万人）	是否采用线路负载均衡		
1							是□ 否□		
该机房的手机证券站点基本情况（如有请填写）									
手机证券系统架构	Browser/Server□　Client/Server□　其他□								
手机证券 WAP 站点网址（如有）									
手机行情来源（可多选）	总部□　营业部□　其它□								
	压力测试值		历史峰值		本年度峰值				
客户同时在线最大支持数（万人）									
最大同时在线请求（笔/秒）									
扩展系统处理能力所需时间（自然日）									
该机房的手机证券站点详细情况（请逐一列出，表格不够可增加）									
序号	互联网IP地址	所属运营商	软件开发商	软件名称及版本	主机数量（台）	最大客户支持数(万人)	是否采用线路负载均衡	客户认证信息传输情况	客户网络地址记录情况
1							是□否□	明文传输□ 加密传输□	客户端源 IP 地址、MAC 地址□ 代理服务器 IP 地址、MAC 地址□

表 0.7　附表（续）

该机房的网页下单站点情况(如有请填写)			
下单网页网址			
下单网页 IP 地址			
服务器证书建设方式	自建□　第三方□	证书颁发机构名称	
网页下单系统软件名称		软件开发商	
	压力测试值	历史峰值	本年度峰值
客户同时在线最大支持数（万人）			
最大同时在线请求（笔/秒）			
扩展系统处理能力所需时间（自然日）			

依托第三方电子商务平台的情况(如有请填写)				
序号	依托的第三方电子商务平台名称	网页网址	服务器证书建设方式	第三方证书建设服务商名称
1	淘宝□ 腾讯□ 京东□ 其他		自建□ 第三方□	
2	同上		同上	

门户网站系统情况(如有请填写)			
网　址		IP 地址	
ICP 备案号		系统开发商	
域名服务商		域名解析服务器地址	
压力测试最大客户支持数（万人）		本年度系统日均访问量（万人次）	

门户网站防篡改措施（如有请填写）			
防篡改系统品牌		防篡改系统厂商	
防篡改措施(请简述)			

表 0.7　附表（续）

该机房的网上信息系统监控情况（不同监控软件请逐一填写）						
软件名称及版本	软件厂商	监控对象	监控内容	监控方式	日志保存时间	开发方式
		中间件软件	进程状态□ 日志信息□ cpu 使用率□ 内存利用率□ 并发线程数□ 并发处理量□ 关键业务指标□	交易时间人工监控□ 交易时间软件监控□ 非交易时间人工监控□ 非交易时间软件监控□		
		服务器	运行状况□ cpu 使用率□ 内存利用率□ 磁盘空间□ 通信端口□ 日志记录□	同上		
		存储	运行状况□ 数据交换延时□ 存储电池□ 日志记录□	同上		
		数据库	日志信息□ 表空间使用率□ 连接数□ 日志记录□	同上		
		门户网站	网页内容□ 日均访问量□	同上		

该机房的网上信息系统数据备份情况										
备份内容	备份方式	备份周期	备份介质	是否压缩	备份数据量（GB）	是否本地存放	同城存放地与主中心直线距离(km)	异地存放地与主中心直线距离(km)	有效性验证方式	验证周期
系统程序				是□ 否□		是□ 否□				
配置参数				是□ 否□		是□ 否□				
系统日志				是□ 否□		是□ 否□				
安全审计数据				是□ 否□		是□ 否□				
门户网站信息				是□ 否□		是□ 否□				

表0.8　重要信息系统情况

基本情况			
信息系统全称			
所在机房名称			
备份系统情况			
系统备份方式	热备□　　温备□　　冷备□	是否建立灾备系统	同城灾备□　异地灾备□
同城备份系统所在机房名称（如有）			
与主机房直线距离（km）			
异地备份系统所在机房名称（如有）			
与主机房直线距离（km）			

系统备份能力			
	故障应对能力	灾难应对能力	重大灾难应对能力
信息系统恢复时间目标 RTO	分钟	小时	天
信息系统恢复点目标 RPO	秒	分钟	小时

数据备份情况（不同备份内容请逐一填写）										
备份内容	备份方式	备份周期	备份介质	是否压缩	备份数据量（GB）	是否本地存放	同城存放地与主中心直线距离（km）	异地存放地与主中心直线距离（km）	有效性验证方式	验证周期
				是□ 否□		是□ 否□				

表 0.8　重要信息系统情况（续）

系统监控情况（不同监控软件请逐一填写）							
软件名称及版本	软件厂商	监控对象	监控内容	监控方式	日志保存时间（天）	监控范围	报警手段
		信息系统	进程状态□ 日志信息□ cpu 使用率□ 内存利用率□ 并发线程数□ 并发处理量□ 关键业务指标□	交易时间人工监控□ 交易时间软件监控□ 非交易时间人工监控□ 非交易时间软件监控□		主用系统□ 备份系统□ 同城备份系统□ 异地备份系统□	声光报警□ 自动拨号语音报警□ 短信报警□ 电子邮件报警□ 其他□
		数据库	日志信息□ 表空间使用率□ 连接数□ 日志记录□	同上		同上	
		服务器	运行状况□ cpu 使用率□ 内存利用率□ 磁盘空间□ 通信端口□ 日志记录□	同上		同上	
		存储	运行状况□ 数据交换延时□ 存储电池□ 日志记录□	同上		同上	

