ICS 03.060
A 11

JR

中华人民共和国金融行业标准

JR/T 0146.3—2016

证券期货业信息系统审计指南 第3部分：证券登记结算机构

Securities and futures industry audit guideline for information system —

Part 3: Securities depository and clearing corporation

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

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 0146.3-2016《证券期货业信息系统审计指南》的第3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3部分：证券登记结算机构

1 范围

本部分给出了证券登记结算机构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登记结算机构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。

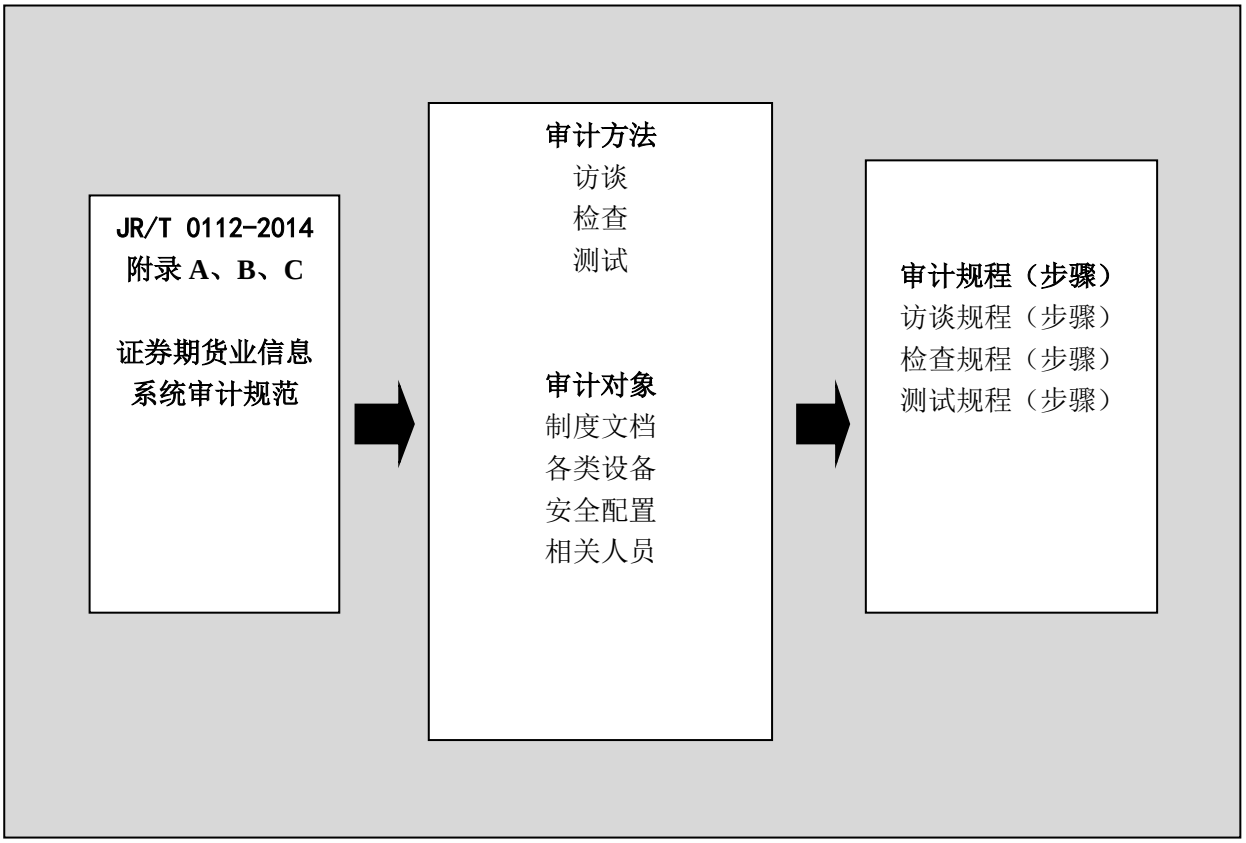

图1 概念性框架

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K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、交易系统、重要信息系统、信息系统建设合规、信息系统应用绩效、信息系统托管的审计方法。附录L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L，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　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、制定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□	

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
1.1.16.	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□	
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□	

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
1.1.22.	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□	
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□	
1.1.25.	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□	
1.1.26.	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。	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□	
1.1.27.	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□	
1.1.28.	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
1.1.29.	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□	
1.1.30.	是否建立保密制度，并定期或不定期的对保密制度执行情况进行检查或考核。	a)检查安全保密制度； b)检查是否对安全保密制度执行情况进行检查或考核，并查看检查记录或考核记录。	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□	
1.2.5.	是否明确需要定期修订的安全管理制度，并指定负责人或负责部门负责制度的日常维护。	a)检查是否具有需要定期修订的安全管理制度列表，查看列表是否注明修订周期； b)询问负责制度的日常维护部门的的负责人，了解对需要定期修订的安全管理制度进行修订的周期； c)检查修订记录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□	

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
1.2.6.	是否根据安全管理制度的相应密级确定评审和修订的操作范围。	a)访谈安全主管，询问评审和修订有密级的安全管理制度时对参加评审和修订的人员是否考虑到相应保密要求； b)检查评审和修订记录，判断是否根据安全管理制度的相应密级进行评审和修订。	是□ 否□ 不适用□	
1.3.	**日常操作**			
1.3.1.	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□	
1.3.2.	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□	
1.4.4.	有密级的安全管理制度，是否注明安全管理制度密级，并进行密级管理。	a)访谈安全主管，询问对有密级的管理制度是否注明密级，采取相应措施有效管理； b)检查涉密文件登记记录，确认按照相关规定管理有密级的安全管理制度。	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□	

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
2.2.	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□	
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□	

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
2.10.	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□	
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□	
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，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，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。	检查合作与沟通的会议纪要或来往函件等，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□	

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
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□	
3.6.	是否制定会员单位共同遵守的接口标准和规则，监督会员严格执行。	a)检查会员单位共同遵守的接口标准和规则； b)检查会员沟通记录，判断是否督促会员执行相关规定。	是□ 否□ 不适用□	
3.7.	是否完成对会员单位远程接入系统的安全监控与管理，指导会员对信息安全突发事件进行应急处置。	a)查看对会员单位远程接入系统进行安全监控与管理的情况说明； b)检查沟通记录，判断是否指导会员对信息安全突发事件进行应急处置。	是□ 否□ 不适用□	
3.8.	是否加强对会员的日常性技术支持，不断提高服务能力和水平。	a)检查服务记录，判断是否对会员提供日常性技术支持； b)访谈信息技术负责人，判断是否不断提高服务能力和水平。	是□ 否□ 不适用□	
3.9.	是否组织会员单位定期开展联网测试和应急演练，及时发现安全隐患。	检查“表 L.8-组织市场各经营机构参加的应急演练情况”，检查联网测试和应急演练报告，判断是否组织会员单位定期开展联网测试和应急演练，及时发现安全隐患。	是□ 否□ 不适用□	
4.	**经费管理**			
4.1.	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□	
4.2.	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 L.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□	
4.3.	是否落实软件采购经费，做好软件正版化工作。	a)检查“表 L.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□	

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
4.4.	安全建设的投入是否超过IT总投入的15%。	检查“表 L.2-信息技术投入情况-合计（万元）”、“表L.2-其中:安全投入费用（万元）”，判断安全建设的投入是否超过 IT 总投入的15%。	是□ 否□ 不适用□	
4.5.	是否对资金的使用进行绩效考核。	获取信息技术部门的绩效考核表,检查考核表中是否对资金的使用进行绩效考核。	是□ 否□ 不适用□	
5.	**人员管理**			
5.1.	**教育培训**			
5.1.1.	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 L.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□	
5.1.2.	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□	
5.1.3.	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□	
5.1.4.	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□	

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
5.1.5.	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□	
5.2.	**人员考核**			
5.2.1.	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□	
5.2.2.	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□	
5.2.3.	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□	
5.3.	**人员离岗**			
5.3.1.	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□	
5.3.2.	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□	
5.4.	**人员录用**			
5.4.1.	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□	

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
5.4.2.	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□	
5.4.3.	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□	
5.4.4.	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□	
5.4.5.	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。	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。	是□ 否□ 不适用□	
5.5.	**外部人员管理**			
5.5.1.	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□	

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
5.5.2.	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□	
6.	**组织管理**			
6.1.	**岗位设置**			
6.1.1.	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□	
6.1.2.	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□	
6.1.3.	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□	
6.1.4.	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□	
6.1.5.	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 L.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□	
6.1.6.	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□	

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
6.1.7.	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□	
6.1.8.	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□	
6.1.9.	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□	
6.1.10.	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□	
6.1.11.	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□	
6.1.12.	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□	
6.1.13.	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□	
6.1.14.	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□	

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
6.1.15.	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□	
6.1.16.	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□	
6.1.17.	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□	
6.1.18.	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□	
6.1.19.	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□	
6.1.20.	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□	
6.1.21.	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□	
6.1.22.	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□	
6.1.23.	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□	

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
6.1.24.	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 L.9-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□	
6.1.25.	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□	
6.1.26.	是否对关键和敏感岗位进行重点管理，重要操作应当实行双人操作复核制度。	a)检查岗位说明和操作流程，明确关键和敏感岗位； b)检查关键和敏感岗位操作记录，确认实行双人复核。	是□ 否□ 不适用□	
6.1.27.	是否配备保密管理人员，落实技术保密措施，每年至少开展两次保密检查，确保不发生数据泄露等失密事件。	a)查看技术保密措施情况说明，访谈保密管理人员，了解技术保密措施的落实情况； b)查看保密检查工作记录，判断保密检查次数>= 2 次/年。	是□ 否□ 不适用□	
6.2.	**机构设置**			
6.2.1.	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□	
6.2.2.	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□	
6.2.3.	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□	

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
6.2.4.	是否成立指导和管理信息安全工作的委员会或领导小组，其最高领导由单位主管领导委任或授权。	a)检查“表 L.1-指导和管理信息安全工作的委员会或领导小组组成人员”，检查是否有信息安全管理委员会或领导小组成立的正式文件和成员名单； b)访谈单位主管领导，了解指导和管理信息安全工作的委员会或领导小组的最高领导是否由其委任或授权。	是□ 否□ 不适用□	
6.3.	**审核检查**			
6.3.1.	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□	
6.3.2.	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□	
6.3.3.	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；安全检查应至少每月一次。	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月一次。	是□ 否□ 不适用□	
6.4.	**授权审批**			
6.4.1.	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□	

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
6.4.2.	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□	
6.4.3.	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□	
6.4.4.	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，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 L.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 L.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 L.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
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 L.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□	
3.8.	消防设施是否具备自动监测报警和气体灭火能力，通过当地公安机关的验收并保持功能正常。	a)检查“表 L.3-消防情况”、“表 L.3 机房监控情况”和公司提供的机房情况说明，包括自动灭火设施和气体灭火能力，查看消防验收材料； b)现场检查公司的机房的自动灭火设施，是否符合情况说明。	是□ 否□ 不适用□	
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□	

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
4.2.	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□	
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□	

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
6.5.	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.	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□	
7.5.	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□	
7.6.	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□	
7.7.	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□	

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
7.8.	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□	
7.9.	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□	
7.10.	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□	
7.11.	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□	
7.12.	是否机房出入应当安排专人负责管理，人员进出记录应至少保存 3 个月。	a)检查机房出入口是否有专人值守负责控制、鉴别进入机房的人员，是否有值守记录和电子门禁记录； b)检查人员进出监控记录是否保存 3 个月以上。	是□ 否□ 不适用□	
7.13.	是否采用监控设备将机房人员进出情况传输到值班点，对外来人员出入机房进行控制、鉴别和记录。	a)现场检查机房和重要区域是否配置了电子门禁系统，每道电子门禁系统是否都有验收文档或产品安全认证资质； b)现场检查来访人员进入机房时是否对其行为进行限制和监控； c)现场检查是否采用监控设备将机房人员进出情况传输到值班点。	是□ 否□ 不适用□	
7.14	是否对机房和办公环境实行统一策略的安全管理，对出入人员进行相应级别的授权，对进入重要安全区域的活动行为实时监视和记录。	a)检查机房与办公环境管理相关制度； b)检查办公环境是否有与机房相同的物理安全措施，如门禁控制、摄像监控系统等，出入办公环境和机房不同区域是否要经过相应级别的授权； c)现场观察机房运维管理，是否符合情况说明； d)检查门禁记录和机房监控录像记录。	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□	

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
8.2.	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□	
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 L.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 L.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 L.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 L.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□	

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
8.10.	是否对机房和设备至少每 2 小时巡检一次，重要敏感时期提高巡检频度。	a)审阅机房管理制度及巡检管理相关制度，是否规定对机房和设备至少每 2 小时巡检一次； b)审阅机房管理制度及巡检管理相关制度，是否规定重要敏感时期提高巡检频度； c)检查机房和设备巡检记录，确认是否符合审计项要求。	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.	空调系统是否采用恒温恒湿的精密空调，并保证有足够的富余能力。	a)检查“表 L.3-空调”和机房空调情况说明，精密空调热容量是否与机房中配置的设备功率相匹配； b)检查机房精密空调的冗余，应当在缺少任何一台精密空调工作的情况下，剩余精密空调的热容量与机房中配置的设备功率相匹配。	是□ 否□ 不适用□	
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□	

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
10.3.	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□	
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□	

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
11.4.	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

<table>
<tr><td>被审计部门：</td><td>索引号：WLGL</td></tr>
<tr><td>审计主题：网络管理</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 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.	安全管理			
1.1.	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□	
1.2.	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□	
1.3.	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□	
1.4.	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 L.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□	
1.5.	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□	
1.6.	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□	

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
1.7.	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□	
1.8.	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□	
1.9.	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□	
1.10.	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□	
1.11.	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□	
1.12.	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□	
1.13.	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□	

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
1.14.	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□	
1.15.	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□	
1.16.	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□	
2.	**安全审计**			
2.1.	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□	
2.2.	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□	
2.3.	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□	

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
2.4.	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□	
2.5.	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□	
2.6.	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□	
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□	

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
3.4.	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□	
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□	

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.	**结构安全**			
4.1.	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□	
4.2.	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□	
4.3.	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□	
4.4.	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□	
4.5.	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□	

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
4.6.	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 L.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□	
4.7.	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□	
4.8.	通信带宽是否保持在历史流量峰值的 4 倍以上。	a)检查网络设计或验收文档，查看带宽设计容量； b)检查“表 L.6-外联通信情况”、“表 L.6-内部通信情况”、网络监控日志，查看历史峰值。确定通信带宽是否保持在历史流量峰值的 4 倍以上。	是□ 否□ 不适用□	
4.9.	重要线路是否至少具有一条以上的备份线路。	检查“表 L.6-外联通信情况”、“表 L.6-内部通信情况”网络设计或验收文档，查看是否至少具有一条以上的备份线路。	是□ 否□ 不适用□	
4.10.	与交易业务相关的系统是否在行业专网上部署。	检查网络设计或验收文档，查看与交易业务相关的系统是否在行业专网上部署。	是□ 否□ 不适用□	
5.	**身份鉴别**			
5.1.	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□	
5.2.	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□	
5.3.	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□	
5.4.	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□	
5.5.	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□	

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
5.6.	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□	
5.7.	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□	
5.8.	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□	
5.9.	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□	
5.10.	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□	
5.11.	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□	
5.12.	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□	