表0.9　信息安全等级保护工作情况

基本情况				
信息系统安全建设组织保障工作情况	是否明确主管领导、负责部门和具体负责人			是□　否□
	是否对信息系统安全建设整改工作进行总体部署			是□　否□
信息系统安全等级保护工作主管领导	姓名		职务	
	办公电话		电子邮件	
信息系统安全等级保护工作联系人	姓名		职务	
	办公电话		电子邮件	

信息系统备案情况				
序号	信息系统名称	定级级别	备案受理公安机关	备案证明编号
1		三级□ 二级□		
2		三级□ 二级□		

本年度开展安全建设整改的信息系统情况	
信息安全等级保护安全建设整改咨询机构名称（全称）	
信息安全等级保护等级测评机构名称（全称）	

序号	信息系统名称	定级级别	是否进行了信息安全保护现状分析	是否制定信息系统安全建设整改方案	是否开展信息系统安全建设整改工作	是否组织开展信息系统安全自查工作	是否进行了信息安全等级测评工作	是否达到了信息安全等级要求	该信息系统发生安全事件、事故数量
1		三级□ 二级□	是□ 否□	是□ 否□	是□ 否□	是□ 否□	是□ 否□	是□ 否□	
2		三级□ 二级□	是□ 否□	是□ 否□	是□ 否□	是□ 否□	是□ 否□	是□ 否□	

表0.10　应急管理情况

公司信息安全应急联络人					
姓名	职务	办公电话	手机号码	传真号码	电子邮件

本年度应急演练情况			
针对集中交易系统故障开展应急演练的次数（次）		对灾备系统切换进行应急演练的次数（次）	
针对第三方存管系统与银行开展联合演练的次数（次）		针对网络通信故障开展应急演练的次数（次）	
针对网上交易盗买盗卖开展应急演练的次数（次）		针对网页篡改开展应急演练的次数（次）	
针对病毒入侵、DDOS 攻击、渗透式攻击等开展应急演练的次数（次）		针对电力故障开展应急演练的次数（次）	
针对消防等开展的应急演练的次数（次）		对空调故障开展应急演练的次数（次）	

参加交易所等市场核心机构组织的应急演练情况		
序号	应急演练内容	应急演练时间
1		

公司自行组织的信息安全应急演练情况		
序号	应急演练内容	应急演练时间
1		

表0.11　软件正版化情况

基本情况				
组织机构	负责本单位软件正版化工作的部门		部门成立时间	
	分管领导		分管领导职务	
	负责本单位软件正版化工作的责任人		责任人职务	
自查情况	本年度开展软件正版化自查的次数			

软件正版化情况（截止到本年度年底）																
一、操作系统																
序号	操作系统类别	软件版本	软件类型	正版软件情况			安装操作系统的计算机情况			许可					本年度维护费用(万元)
				总套数(套)	新购套数(套)	新购金额(万元)	计算机类别	应安装该操作系统的计算机数量（台）	已安装该正版操作系统的计算机数量(台)	许可类型	许可数(个)	是否在授权期内	正版化率(%)	是否签署协议	
1	Windows□ DOS□ Linux□ Unix□ IBM Aix□ HP-Unix□ Solaris□ Novell□ Mac OS□ Android□ 其他□		国内□ 国外□				服务器□ 台式机□ 便携机□			预装许可□ 单机许可□ 场地许可□ 开源免费□ 单人许可□ 开放式许可□ 网络许可□ 租赁许可□ 自行开发□ 其他□		是□ 否□		是□ 否□	
2	同上		同上				同上			同上		同上		同上	

表 0.11　软件正版化情况（续）

二、杀毒软件															
序号	杀毒软件类别	软件版本	软件类型	正版软件情况			安装杀毒软件的计算机情况			许可					本年度维护费用(万元)
				总套数(套)	新购套数(套)	新购金额(万元)	计算机类别	应安装该杀毒软件的计算机数量（台）	已安装该正版杀毒软件的计算机数量(台)	许可类型	许可数(个)	是否在授权期内	正版化率(%)	是否签署协议	
1	瑞星□ 金山□ 江民□ 360□ 趋势□ 诺顿□ 赛门铁克□ 卡巴斯基□ MCAFEE□ 其他□		国内□ 国外□				服务器□ 台式机□ 便携机□			预装许可□ 单机许可□ 场地许可□ 开源免费□ 单人许可□ 开放式许可□ 网络许可□ 租赁许可□ 自行开发□ 其他□		是□ 否□		是□ 否□	
2	同上		同上				同上			同上		同上		同上	