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.	**网络运维**			
6.1.	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□	
6.2.	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□	
6.3.	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□	
6.4.	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□	
6.5.	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□	

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
6.6.	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□	
6.7.	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□	
6.8.	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□	
6.9.	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□	
6.10.	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□	

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
6.11.	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□	
6.12.	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□	
6.13.	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□	

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.	**安全管理**			
1.1.	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□	
1.2.	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□	
2.	**产品采购**			
2.1.	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 L.10-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□	
2.2.	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□	
2.3.	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□	
3.	**配置管理**			
3.1.	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□	
3.2.	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□	

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
3.3.	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□	
3.4.	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□	
3.5.	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□	
3.6.	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□	
3.7.	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□	
3.8.	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□	
4.	**日常操作**			
4.1.	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□	
4.2.	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□	
4.3.	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□	
4.4.	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□	

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
4.5.	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□	
4.6.	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□	
4.7.	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□	
4.8.	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□	
4.9.	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□	
5.	**事件与问题管理**			
5.1.	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□	
5.2.	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□	
5.3.	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。	查看运维事件记录，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□	
5.4.	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□	
5.5.	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□	

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
5.6.	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□	
5.7.	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□	
5.8.	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□	
5.9.	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□	
6.	**数据和介质管理**			
6.1.	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□	
6.2.	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□	
6.3.	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□	

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
6.4.	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□	
6.5.	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□	
6.6.	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□	
6.7.	交易业务系统数据是否至少每交易日备份一次。	查看“表 L.4-数据备份情况”、“表 L.5-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□	
6.8.	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□	
6.9.	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□	
6.10.	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□	
6.11.	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□	

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
6.12.	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 L.4-数据备份情况”、“表 L.5-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□	
6.13.	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□	
6.14.	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□	
6.15.	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□	
6.16.	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 L.4-数据备份情况”和数据备份记录，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□	
6.17.	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□	
6.18.	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□	
6.19.	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□	
6.20.	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□	
6.21.	对执行程序、源代码及相关文档是否采取严密措施妥善、安全保管。	访谈安全管理员，为妥善、安全保管执行程序、源代码及相关文档，采取了哪些措施。	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
7.	**调查处理**			
7.1.	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□	
7.2.	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□	
7.3.	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□	
7.4.	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□	
7.5.	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□	
7.6.	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□	
7.7.	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□	

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
7.8.	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□	
7.9.	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□	
7.10.	是否向中国证监会进行预警报告、应急报告和事件总结报告。	检查应急报告记录，是否向证信办进行应急报告。	是□ 否□ 不适用□	
7.11.	发生信息安全事件影响到其他机构的，是否及时向有关机构进行应急通报。	检查应急报告记录，发生信息安全事件影响到其它机构的，是否向有关机构进行应急通报。	是□ 否□ 不适用□	
8.	**外包软件开发**			
8.1.	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□	
8.2.	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□	
8.3.	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□	
9.	**应急处置**			
9.1.	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□	

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
9.2.	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□	
9.3.	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□	
9.4.	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□	
9.5.	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□	
9.6.	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□	
9.7.	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□	
9.8.	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□	
9.9.	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□	

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
9.10.	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□	
9.11.	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□	
9.12.	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□	
9.13.	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□	
10.	**应急演练**			
10.1.	是否定期进行消防设施的使用培训和演习。	a)检查“表L.8-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□	
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 L.8-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 L.8-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.	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□	
11.24.	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□	
11.25.	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□	

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.	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□	
11.27.	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□	
11.28.	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□	
11.29.	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□	
11.30.	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□	
11.31.	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□	

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□	
11.33.	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□	
11.34.	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□	
11.35.	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□	
11.36.	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 L.8-本年度应急演练情况”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□	
11.37.	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□	
11.38.	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□	
11.39.	应急培训内容是否包括应急预案、证券期货业信息安全应急处置的有关规定。	检查应急培训记录，培训内容是否包括应急预案、证券期货业信息安全应急处置的有关规定。	是□ 否□ 不适用□	
11.40.	是否随着信息系统的变更定期对原有的应急预案重新评估，修订完善。	检查应急预案定期修订的记录，判断是否随着信息系统的变更定期对原有的应急预案重新评估，修订完善。	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
11.41.	是否向证信办报备应急预案。	检查应急预案报备记录。	是□ 否□ 不适用□	
11.42.	是否每年向证信办报告年度应急演练情况。	检查应急演练报备记录，核心机构是否每年向中国证监会报告年度应急演练情况。	是□ 否□ 不适用□	
12.	**资产管理**			
12.1.	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□	
12.2.	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□	
12.3.	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□	
12.4.	d)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□	
12.5.	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□	
13.	**自行软件开发**			
13.1.	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□	

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
13.2.	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□	
13.3.	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□	
13.4.	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□	
13.5.	是否拥有行情、交易、结算、开户等关键核心系统的执行程序及源代码所有权和自主研发能力。	检查“表 L.5-信息系统全称”、“表 L.5-软件开发情况”，访谈开发负责人，询问是否拥有行情、交易、结算、开户等关键核心系统的执行程序及源代码所有权和自主研发能力。	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：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L.7-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L.7-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证信办。	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证信办。	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L.7-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□	
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L.7-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□	

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
4.2.	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.	定级结果是否经过证信办批准，由证信办出具定级审核意见。	检查是否将定级结果向证信办报批，并由证信办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L.9-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L.9-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L.9-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L.9-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□	

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
9.	办公文字处理软件是否有授权。	检查“表L.9-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□	
10.	办公专业处理软件是否有授权。	检查“表L.9-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L.9-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L.9-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）
登记结算系统审计底稿

表G.1至表G.2给出了登记结算系统审计的程序、内容及相关记录要求。

表G.1 登记结算系统审计底稿

被审计部门：	索引号：DJJSXT
审计主题：登记结算系统	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　登记结算系统审计底稿（续）

审计证据列表：

表G.2　登记结算系统审计底稿

序号	审计项	审计程序	审计结论	备注
1.	**数据库管理**			
1.1.	**身份鉴别**			
1.1.1.	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□	
1.1.2.	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□	
1.1.3.	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□	
1.1.4.	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□	
1.1.5.	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□	
1.2.	**安全审计**			
1.2.1.	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□	
1.2.2.	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□	
1.2.3.	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□	

表 G.2　登记结算系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
1.2.4.	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□	
1.2.5.	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□	
1.2.6.	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□	
1.3.	**数据库运维**			
1.3.1.	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□	
1.3.2.	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□	
1.3.3.	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□	
1.3.4.	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□	
1.3.5.	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　登记结算系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.	**核心系统**			
2.1.	**结构安全**			
2.1.1.	结算系统容量是否至少达到当前市场品种、市值、交易量和投资者规模的 2 倍以上。	审阅结算系统情况说明相关文档，检查结算系统容量是否至少达到当前市场品种、市值、交易量和投资者规模的 2 倍以上。	是□ 否□ 不适用□	
2.1.2.	处理能力是否至少具有历史交易峰值 4 倍以上的日处理能力。	检查“表 L.4-登记结算系统处理能力”，检查处理能力评估报告，判断处理能力是否至少具有历史交易峰值 4 倍以上的日处理能力。	是□ 否□ 不适用□	
3.	**主机管理**			
3.1.	**身份鉴别**			
3.1.1.	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□	
3.1.2.	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□	
3.1.3.	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□	
3.1.4.	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□	
3.1.5.	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□	
3.1.6.	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 L.11 附表一-信息系统名称”、“表 L.11 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□	

表 G.2　登记结算系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
3.1.7.	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□	
3.1.8.	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□	
3.1.9.	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□	
3.2.	**访问控制**			
3.2.1.	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□	
3.2.2.	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□	
3.2.3.	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□	
3.2.4.	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□	

表 G.2　登记结算系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
3.2.5.	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□	
3.3.	**安全审计**			
3.3.1.	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□	
3.3.2.	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□	
3.3.3.	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□	
3.3.4.	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□	
3.3.5.	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□	

表 G.2　登记结算系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
3.3.6.	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□	
3.4.	**安全管理**			
3.4.1.	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□	
3.4.2.	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 L.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□	
3.4.3.	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□	

表 G.2　登记结算系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
3.4.4.	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 L.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□	
3.4.5.	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□	
3.4.6.	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□	
3.4.7.	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□	
3.4.8.	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□	

表 G.2　登记结算系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
3.4.9.	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□	
3.5.	**资源控制**			
3.5.1.	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□	
3.5.2.	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□	
3.5.3.	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□	
3.6.	**主机运维**			
3.6.1.	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 L.4-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□	
3.6.2.	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□	
4.	**系统管理**			
4.1.	**系统架构**			
4.1.1.	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□	
4.1.2.	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□	

表 G.2　登记结算系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
4.2.	**系统建设**			
4.2.1.	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□	
4.2.2.	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□	
4.2.3.	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□	
4.2.4.	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□	
4.2.5.	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□	
4.2.6.	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□	
4.2.7.	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□	

表 G.2　登记结算系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
4.2.8.	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□	
4.2.9.	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□	
4.2.10.	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□	
4.2.11.	是否制定了本机构与市场相关主体信息系统安全互联的技术规则，并报证信办备案，同时依法督促市场相关主体执行技术规则。	a)访谈信息技术负责人，询问是否制定了本机构与市场相关主体信息系统安全互联的技术规则； b)检查技术规则，查看向证信办备案的记录。	是□ 否□ 不适用□	
4.3.	**测试验收**			
4.3.1.	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□	

表 G.2　登记结算系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
4.3.2.	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□	
4.3.3.	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□	
4.3.4.	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□	
4.3.5.	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□	
4.3.6.	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□	
4.3.7.	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□	
4.3.8.	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　登记结算系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
4.3.9.	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 L.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□	
4.3.10.	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□	
4.3.11.	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□	
4.3.12.	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□	
4.3.13.	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□	
4.3.14.	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□	
4.3.15.	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□	
4.3.16.	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□	

表 G.2　登记结算系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
4.3.17.	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□	
4.3.18.	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□	
4.3.19.	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□	
4.3.20.	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□	
4.3.21.	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□	
4.3.22.	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□	
4.3.23.	系统上线或变更升级前，是否对执行程序及源代码进行严格审查、测试。	a)访谈开发负责人，系统上线或变更升级前，是否对执行程序及源代码进行严格审查、测试； b)检查对执行程序及源代码的审查结果、测试报告。	是□ 否□ 不适用□	
4.4.	**系统运维**			
4.4.1.	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□	

表 G.2　登记结算系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
4.4.2.	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□	
4.4.3.	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□	
4.4.4.	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□	
4.4.5.	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□	
4.4.6.	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□	
4.4.7.	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　登记结算系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
4.4.8.	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 L.5-系统监控情况-服务器”，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□	
4.4.9.	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 L.5-系统监控情况-存储”，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□	
4.4.10.	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 L.5-系统监控情况-数据库”，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□	
4.4.11.	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 L.5-系统监控情况-信息系统”，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□	
4.4.12.	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□	
4.4.13.	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□	
4.4.14.	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□	

表 G.2　登记结算系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
4.4.15.	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□	
4.4.16.	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□	
4.4.17.	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□	
4.4.18.	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□	
4.4.19.	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□	
4.4.20.	是否对系统资源的使用进行预测，以确保充足的处理速度和存储容量，管理人员应随时注意系统资源的使用情况，包括处理器、存储设备和输出设备。	a)检查系统、数据库以及网络评估报告，是否对资源的使用进行预测,以确保充足的处理速度和存储容量; b)访谈系统管理员,了解是否监控系统资源的使用情况，包括处理器、存储设备和输出设备。	是□ 否□ 不适用□	
4.5.	**变更管理**			
4.5.1.	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□	
4.5.2.	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　登记结算系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
4.5.3.	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□	
4.5.4.	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□	
4.5.5.	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□	
4.5.6.	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□	
4.5.7.	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□	
4.5.8.	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□	
4.5.9.	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□	
4.5.10.	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□	

表 G.2　登记结算系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
4.5.11.	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□	
4.5.12.	是否定期检查变更控制的申报和审批程序的执行情况，评估系统现有状况与文档记录的一致性。	抽查定期检查变更控制的申报和审批程序的执行情况记录，是否评估系统现有状况与文档记录的一致性。	是□ 否□ 不适用□	
4.5.13.	重大的系统变更升级是否组织会员进行严格的联网测试，是否制定专项的应急预案和回退方案。	检查重大系统变更的专项应急预案和回退方案、联网测试记录，是否组织会员进行严格的联网测试。	是□ 否□ 不适用□	
4.5.14.	在开展重大信息系统项目建设、迁移或改造时，是否事前向证信办进行报告，并定期报告项目进展情况。	检查项目建设报告记录，是否在开展重大信息系统项目建设、迁移或改造时，事前向证信办进行报告，并定期报告项目进展情况。	是□ 否□ 不适用□	
4.6.	**安全管理**			
4.6.1.	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□	
4.6.2.	是否每月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。	检查“表 L.3-该机房的网络安全检查情况”，检查是否有网络漏洞扫描报告，是否至少每月进行一次漏洞扫描，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□	

表 G.2　登记结算系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
4.6.3.	实施漏洞扫描或漏洞修补前，是否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。	检查漏洞扫描和修补报告，查看扫描和修补工作是否在恰当的时间，对可能存在的风险进行充分评估和准备，制定回退方案，备份重要数据后进行的。	是□ 否□ 不适用□	
4.6.4.	漏洞扫描或漏洞修补后，是否进行验证测试，以保证系统的正常运行。	检查漏洞扫描和修补报告，查看完成扫描和修补工作后，是否进行了验证测试，以保证网络系统的正常运行。	是□ 否□ 不适用□	
4.7.	**身份鉴别**			
4.7.1.	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□	
4.7.2.	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□	
4.7.3.	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□	
4.7.4.	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□	
4.7.5.	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□	

表 G.2　登记结算系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
4.7.6.	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□	
4.7.7.	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□	
4.7.8.	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□	
4.7.9.	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□	
4.7.10.	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□	
4.7.11.	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□	
4.7.12.	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□	
4.7.13.	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　登记结算系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
4.8.	**访问控制**			
4.8.1.	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□	
4.8.2.	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□	
4.8.7.	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□	
4.8.4.	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□	
4.8.5.	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　登记结算系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
4.8.6.	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□	
4.9.	**资源控制**			
4.9.1.	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□	
4.9.2.	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□	
4.9.3.	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□	
4.9.4.	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□	
4.9.5.	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□	
4.9.6.	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□	
4.9.7.	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　登记结算系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
4.10.	**数据安全**			
4.10.1.	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□	
4.10.2.	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□	
4.10.3.	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□	
4.11.	**备份能力**			
4.11.1.	是否至少每天备份数据一次；备份介质应当在本地机房、同城及异地安全可靠存放；每周至少对数据备份进行一次有效性验证。	a)检查“表 L.5-数据备份情况”，查看数据备份记录，确认开户、交易、行情、转账、登记、存管、结算、查询和相关业务办理的数据等重重要数据每日在本地、同城、异地备份； b)查看数据有效性验证记录,确认每周对数据备份进行了一次有效性验证。	是□ 否□ 不适用□	
4.11.2.	实时信息系统灾难应对能力是否满足：信息系统恢复时间目标 RTO 小于 3 小时；信息系统恢复点目标 RPO 小于 1 分钟；备份系统具有满足业务需求的处理能力。	检查“表 L.5-系统备份能力”，查看实时信息系统灾难应对能力达标证明材料（包括：灾难备份系统建设情况、备份策略、应急演练记录等），判断实时信息系统灾难应对能力是否满足：RTO 小于 3 小时；信息系统恢复点目标 RPO 小于 1 分钟；备份系统具有满足业务需求的处理能力。	是□ 否□ 不适用□	
4.11.3.	非实时信息系统灾难应对能力是否满足：信息系统恢复时间目标 RTO 小于 6 小时；信息系统恢复点目标 RPO 等于 0 秒；备份系统具有满足业务需求的处理能力。	检查“表 L.5-系统备份能力”，查看非实时信息系统灾难应对能力达标证明材料（包括：灾难备份系统建设情况、备份策略、应急演练记录等），判断非实时信息系统灾难应对能力是否满足：RTO 小于 6 小时；信息系统恢复点目标 RPO 等于 0 秒；备份系统具有满足业务需求的处理能力。	是□ 否□ 不适用□	