表 0.11　软件正版化情况（续）

三、办公文字处理软件																
序号	办公软件类别	软件名称及版本	软件类型	正版软件情况			安装办公软件的计算机情况			许可					本年度维护费用(万元)
				总套数(套)	新购套数(套)	新购金额(万元)	计算机类别	应安装该办公软件的计算机数量（台）	已安装该正版办公软件的计算机数量(台)	许可类型	许可数（个）	是否在授权期内	正版化率(%)	是否签署协议	
1	微软 Office□ 金山 Office□ 永中 Office□ 其他□		国内□ 国外□				服务器□ 台式机□ 便携机□			预装许可□ 单机许可□ 场地许可□ 开源免费□ 单人许可□ 开放式许可□ 网络许可□ 租赁许可□ 自行开发□ 其他□		是□ 否□		是□ 否□	
2	同上		同上				同上			同上		同上		同上	

表 0.11　软件正版化情况（续）

四、办公专业处理软件															
序号	办公专业处理软件类别	软件名称及版本	软件类型	正版软件情况			安装办公软件的计算机情况			许可					本年度维护费用(万元)
				总套数(套)	新购套数(套)	新购金额(万元)	计算机类别	应安装该办公软件的计算机数量（台）	已安装该正版办公软件的计算机数量（台）	许可类型	许可数(个)	是否在授权期内	正版化率(%)	是否签署协议	
1	财务软件□ ERP□ CRM□ 其他□		国内□ 国外□				服务器□ 台式机□ 便携机□			预装许可□ 单机许可□ 场地许可□ 开源免费□ 单人许可□ 开放式许可□ 网络许可□ 租赁许可□ 自行开发□ 其他□		是□ 否□		是□ 否□	
2	同上		同上				同上			同上		同上		同上	

表 0.11　软件正版化情况（续）

五、应用服务器软件														
序号	应用服务器类别	软件名称及版本	正版软件情况			安装应用服务器的计算机情况			许可					本年度维护费用（万元）
			总套数（套）	新购套数（套）	新购金额（万元）	计算机类别	应安装该应用服务器的计算机数量（台）	已安装该正版应用服务器的计算机数量（台）	许可类型	许可数（个）	是否在授权期内	正版化率(%)	是否签署协议	
1	恒生□ 金证□ 金仕达□ 顶点□ 通达信□ 根网□ 铭创□ CTP□ 易盛□ 赢时胜□ Apache□ Tomcat□ weblogic□ 文华□ 澎博□ 其他□					服务器□ 台式机□ 便携机□			预装许可□ 单机许可□ 场地许可□ 开源免费□ 单人许可□ 开放式许可□ 网络许可□ 租赁许可□ 自行开发□ 其他□		是□ 否□		是□ 否□	
2	同上					同上			同上		同上		同上	

表 0.11　软件正版化情况（续）

六、数据库软件														
序号	数据库类别	软件版本	正版软件情况			安装数据库的计算机情况			许可					本年度维护费用（万元）
			总套数（套）	新购套数（套）	新购金额（万元）	计算机类别	应安装该数据库的计算机数量（台）	已安装该正版数据库的计算机数量（台）	许可类型	许可数（个）	是否在授权期内	正版化率(%)	是否签署协议	
1	ORACLE□ MS SQL□ Sybase□ DB2□ Domino□ 人大金仓□ 其他□					服务器□ 台式机□ 便携机□			预装许可□ 单机许可□ 场地许可□ 开源免费□ 单人许可□ 开放式许可□ 网络许可□ 租赁许可□ 自行开发□ 其他□		是□ 否□		是□ 否□	
2	同上					同上			同上		同上		同上	

表 0.11　软件正版化情况(续)

七、专用业务软件														
序号	专用业务软件类别	软件名称及版本	正版软件情况			安装专用业务软件的计算机情况			许可					本年度维护费用(万元)
			总套数(套)	新购套数(套)	新购金额(万元)	计算机类别	应安装该专用业务软件的计算机数量（台）	已安装该正版专用业务软件的计算机数量（台）	许可类型	许可数(个)	是否在授权期内	正版化率(%)	是否签署协议	
1						服务器□ 台式机□ 便携机□			预装许可□ 单机许可□ 场地许可□ 开源免费□ 单人许可□ 开放式许可□ 网络许可□ 租赁许可□ 自行开发□ 其他□		是□ 否□		是□ 否□	
2						同上			同上		同上		同上	