表 G.2　登记结算系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
4.11.4.	实时信息系统故障应对能力是否满足：信息系统恢复时间目标 RTO 小于 3 分钟；信息系统恢复点目标 RPO 小于 30 秒；备份系统具有满足业务需求的处理能力。	检查“表 L.5-系统备份能力”，查看实时信息系统故障应对能力达标证明材料（包括：灾难备份系统建设情况、备份策略、应急演练记录等），判断实时信息系统故障应对能力是否满足：RTO 小于 3 分钟；信息系统恢复点目标 RPO 小于 30 秒；备份系统具有满足业务需求的处理能力。	是□ 否□ 不适用□	
4.11.5.	非实时信息系统故障应对能力是否满足：信息系统恢复时间目标 RTO 小于 1 小时；信息系统恢复点目标 RPO 等于 0 秒；备份系统具有满足业务需求的处理能力。	检查“表 L.5-系统备份能力”，查看非实时信息系统故障应对能力达标证明材料（包括：灾难备份系统建设情况、备份策略、应急演练记录等），判断非实时信息系统故障应对能力是否满足：RTO 小于 1 小时；信息系统恢复点目标 RPO 等于 0 秒；备份系统具有满足业务需求的处理能力。	是□ 否□ 不适用□	
4.11.6.	实时信息系统重大灾难应对能力是否满足：信息系统恢复时间 RTO 小于 3 天；信息系统恢复点目标RPO小于5分钟；备份系统具有满足业务需求的处理能力。	检查“表 L.5-系统备份能力”，查看实时信息系统重大灾难应对能力达标证明材料（包括：灾难备份系统建设情况、备份策略、应急演练记录等），判断实时信息系统重大灾难应对能力是否满足：信息系统恢复时间 RTO 小于 3 天；信息系统恢复点目标 RPO 小于 5 分钟；备份系统具有满足业务需求的处理能力。	是□ 否□ 不适用□	
4.11.7.	非实时信息系统重大灾难应对能力是否满足：信息系统恢复时间目标 RTO 小于 3 天；信息系统恢复点目标 RPO 等于 0 秒；备份系统具有满足业务需求的处理能力。	检查“表 L.5-系统备份能力”，查看非实时信息系统重大灾难应对能力达标证明材料（包括：灾难备份系统建设情况、备份策略、应急演练记录等），判断非实时信息系统重大灾难应对能力是否满足：信息系统恢复时间目标 RTO 小于 3 天；信息系统恢复点目标 RPO 等于 0 秒；备份系统具有满足业务需求的处理能力。	是□ 否□ 不适用□	
4.11.8.	重要业务数据、执行程序和源代码是否同时备份到同城和异地的安全地点。	检查“表 L.5-数据备份情况”，查看备份记录，开户、交易、行情、转账、登记、存管、结算、查询和相关业务办理的数据、执行程序和源代码是否每日备份到同城和异地的安全地点。	是□ 否□ 不适用□	
4.11.9.	在主用设备故障时，是否能切换到备份系统，自动隔离并保留故障设备以备事后调查。	a)检查应急演练报告中主备实时切换方法，及切换演练记录； b)检查操作记录，主备实时切换后，是否自动隔离并保留故障设备以备事后调查。	是□ 否□ 不适用□	

表 G.2　登记结算系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
4.11.10.	交易、结算、开户等关键业务系统的同城和异地灾备系统处理能力是否与主系统能力相同。	检查“表 L.5-备份系统处理能力”，检查同城及异地灾备系统处理能力报告和压力测试报告，比对交易、结算、开户等关键业务系统同城和异地灾备系统与主系统的处理能力指标，判断三者能力是否相同。	是□ 否□ 不适用□	
4.11.11.	备份中心是否能够同时支持会员单位备份系统的接入。	检查备份中心网络通信情况说明，是否能够支持会员单位备份系统的接入。	是□ 否□ 不适用□	
4.12.	**安全审计**			
4.12.1.	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□	
4.12.2.	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□	
4.12.3.	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□	
4.12.4.	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　登记结算系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
4.12.5.	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□	
4.12.6.	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□	
4.12.7.	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□	
4.12.8.	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□	
4.12.9.	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□	
4.12.10.	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□	
4.12.11.	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□	

表 G.2　登记结算系统审计底稿（续）

序号	审计项	审计程序	审计结论	备注
4.12.12.	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□	
4.12.13.	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□	
4.12.14.	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□	
4.12.15.	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□	
4.12.16.	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□	
4.13.	**系统托管**			
4.13.1	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三级系统托管服务。	是□ 否□ 不适用□	
4.13.2	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+系统托管服务。	是□ 否□ 不适用□	
4.13.3	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）
重要信息系统审计底稿

表H.1至表H.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H.1 重要信息系统审计底稿

被审计部门：	索引号：ZYXT
审计主题：重要系统	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　重要信息系统审计底稿（续）

审计证据列表：

表H.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.	**数据库管理**			
1.1.	**身份鉴别**			
1.1.1.	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□	
1.1.2.	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□	
1.1.3.	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□	
1.1.4.	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□	
1.1.5.	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□	
1.2.	**安全审计**			
1.2.1.	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□	
1.2.2.	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□	
1.2.3.	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□	

表 H.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
1.2.4.	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□	
1.2.5.	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□	
1.2.6.	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□	
1.3.	**数据库运维**			
1.3.1.	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□	
1.3.2.	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□	
1.3.3.	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□	
1.3.4.	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□	

表 H.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
1.3.5.	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□	
2.	**网上信息系统**			
2.1.	**数据安全**			
2.1.1.	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 L.5-身份认证方式”、“表 L.5-软件数字证书建设和管理情况”，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□	
2.1.2.	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□	
2.2.	**系统运维**			
2.2.1.	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 L.5-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□	
2.3.	**门户网站**			
2.3.1.	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 L.5-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□	
2.3.2.	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□	
2.3.3.	是否对网站内容进行 24 小时实时监控。	检查“表 L.5-系统监控情况-门户网站”，审阅门户网站情况说明，是否对网站内容进行 24 小时实时监控。	是□ 否□ 不适用□	
3.	**主机管理**			
3.1.	**身份鉴别**			
3.1.1.	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□	

表 H.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
3.1.2.	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□	
3.1.3.	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□	
3.1.4.	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□	
3.1.5.	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□	
3.1.6.	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 L.11 附表一-信息系统名称”、“表 L.11 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□	
3.1.7.	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□	
3.1.8.	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□	
3.1.9.	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　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
3.2.	**访问控制**			
3.2.1.	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□	
3.2.2.	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 DB5 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□	
3.2.3.	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□	
3.2.4.	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□	
3.2.5.	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□	
3.3.	**安全审计**			
3.3.1.	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　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
3.3.2.	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□	
3.3.3.	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□	
3.3.4.	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□	
3.3.5.	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□	
3.3.6.	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□	

表 H.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
3.4.	**安全管理**			
3.4.1.	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□	
3.4.2.	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 L.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□	
3.4.3.	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□	
3.4.4.	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 L.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□	

表 H.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
3.4.5.	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□	
3.4.6.	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□	
3.4.7.	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□	
3.4.8.	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□	
3.4.9.	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□	
3.5.	**资源控制**			
3.5.1.	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□	
3.5.2.	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□	
3.5.3.	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□	

表 H.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
3.6.	**主机运维**			
3.6.1.	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L.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□	
3.6.2.	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□	
4.	**系统管理**			
4.1.	**系统架构**			
4.1.1.	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□	
4.1.2.	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□	
4.2.	**系统建设**			
4.2.1.	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□	
4.2.2.	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□	

表 H.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
4.2.3.	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□	
4.2.4.	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□	
4.2.5.	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□	
4.2.6.	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□	
4.2.7.	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□	
4.2.8.	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□	
4.2.9.	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□	
4.2.10.	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□	
4.2.11.	是否制定了本机构与市场相关主体信息系统安全互联的技术规则，并报证信办备案,同时依法督促市场相关主体执行技术规则。	a)访谈信息技术负责人，询问是否制定了本机构与市场相关主体信息系统安全互联的技术规则； b)检查技术规则，查看向证信办备案的记录。	是□ 否□ 不适用□	

表 H.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
4.3.	**测试验收**			
4.3.1.	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□	
4.3.2.	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□	
4.3.3.	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□	
4.3.4.	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□	
4.3.5.	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□	
4.3.6.	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□	
4.3.7.	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 H.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
4.3.8.	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□	
4.3.9.	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 L.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□	
4.3.10.	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□	
4.3.11.	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□	
4.3.12.	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□	
4.3.13.	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□	
4.3.14.	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 H.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
4.3.15.	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□	
4.3.16.	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□	
4.3.17.	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□	
4.3.18.	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□	
4.3.19.	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□	
4.3.20.	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□	
4.3.21.	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□	
4.3.22.	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　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
4.3.23.	系统上线或变更升级前，是否对执行程序及源代码进行严格审查、测试。	a)访谈开发负责人，系统上线或变更升级前，是否对执行程序及源代码进行严格审查、测试； b)检查对执行程序及源代码的审查结果、测试报告。	是□ 否□ 不适用□	
4.4.	**系统运维**			
4.4.1.	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□	
4.4.2.	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□	
4.4.3.	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□	
4.4.4.	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□	
4.4.5.	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□	

表 H.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
4.4.6.	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□	
4.4.7.	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□	
4.4.8.	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 L.5-系统监控情况-服务器”，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□	
4.4.9.	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 L.5-系统监控情况-存储”，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□	
4.4.10.	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 L.5-系统监控情况-数据库”，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□	
4.4.11.	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 L.5-系统监控情况-信息系统”，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□	

表 H.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
4.4.12.	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□	
4.4.13.	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□	
4.4.14.	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□	
4.4.15.	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□	
4.4.16.	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□	
4.4.17.	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□	
4.4.18.	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□	
4.4.19.	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□	

表 H.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
4.4.20.	是否对系统资源的使用进行预测，以确保充足的处理速度和存储容量，管理人员应随时注意系统资源的使用情况，包括处理器、存储设备和输出设备。	a)检查系统、数据库以及网络评估报告，是否对资源的使用进行预测，以确保充足的处理速度和存储容量； b)访谈系统管理员，了解是否监控系统资源的使用情况，包括处理器、存储设备和输出设备。	是□ 否□ 不适用□	
4.5.	**变更管理**			
4.5.1.	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□	
4.5.2.	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□	
4.5.3.	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□	
4.5.4.	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□	
4.5.5.	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□	
4.5.6.	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□	

表 H.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
4.5.7.	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□	
4.5.8.	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□	
4.5.9.	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□	
4.5.10.	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□	
4.5.11.	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□	
4.5.12.	是否定期检查变更控制的申报和审批程序的执行情况，评估系统现有状况与文档记录的一致性。	抽查定期检查变更控制的申报和审批程序的执行情况记录，是否评估系统现有状况与文档记录的一致性。	是□ 否□ 不适用□	
4.5.13.	重大的系统变更升级是否组织会员进行严格的联网测试，是否制定专项的应急预案和回退方案。	检查重大系统变更的专项应急预案和回退方案、联网测试记录，是否组织会员进行严格的联网测试。	是□ 否□ 不适用□	
4.5.14.	在开展重大信息系统项目建设、迁移或改造时，是否事前向证信办进行报告，并定期报告项目进展情况。	检查项目建设报告记录，是否在开展重大信息系统项目建设、迁移或改造时，事前向证信办进行报告，并定期报告项目进展情况。	是□ 否□ 不适用□	

表 H.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
4.6.	**安全管理**			
4.6.1.	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□	
4.6.2.	是否每月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。	检查“表 L.3-该机房的网络安全检查情况”，检查是否有网络漏洞扫描报告，是否至少每月进行一次漏洞扫描，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□	
4.6.3.	实施漏洞扫描或漏洞修补前，是否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。	检查漏洞扫描和修补报告，查看扫描和修补工作是否在恰当的时间，对可能存在的风险进行充分评估和准备，制定回退方案，备份重要数据后进行的。	是□ 否□ 不适用□	
4.6.4.	漏洞扫描或漏洞修补后，是否进行验证测试，以保证系统的正常运行。	检查漏洞扫描和修补报告，查看完成扫描和修补工作后，是否进行了验证测试，以保证网络系统的正常运行。	是□ 否□ 不适用□	
4.7.	**身份鉴别**			
4.7.1.	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□	
4.7.2.	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□	

表 H.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
4.7.3.	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□	
4.7.4.	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□	
4.7.5.	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□	
4.7.6.	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□	
4.7.7.	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□	
4.7.8.	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□	
4.7.9.	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□	
4.7.10.	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□	
4.7.11.	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□	
4.7.12.	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□	

表 H.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
4.7.13.	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□	
4.8.	**访问控制**			
4.8.1.	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□	
4.8.2.	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□	
4.8.7.	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□	
4.8.4.	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□	
4.8.5.	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　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
4.8.6.	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□	
4.9.	**资源控制**			
4.9.1.	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□	
4.9.2.	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□	
4.9.3.	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□	
4.9.4.	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□	
4.9.5.	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□	
4.9.6.	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□	
4.9.7.	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　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
4.10.	**数据安全**			
4.10.1.	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□	
4.10.2.	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□	
4.10.3.	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□	
4.11.	**备份能力**			
4.11.1.	是否至少每天备份数据一次；备份介质应当在本地机房、同城及异地安全可靠存放；每周至少对数据备份进行一次有效性验证。	a)检查“表 L.5-数据备份情况”，查看数据备份记录，确认开户、交易、行情、转账、登记、存管、结算、查询和相关业务办理的数据等重重要数据每日在本地、同城、异地备份； b)查看数据有效性验证记录，确认每周对数据备份进行了一次有效性验证。	是□ 否□ 不适用□	
4.11.2.	实时信息系统灾难应对能力是否满足：信息系统恢复时间目标 RTO 小于 3 小时；信息系统恢复点目标 RPO 小于 1 分钟；备份系统具有满足业务需求的处理能力。	检查“表 L.5-系统备份能力”，查看实时信息系统灾难应对能力达标证明材料（包括：灾难备份系统建设情况、备份策略、应急演练记录等），判断实时信息系统灾难应对能力是否满足：RTO 小于 3 小时；信息系统恢复点目标 RPO 小于 1 分钟；备份系统具有满足业务需求的处理能力。	是□ 否□ 不适用□	