表0.12　重要信息系统商用密码使用情况

<table>
<tr><td colspan="8">基本情况</td></tr>
<tr><td colspan="2">信息系统中是否使用了密码设备</td><td colspan="3">是□　否□</td><td colspan="2">是否采用了含密码产品</td><td>是□　否□</td></tr>
<tr><td colspan="2">是否采用了 CA 认证技术</td><td colspan="3">是□　否□</td><td colspan="2">具有 CA 认证系统（发证）□　　具有 CA 认证系统（验证）□</td></tr>
<tr><td colspan="8">信息系统密码相关制度建立和落实情况</td></tr>
<tr><td>分管密码安全工作领导</td><td>姓名</td><td colspan="2"></td><td>职务</td><td colspan="3"></td></tr>
<tr><td rowspan="2">密码安全管理机构</td><td>负责人姓名</td><td colspan="2"></td><td>职务</td><td colspan="3"></td></tr>
<tr><td>联系人</td><td colspan="2"></td><td>电话</td><td colspan="3"></td></tr>
<tr><td>密码安全专职管理机构</td><td>负责人</td><td colspan="2"></td><td>电话</td><td colspan="3"></td></tr>
<tr><td rowspan="2">密码安全管理员</td><td>本单位内设机构数量（个）</td><td colspan="2"></td><td>密码安全员数量（个）</td><td colspan="3"></td></tr>
<tr><td>专职密码安全员数量（个）</td><td colspan="6"></td></tr>
<tr><td>岗位责任和事故责任追究</td><td>岗位密码安全责任制度</td><td>已制定□
未制定□</td><td>安全责任事故</td><td>未发生□
发生过□</td><td>事故查处</td><td colspan="2">所有事故均已查处相关责任人□
有事故未查处相关责任人□</td></tr>
</table>

表 0.12　重要信息系统商用密码使用情况（续）

密码安全管理制度建立和落实情况				
人员管理	重要岗位人员签署安全保密协议	全部签订□ 未签订□ 部分签订□	制定人员离岗安全规定	已制定□ 未制定□
	外部人员访问审批制度	已制定□ 未制定□	-	-
资产管理	密码设备安全管理制度	已制定□ 未制定□	指定专人进行密码设备管理	有专人□ 无专人□
	密码设备维修、维护和报废管理制度	已制定□ 未制定□	密码设备维修、维护和报废记录	完整□　不完整□
存储介质管理	制定存储介质管理制度	已制定□ 未制定□	存储介质管理记录	完整□　不完整□
	制定存储介质操作规范	已制定□ 未制定□	-	-
运行维护管理	制定密码日常运维制度	已制定□ 未制定□	制定密码运维操作手册	已制定□ 未制定□
	密码运维操作记录;	完整□　不完整□	制定密码应急管理预案	已制定□ 未制定□
年度培训考核	制定密码年度培训计划	已制定□ 未制定□	本年度接受密码操作培训的人数（人）	
	本年度接受密码操作考核的次数（次）		-	-

表 0.12　重要信息系统商用密码使用情况（续）

公司所有信息系统的密码设备数量统计													
		密码应用软件数量（台、套、个）		智能 IC 卡数量（台、套、个）		智能密码钥匙数量（台、套、个）		密码机数量（台、套、个）		其他密码产品数量（台、套、个）		含密产品数量（台、套、个）	
		三级	二级	三级	二级	三级	二级	三级	二级	三级	二级	三级	二级
已获得国密局批准型号	国内												
	国外												
未获得国密局批准型号	国内												
	国外												

表0.13为表0.12的附表，表0.13需按信息系统分别填写。

表0.13　附表一

信息系统名称		**信息系统安全等级**	三级□ 二级□
系统运行环境	Windows□ Linux□ Unix□ 其他	**运维方式**	自行运维□　外包□

密码使用基本情况							
密码设备数量（套）		含密产品数量（套）		取得国密局型号数量（套）		未取得国密局型号数量（套）	
实现的密码功能（多选）	电子门禁□ 安全访问路径□ 身份鉴别□ 访问控制□ 审计记录□ 程序安全□ 数据传输□ 数据存储□ 密钥管理□	是否物理隔离密码设备	是□ 否□	是否专人负责密码设备操作	是□ 否□	是否建立密码相关制度	是□ 否□

本系统中密码应用软件使用情况（如有请填写）

序号	密码应用软件名称	软件版本	数量	获国密局批准	生产厂家名称	厂商类型	使用时间	互联网接入	互联网接入IP地址/网址	算法使用情况	算法类型	实现的密码功能	密钥管理	密码协议	用途
1				是□ 否□		国内□ 国外□		是□ 否□		SM1□ SM2□ SM3□ SM4□ RSA1024□ RSA2048□ DES□ MD5□ SHA-1□ SHA-256□ 3DES□ AES□ 其他□	国内□ 国外□	电子门禁□ 安全访问路径□ 身份鉴别□ 访问控制□ 审计记录□ 程序安全□ 数据传输□ 数据存储□ 密钥管理□	是□ 否□	IPSec□ SSL□ 其他□	