表 H.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
4.11.3.	非实时信息系统灾难应对能力是否满足：信息系统恢复时间目标 RTO 小于 6 小时；信息系统恢复点目标 RPO 等于 0 秒；备份系统具有满足业务需求的处理能力。	检查“表 L.5-系统备份能力”，查看非实时信息系统灾难应对能力达标证明材料（包括：灾难备份系统建设情况、备份策略、应急演练记录等），判断非实时信息系统灾难应对能力是否满足：RTO 小于 6 小时；信息系统恢复点目标 RPO 等于 0 秒；备份系统具有满足业务需求的处理能力。	是□ 否□ 不适用□	
4.11.4.	实时信息系统故障应对能力是否满足：信息系统恢复时间目标 RTO 小于 3 分钟；信息系统恢复点目标 RPO 小于 30 秒；备份系统具有满足业务需求的处理能力。	检查“表 L.5-系统备份能力”，查看实时信息系统故障应对能力达标证明材料（包括：灾难备份系统建设情况、备份策略、应急演练记录等），判断实时信息系统故障应对能力是否满足：RTO 小于 3 分钟；信息系统恢复点目标 RPO 小于 30 秒；备份系统具有满足业务需求的处理能力。	是□ 否□ 不适用□	
4.11.5.	非实时信息系统故障应对能力是否满足：信息系统恢复时间目标 RTO 小于 1 小时；信息系统恢复点目标 RPO 等于 0 秒；备份系统具有满足业务需求的处理能力。	检查“表 L.5-系统备份能力”，查看非实时信息系统故障应对能力达标证明材料（包括：灾难备份系统建设情况、备份策略、应急演练记录等），判断非实时信息系统故障应对能力是否满足：RTO 小于 1 小时；信息系统恢复点目标 RPO 等于 0 秒；备份系统具有满足业务需求的处理能力。	是□ 否□ 不适用□	
4.11.6.	实时信息系统重大灾难应对能力是否满足：信息系统恢复时间 RTO 小于 3 天；信息系统恢复点目标 RPO 小于 5 分钟；备份系统具有满足业务需求的处理能力。	检查“表 L.5-系统备份能力”，查看实时信息系统重大灾难应对能力达标证明材料（包括：灾难备份系统建设情况、备份策略、应急演练记录等），判断实时信息系统重大灾难应对能力是否满足：信息系统恢复时间 RTO 小于 3 天；信息系统恢复点目标 RPO 小于 5 分钟；备份系统具有满足业务需求的处理能力。	是□ 否□ 不适用□	
4.11.7.	非实时信息系统重大灾难应对能力是否满足：信息系统恢复时间目标 RTO 小于 3 天；信息系统恢复点目标 RPO 等于 0 秒；备份系统具有满足业务需求的处理能力。	检查“表 L.5-系统备份能力”，查看非实时信息系统重大灾难应对能力达标证明材料（包括：灾难备份系统建设情况、备份策略、应急演练记录等），判断非实时信息系统重大灾难应对能力是否满足：信息系统恢复时间目标 RTO 小于 3 天；信息系统恢复点目标 RPO 等于 0 秒；备份系统具有满足业务需求的处理能力。	是□ 否□ 不适用□	

表 H.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
4.11.8.	重要业务数据、执行程序和源代码是否同时备份到同城和异地的安全地点。	检查“表 L.5-数据备份情况”，查看备份记录，开户、交易、行情、转账、登记、存管、结算、查询和相关业务办理的数据、执行程序和源代码是否每日备份到同城和异地的安全地点。	是□ 否□ 不适用□	
4.11.9.	在主用设备故障时，是否能切换到备份系统，自动隔离并保留故障设备以备事后调查。	a)检查应急演练报告中主备实时切换方法，及切换演练记录； b)检查操作记录，主备实时切换后，是否自动隔离并保留故障设备以备事后调查。	是□ 否□ 不适用□	
4.11.10.	交易、结算、开户等关键业务系统的同城和异地灾备系统处理能力是否与主系统能力相同。	检查“表 L.5-备份系统处理能力”，检查同城及异地灾备系统处理能力报告和压力测试报告,比对交易、结算、开户等关键业务系统同城和异地灾备系统与主系统的处理能力指标，判断三者能力是否相同。	是□ 否□ 不适用□	
4.11.11.	备份中心是否能够同时支持会员单位备份系统的接入。	检查备份中心网络通信情况说明，是否能够支持会员单位备份系统的接入。	是□ 否□ 不适用□	
4.12.	**安全审计**			
4.12.1.	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□	
4.12.2.	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□	

表 H.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
4.12.3.	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□	
4.12.4.	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□	
4.12.5.	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□	
4.12.6.	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□	
4.12.7.	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□	
4.12.8.	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□	
4.12.9.	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□	
4.12.10.	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　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
4.12.11.	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□	
4.12.12.	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□	
4.12.13.	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□	
4.12.14.	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□	
4.12.15.	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□	
4.12.16.	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□	

表 H.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
4.13	**系统托管**			
4.13.1	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三级系统托管服务。	是□ 否□ 不适用□	
4.13.2	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+系统托管服务。	是□ 否□ 不适用□	
4.13.3	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）
信息系统建设合规审计底稿

表I.1至表I.2给出了信息系统建设合规审计的程序、内容及相关记录要求。

表I.1 信息系统建设合规审计底稿

被审计部门：	索引号：HGSJ
审计主题：合规审计	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 I.1　信息系统建设合规审计底稿（续）

审计证据列表：

表I.2　信息系统建设合规审计底稿

序号	审计项	审计程序	审计结论	备注
1	**需求论证**			
1.1	**需求分析**			
1.1.1	是否有项目需求说明书,应包括项目需求分析、功能和性能要求等。	a)检查是否有需求说明书等，应有立项依据、业务处理能力、计算能力等方面的说明； b)检查需求说明书是否有审批，比如会议纪要、电子化留痕、负责人签字等。	是□ 否□ 不适用□	
1.1.2	是否有项目计划书,应包括经费预算、项目目标、项目进度、风险评估等	a)检查是否有项目计划书等，应包括项目经费预算、项目目标、项目进度、风险评估等； b)检查项目计划书是否有审批，比如会议纪要、电子化留痕、负责人签字等。	是□ 否□ 不适用□	
1.2	**可行性论证**			
1.2.1	技术报告是否有性能功能指标、交付物、项目进度计划、后期维护等可衡量的预期指标。	a)检查是否有可行性技术报告，应包括性能功能指标、交付物、项目进度计划、后期维护等可衡量的预期指标等可衡量的预期指标； b)检查可行性技术报告是否有审批，比如会议纪要、电子化留痕、负责人签字等。	是□ 否□ 不适用□	
1.2.2	项目目标是否与现有需求相匹配。	检查可行性技术报告与需求说明书的项目需求、功能和性能相匹配的评审和审批，比如第三方评估报告、会议纪要、负责人签字或电子化留痕等。	是□ 否□ 不适用□	
1.2.3	项目依据是否符合监管要求，或符合组织业务和技术发展目标及原则。	检查可行性分析报告是否有符合监管要求的说明（合规性分析），或符合组织业务和技术发展目标及原则的说明（必要性分析）。	是□ 否□ 不适用□	
1.2.4	可行性分析是否已充分考虑复用现有资源的可能性。	检查可行性分析报告是否包括复用现有软硬件设备、基础设施等的分析。	是□ 否□ 不适用□	
2	**预算制定**			
2.1	**预算编制**			
2.1.1	预算方案是否根据相关法律法规及企业章程、以及上级单位的有关要求报经审议批准。	a)检查财务或预算管理制度是否包括预算编制的审批流程； b)检查预算编制方案按有关规定的审批记录，比如会议纪要、电子化留痕、负责人签字等。	是□ 否□ 不适用□	