表 0.13　附表一（续）

本系统中智能卡使用情况（如有请填写）												
序号	智能卡名称	型号	数量	获国密局批准	生产厂家名称	厂商类型	厂商资质	使用时间	接口类型	算法使用情况	算法类型	用途
1				是□ 否□		国内□ 国外□	商用密码产品销售许可证□ 计算机信息系统安全专用产品销售许可证□ 电子认证服务许可证□ 电子认证服务使用密码许可证□ 涉密信息系统产品检测证书□ 其他□		接触式□ 非接触式□	SM1□ SM2□ SM3□ SM4□ RSA1024□ RSA2048□ DES□ MD5□ SHA-1□ SHA-256□ 3DES□ AES□ 其他□	国内□ 国外□	
本系统中智能密码钥匙使用情况（如有请填写）												
序号	名称	型号	数量	获国密局批准	生产厂家名称	厂商类型	厂商资质	使用时间	个性化特征	算法使用情况	算法类型	用途
1				是□ 否□		国内□ 国外□	商用密码产品销售许可证□ 计算机信息系统安全专用产品销售许可证□ 电子认证服务许可证□ 涉密信息系统产品检测证书□ 其他□		指纹□ 按键□ 可视□ 其他□	SM1□ SM2□ SM3□ SM4□ RSA1024□ RSA2048□ DES□ MD5□ SHA-1□ SHA-256□ 3DES□ AES□ 其他□	国内□ 国外□	

表 0.13　附表一（续）

本系统中数字证书使用情况（如有请填写）									
CA 数字证书名称	签发方式	建设方式	储存介质	用途	用途	根证书供应商	数字证书产品资质	加密算法	算法类型
	自主签发□ 第三方签发□	自建□ 第三方□	文件□ USBKEY□	网上交易□ 网上远程开户□ 内部办公□ 其他□	加密□ 签名□ 身份认证□ 其他□		商用密码产品销售许可证□ 电子认证服务许可证□ 电子认证服务使用密码许可证□ 涉密信息系统产品检测证书□ 其他□	SM1□ SM2□ SM3□ SM4□ RSA1024□ RSA2048□ DES□ MD5□ SHA-1□ SHA-256□ 3DES□ AES□ 其他□	国内□ 国外□

本系统中密码机使用情况（包括服务器密码机、安全网关、VPN、金融数据密码机等）													
序号	名称	型号	数量	获国密局批准	生产厂家名称	厂商类型	厂商资质	使用时间	是否接入互联网	接入互联网IP 地址/网址	算法使用情况	算法类型	用途
1				是□ 否□		国内□ 国外□	商用密码产品销售许可证□ 计算机信息系统安全专用产品销售许可证□ 涉密信息系统产品检测证书□ 其他□		是□ 否□		SM1□ SM2□ SM3□ SM4□ RSA1024□ RSA2048□ DES□ MD5□ SHA-1□ SHA-256□ 3DES□ AES□ 其他□	国内□ 国外□	

表0.14为表0.12的附表，表0.14应按密码服务系统分别填写。

表0.14　附表二

密码服务系统名称			
密码服务系统建设或集成机构情况			
密码服务系统建设或集成机构	有□ 无□	密码服务系统建设或集成机构名称	
机构性质	国有□ 民营□ 外资□	商密相关资质	生产定点单位□ 销售许可单位 □ 无□
建设时间		是否签订信息安全与保密协议	是□　　否□
建设内容（简述，100 字内）			
密码服务系统运维机构情况			
系统运维机构	有□ 无□	系统运维机构名称	
机构性质	国有□ 民营□ 外资□	商密相关资质	生产定点单位□ 销售许可单位 □ 无□
服务方式	远程在线服务□ 现场服务□	是否签订信息安全与保密协议	是□　　否□
服务内容（简述，100 字内）			
密码服务系统测评机构情况			
密码服务系统测评机构	有□ 无□	密码服务系统测评机构名称	

表 0.14 附表二（续）

机构性质	国有□ 民营□ 外资□	是否具备测评证书	是□　　否□
测评时间		测评证书编号	
测评内容（简述，100 字内）			

表 0.15　A 型营业部情况

<table>
<tr><td colspan="8">基本情况</td></tr>
<tr><td colspan="2">单位名称（全称）</td><td colspan="2"></td><td>所属证监局</td><td colspan="3"></td></tr>
<tr><td colspan="2">所属分公司</td><td colspan="2"></td><td>机构编码</td><td colspan="3"></td></tr>
<tr><td colspan="2">详细地址</td><td colspan="2"></td><td>邮　　编</td><td colspan="3"></td></tr>
<tr><td colspan="8">IT 人员情况</td></tr>
<tr><td rowspan="2">IT 专职员工情况</td><td>总数(人)</td><td>专职软件开发人员数量（人）</td><td>专职运维人员数量（人）</td><td colspan="2">具有计算机相关专业学历员工数量（人）</td><td colspan="2">从事信息技术工作年限 1 年以上员工数量（人）</td></tr>
<tr><td></td><td></td><td></td><td colspan="2"></td><td colspan="2"></td></tr>
<tr><td rowspan="2">IT 兼职员工情况</td><td>总数(人)</td><td colspan="3">具有计算机相关专业学历员工数量（人）</td><td colspan="3">从事信息技术工作年限 1 年以上员工数量(人)</td></tr>
<tr><td></td><td colspan="3"></td><td colspan="3"></td></tr>
<tr><td colspan="8">机房情况</td></tr>
<tr><td colspan="2">机房面积（m^b）</td><td colspan="6"></td></tr>
<tr><td colspan="8">电力情况</td></tr>
<tr><td colspan="2">供电方式（可多选）</td><td colspan="6">三变电站三路供电 □　双变电站双路供电□　单变电站双路供电 □
单路供电□　UPS 设备□　备用发电机□</td></tr>
<tr><td colspan="2">供电站名称（供电来源）</td><td colspan="6"></td></tr>
<tr><td colspan="3">机房设备总功率（KVA）</td><td></td><td colspan="2">现场交易主机总功率（KVA）</td><td colspan="2"></td></tr>
<tr><td colspan="3">电力设施检查周期</td><td></td><td colspan="2">机房空调设施检查周期</td><td colspan="2"></td></tr>
<tr><td colspan="3">UPS 电池放电测试周期</td><td></td><td colspan="2">消防设施检查周期</td><td colspan="2"></td></tr>
<tr><td colspan="8">UPS（不同品牌和功率应增加表格分别填写）</td></tr>
<tr><td colspan="3">UPS 总功率（KVA）</td><td></td><td>平均满载运行时间（小时）</td><td></td><td>平均负载率（%）</td><td></td></tr>
<tr><td>UPS 品牌</td><td>单台功率（KVA）</td><td>数量（台）</td><td colspan="2">联机方式</td><td>满载运行时间（小时）</td><td>当前负载率（%）</td><td>已使用年限（年）</td></tr>
<tr><td></td><td></td><td></td><td colspan="2">并机□ 串机□
未联接□</td><td></td><td></td><td></td></tr>
</table>

表 0.15　A 型营业部情况（续）

发电机（不同品牌和功率应增加表格分别填写）					
品牌	功率（KVA）	储油量维持供电时间（小时）	配备方式	启用所需时间（分钟）	已使用年限
			购买□　租赁发电车□ 租赁物业发电机□		

消防情况			
是否通过当地消防部门验收	是□　否□	是否已向当地消防部门备案	是 □　否 □
消防类型（可多选）	自动喷水灭火□　自动气体灭火□　手动气体灭火 □ 自动泡沫灭火□　手动泡沫灭火□　干粉灭火　□		

机房监控			
是否有视频监控系统	是□　否□	视频资料保存时间（天）	
是否安装门禁系统	是□　否□	门禁系统软件名称	
是否安装环境集中监控系统	是□　否□	环境集中监控软件名称	
环境监控对象（可多选）	空调□　新风机□　温湿度□　配电柜□　UPS□　UPS 电池（整组）□ UPS 电池（单个）□　漏水检测□　机房进出□　消防设施□		
环境监控报警手段（可多选）	声光报警□　自动拨号语音报警□　短信报警□ 电子邮件报警□		

系统监控情况（不同监控软件请逐一填写）							
软件名称及版本	软件厂商	监控对象	监控内容	监控方式	日志保存时间（天）	监控范围	报警手段
		交易软件	进程状态□ 日志信息□ cpu 使用率□ 内存利用率□ 并发线程数□ 并发处理量□ 关键业务指标□	交易时间人工监控□ 交易时间软件监控□ 非交易时间人工监控□ 非交易时间软件监控□		主用系统□ 备份系统□ 同城备份系统□ 异地备份系统□	声光报警□ 自动拨号语音报警□ 短信报警□ 电子邮件报警□ 其他□
		数据库	日志信息□ 表空间使用率□ 连接数□ 日志记录□	同上		同上	
		服务器	运行状况□ cpu 使用率□ 内存利用率□ 磁盘空间□ 通信端口□ 日志记录□	同上		同上	
		存储	运行状况□ 数据交换延时□ 存储电池□ 日志记录□	同上		同上	

表 0.15　A 型营业部情况（续）

<table>
<tr><td colspan="6">行情揭示软件情况（如有请请写，表格不够可增加）</td></tr>
<tr><td colspan="2">软件名称</td><td>软件版本</td><td>软件开发商</td><td>数量（套）</td><td>投入使用时间</td></tr>
<tr><td colspan="2"></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="6">行情资讯软件情况（如有请填写，表格不够可增加）</td></tr>
<tr><td colspan="2">软件名称</td><td>软件版本</td><td>软件开发商</td><td>数量（套）</td><td>投入使用时间</td></tr>
<tr><td colspan="2"></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="6">行情接收情况（如有请填写）</td></tr>
<tr><td rowspan="4">行情接收方式</td><td rowspan="2">深圳行情</td><td colspan="4">主：　多媒体高速单向小站□　双向卫星小站□　总部□　其它□</td></tr>
<tr><td colspan="4">备：　多媒体高速单向小站□　双向卫星小站□　总部□　其它□</td></tr>
<tr><td rowspan="2">上海行情</td><td colspan="4">主：单向宽带广播卫星小站□　宽带双向小站□　总部□　其它□</td></tr>
<tr><td colspan="4">备：单向宽带广播卫星小站□　宽带双向小站□　总部□　其它□</td></tr>
<tr><td colspan="6">安全防护情况</td></tr>
<tr><td>序号</td><td>防病毒木马软件名称</td><td>软件版本号</td><td colspan="2">软件厂商</td><td>部署方式</td></tr>
<tr><td>1</td><td></td><td></td><td colspan="2"></td><td>总部统一部署□
自行部署□</td></tr>
<tr><td colspan="6">网络边界防护情况（可根据该机房划分安全域增加）</td></tr>
<tr><td>重要安全域隔离情况</td><td colspan="2">隔离方式</td><td colspan="3">隔离手段</td></tr>
<tr><td>局域网与公司广域网</td><td colspan="2">物理隔离□ 逻辑隔离□ 未隔离□
无此项□</td><td colspan="3">防火墙□ 网闸□　数据网关□
路由器□ 交换机□ 协议隔离□　Vlan□
其它□</td></tr>
<tr><td>局域网与互联网</td><td colspan="2">同上</td><td colspan="3">同上</td></tr>
</table>

表 0.15　A 型营业部情况（续）

内部通信连接情况									
1.与总部通信连接情况									
序号	通信对端名称	通信对端机房类型	主备方式	运营商	连接类型	线路类型	带宽	流量负载率（%）	线路用途
1		主机房□ 同城备份机房□ 异地备份机房□ 网上信息机房□ 其它□	主□ 备□		DDN□ SDH□ MSTP□ ATM□ 局域网□ 裸光纤□ 互联网 VPN□ 3G□ 电话拨号□ 其它□	局域网□ 本市□ 本省□ 跨省□ 跨境□			交易□ 行情□ 结算□ 融资融券□ 开户□ 会员服务□ 资讯信息□ 证监会及证监局数据报送□ 保证金监控数据报送□ 资本市场监测数据□ 人民银行反洗钱数据报送□ 上市公司数据报送□ 数据备份□ 银证数据交换□ 中国债券登记公司数据□ 信托保险业务数据交换□ 场外市场数据传输□ 外汇交易中心数据□ 境外市场接入□ 交易仿真测试□ 联合测试□ 视频会议□ 应急指挥□ 办公□ 身份认证□ 其他□
2.与其他营业部通信连接情况									
序号	通信对端名称	通信对端类型	主备方式	运营商	连接类型	线路类型	带宽	流量负载率（%）	线路用途
1		A 型营业部□ B 型营业部□ C 型营业部□	同上		同上	同上			同上

表 0.16　B 型营业部情况

<table>
<tr><td colspan="8">基本情况</td></tr>
<tr><td colspan="2">单位名称（全称）</td><td colspan="2"></td><td>所属证监局</td><td colspan="3"></td></tr>
<tr><td colspan="2">所属分公司</td><td colspan="2"></td><td>机构编码</td><td colspan="3"></td></tr>
<tr><td colspan="2">详细地址</td><td colspan="2"></td><td>邮　编</td><td colspan="3"></td></tr>
<tr><td colspan="8">IT 人员情况</td></tr>
<tr><td rowspan="2">IT 专职员工情况</td><td>总数(人)</td><td>专职软件开发人员数量（人）</td><td colspan="2">专职运维人员数量（人）</td><td>具有计算机相关专业学历员工数量（人）</td><td colspan="2">从事信息技术工作年限 1 年以上员工数量（人）</td></tr>
<tr><td></td><td></td><td colspan="2"></td><td></td><td colspan="2"></td></tr>
<tr><td rowspan="2">IT 兼职员工情况</td><td>总数(人)</td><td colspan="3">具有计算机相关专业学历员工数量（人）</td><td colspan="3">从事信息技术工作年限 1 年以上员工数量(人)</td></tr>
<tr><td></td><td colspan="3"></td><td colspan="3"></td></tr>
<tr><td colspan="8">机房情况（如有请填写）</td></tr>
<tr><td colspan="2">是否有机房</td><td colspan="2">是□　　否□</td><td>机房面积（m[b)]</td><td colspan="3"></td></tr>
<tr><td colspan="8">电力情况</td></tr>
<tr><td colspan="2">供电方式（可多选）</td><td colspan="6">三变电站三路供电 □　双变电站双路供电□　　单变电站双路供电 □
单路供电□　　UPS 设备□　　备用发电机□</td></tr>
<tr><td colspan="2">供电站名称（供电来源）</td><td colspan="6"></td></tr>
<tr><td colspan="2">机房设备总功率（KVA）</td><td colspan="2"></td><td colspan="2">现场交易主机总功率（KVA）</td><td colspan="2"></td></tr>
<tr><td colspan="2">电力设施检查周期</td><td colspan="2"></td><td colspan="2">机房空调设施检查周期</td><td colspan="2"></td></tr>
<tr><td colspan="2">UPS 电池放电测试周期</td><td colspan="2"></td><td colspan="2">消防设施检查周期</td><td colspan="2"></td></tr>
<tr><td colspan="8">UPS（不同品牌和功率应增加表格分别填写）</td></tr>
<tr><td colspan="2">UPS 总功率（KVA）</td><td></td><td>平均满载运行时间（小时）</td><td></td><td>平均负载率（%）</td><td colspan="2"></td></tr>
<tr><td>UPS 品牌</td><td>单台功率（KVA）</td><td>数量（台）</td><td>联机方式</td><td colspan="2">满载运行时间（小时）</td><td>当前负载率（%）</td><td>已使用年限（年）</td></tr>
<tr><td></td><td></td><td></td><td>并机□ 串机□
未联接□</td><td colspan="2"></td><td></td><td></td></tr>
<tr><td colspan="8">发电机（不同品牌和功率应增加表格分别填写）</td></tr>
<tr><td>品牌</td><td>功率（KVA）</td><td>储油量维持供电时间（小时）</td><td colspan="2">配备方式</td><td>启用所需时间（分钟）</td><td colspan="2">已使用年限（年）</td></tr>
<tr><td></td><td></td><td></td><td colspan="2">购买□　租赁发电车□
租赁物业发电机□</td><td></td><td colspan="2"></td></tr>
</table>

表 0.16　B 型营业部情况（续）

行情揭示软件情况（如有请请写，表格不够可增加）				
软件名称	软件版本	软件开发商	数量（套）	投入使用时间

行情资讯软件情况（如有请填写，表格不够可增加）				
软件名称	软件版本	软件开发商	数量（套）	投入使用时间

消防情况			
是否通过当地消防部门验收	是□　　否□	是否已向当地消防部门备案	是 □　否 □
消防类型（可多选）	自动喷水灭火□ 自动泡沫灭火□	自动气体灭火□ 手动泡沫灭火□	手动气体灭火 □ 干粉灭火　　□

安全防护情况				
序号	防病毒木马软件名称	软件版本号	软件厂商	部署方式
1				总部统一部署□ 自行部署□

网络边界防护情况（可根据该机房划分安全域增加）		
重要安全域隔离情况	隔离方式	隔离手段
局域网与公司广域网	物理隔离□ 逻辑隔离□ 未隔离□ 无此项□	防火墙□ 网闸□　数据网关□ 路由器□ 交换机□ 协议隔离□　Vlan□ 其它□
局域网与互联网	同上	同上

内部通信连接情况

表 0.16　B 型营业部情况（续）

1.与总部通信连接情况									
序号	通信对端名称	通信对端机房类型	主备方式	运营商	连接类型	线路类型	带宽	流量负载率（%）	线路用途
1		主机房□ 同城备份机房□ 异地备份机房□ 网上信息机房□ 其它□	主□ 备□		DDN□ SDH□ MSTP□ ATM□ 局域网□ 裸光纤□ 互联网 VPN□ 3G□ 电话拨号□ 其它□	局域网□ 本市□ 本省□ 跨省□ 跨境□			交易□ 行情□ 结算□ 融资融券□ 开户□ 会员服务□ 资讯信息□ 证监会及证监局数据报送□ 保证金监控数据报送□ 资本市场监测数据□ 人民银行反洗钱数据报送□ 上市公司数据报送□ 数据备份□ 银证数据交换□ 中国债券登记公司数据□ 信托保险业务数据交换□ 场外市场数据传输□ 外汇交易中心数据□ 境外市场接入□ 交易仿真测试□ 联合测试□ 视频会议□ 应急指挥□ 办公□ 身份认证□ 其他□
2.与其他营业部通信连接情况									
序号	通信对端名称	通信对端类型	主备方式	运营商	连接类型	线路类型	带宽	流量负载率（%）	线路用途
1		A 型营业部□ B 型营业部□ C 型营业部□	同上		同上	同上			同上

表 0.16　B 型营业部情况（续）

基本情况				
单位名称（全称）			所属证监局	
详细地址			邮　　编	
机房情况（如有，请填写）				
是否有机房	是□　　否□		机房面积（$m^{b)}$	
安全防护情况				
序号	防病毒木马软件名称	软件版本号	软件厂商	部署方式
1				总部统一部署□ 自行部署□