表I.2 信息系统建设合规审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.1.2	是否有预算评审的机构或机制。	a)检查财务或预算管理制度是否包括预算评审机构的设置及人员构成； b)检查财务或预算管理制度是否有预算评审机制。	是□ 否□ 不适用□	
2.1.3	相关预算资料是否完整且归档，相关资料应包括会议纪要、预算申报表等。	检查归档的预算资料是否完整，是否包括预算申报表、审批记录（或会议纪要）等。	是□ 否□ 不适用□	
2.2	**预算调整**			
2.2.1	预算管理是否明确预算调整原则和条件。	检查预算管理制度是否包括预算调整的原则、条件。	是□ 否□ 不适用□	
2.2.2	是否有论述预算调整合理性的书面材料。	a)查看预算调整申报材料，检查关于预算调整的说明； b)检查预算调整申报材料是否有审批记录，比如会议纪要、负责人签字或电子化留痕等。	是□ 否□ 不适用□	
2.2.3	预算管理是否建立预算调整审批程序和流程。	检查预算管理制度是否包括预算调整审批程序和流程	是□ 否□ 不适用□	
2.2.4	预算管理相关预算资料是否完整且归档,相关材料应包括会议纪要、审批记录等。	检查归档的预算调整相关资料是否包括预算调整申报材料、审批记录（或会议纪要）等。	是□ 否□ 不适用□	
2.3	**预算执行**			
2.3.1	预算管理是否建立预算审批程序和流程。	检查预算管理制度是否包括预算执行审批程序和流程	是□ 否□ 不适用□	
2.3.2	预算管理是否建立IT 重大预算项目特别关注制度,例如季报、半年报等。	a)检查预算管理制度是否包括 IT 重大预算项目特别关注制度； b)检查 IT 重大预算项目的季报、半年报等是否包括项目进度、款项拨付等情况。	是□ 否□ 不适用□	
2.3.3	会议纪要、审批记录等相关资料是否完整且归档。	检查归档的相关资料是否完整，是否包括审批记录（或会议纪要）等。	是□ 否□ 不适用□	
3	**项目立项**			
3.1	**立项机构**			
3.1.1	项目管理是否有项目审核小组或委员会。	a)检查项目管理制度是否有关于设立项目立项审核小组或委员会的规定； b)检查项目是否有审核小组或委员会。	是□ 否□ 不适用□	

表 I.2　信息系统建设合规审计底稿（续）

序号	审计项	审计程序	审计结论	备注
3.1.2	项目管理审核小组或委员会成员是否3 人以上（含）。	a)检查项目管理制度是否要求项目管理审核小组或委员会成员是否 3 人以上（含）； b)检查项目立项审核小组或委员会成员是否3人以上（含）。	是□ 否□ 不适用□	
3.1.3	项目管理审核小组或委员会成员是否来自无利害关系部门。	a)检查项目管理制度是否要求项目立项审核小组或委员会的成员符合不相容职务分离控制； b)检查项目立项审核小组或委员会会议纪要，查看审核小组或委员会成员的签名，确认项目立项审核小组或委员会成员符合不相容职务分离控制。	是□ 否□ 不适用□	
3.1.4	项目管理审核小组或委员会成员是否实行任期制。	检查项目管理制度是否要求项目立项审核小组或委员会的成员实行合理的流动机制。	是□ 否□ 不适用□	
3.1.5	项目管理是否建立审核小组或委员会专家库,从专家库中挑选审核委员。	a)检查项目管理制度是否包括项目立项审核小组或委员会专家库的设置、使用及人员构成； b)检查项目立项审核小组或委员会会议纪要，查看审核小组或委员会成员的签名，判断是否在审核小组或委员会专家库中。	是□ 否□ 不适用□	
3.1.6	项目管理审核小组或委员会是否采用投票、打分等决策机制。	a)检查项目管理制度是否包括项目立项审核小组或委员会采用投票、打分等进行决策的机制； b)检查项目立项审核小组或委员会会议纪要，查看记录的投票结果和打分成绩。	是□ 否□ 不适用□	
3.2	立项审批			
3.2.1	项目管理是否有完整有效的项目立项报告。	检查项目立项报告是否包括需求分析、项目论证、项目预算等。	是□ 否□ 不适用□	
3.2.2	项目管理是否有立项审核小组委员会会议纪要或审批结果。	检查是否有项目立项审核小组或委员会会议纪要或审批记录。	是□ 否□ 不适用□	
3.2.3	项目管理会议纪要、审批结果是否由参与审批的全体成员签字。	a)检查会议纪要、审批记录表是否由参与审批的全体成员签字； b)检查参会人员是否来自审核小组或委员会、审核小组或委员会专家库。	是□ 否□ 不适用□	
3.2.4	是否对需求分析、可行性论证、预算编制进行了审查。	检查会议纪要是否包括对需求分析、可行性论证、预算编制的评审意见和评审结果。	是□ 否□ 不适用□	

表 I.2　系统建设合规审计底稿（续）

序号	审计项	审计程序	审计结论	备注
4	**项目采购**			
4.1	**采购申请**			
4.1.1	采购申请表和专项采购相关请示是否按相关规定报批后实施。	a)检查采购管理制度是否包括采购审批流程； b)检查采购审批记录，确定采购申请表和专项采购相关请示按相关规定报批后实施。	是□ 否□ 不适用□	
4.1.2	对同一需求进行分批采购是否提供需求说明。	a)检查采购管理制度是否包括对项目进行非一次性采购的情况，需要提供必要说明的要求； b)检查对项目进行非一次性采购的说明。	是□ 否□ 不适用□	
4.2	**采购程序**			
4.2.1	IT项目采购是否有严格的采购程序，比如有合理的审批流程等。	a)检查采购管理制度是否包括项目采购计划流程、供应商选择流程、采购审批流程等； b)对供应商选择方案进行审阅，包括大额采购招标的工作报告等； c)对采购审批记录进行审阅。	是□ 否□ 不适用□	
4.3	**职责分工**			
4.3.1	是否明确IT项目采购的职责分工。	a)检查采购管理制度是否明确项目采购的职责分工； b)检查项目采购记录，判断是否按照采购管理制度执行采购。	是□ 否□ 不适用□	
4.4	**产品列表**			
4.4.1	是否有可选产品列表。	检查可选产品列表。	是□ 否□ 不适用□	
4.5	**计划制定与审批**			
4.5.1	是否明确、及时、合理制定IT项目采购计划，计划中应包含采购方式、采购时间等内容。	检查项目采购计划是否包括项目信息、采购方式、采购时间等内容。	是□ 否□ 不适用□	
4.5.2	采购计划是否由职能委员会审议通过并形成了会议纪要，会议纪要应由全体参会委员签字。	a)检查采购计划是否由职能委员会审议通过并形成了会议纪要； b)检查采购计划是否由职能委员会全体委员签字。	是□ 否□ 不适用□	
4.6	**询价采购**			
4.6.1	在实际采购阶段是否采用合理方式产生实际采购价格，并有询价过程记录。询价记录应包括厂商出具的书面报价等。	a)检查采购管理制度是否有实际采购价格产生方式的规定； b)检查询价记录是否包括厂商出具的正式报价、询价过程记录、第三方价格信息等。	是□ 否□ 不适用□	

表 I.2 信息系统建设合规审计底稿（续）

序号	审计项	审计程序	审计结论	备注
4.7	**单一品牌或单一来源采购**			
4.7.1	项目是否对单一品牌或单一来源采购有书面说明材料。	a)检查采购管理制度是否要求单一品牌或单一来源采购有书面说明材料； b)检查单一品牌或单一来源采购的书面说明材料。	是□ 否□ 不适用□	
4.8	**采购验收**			
4.8.1	是否对产品验收进行签字留痕确认和复核。	a)检查采购管理制度是否包含验收程序及对各参与执行部门及职责的明确规定等； b)检查验收记录表是否有对产品验收的签字和复核； c)检查入库单是否与验收记录相符合。	是□ 否□ 不适用□	
4.9	**采购归档**			
4.9.1	项目采购相关文档和凭据是否归档。	检查归档的资料是否包括采购计划、会议纪要、供应商出具的报价表、采购询价记录、单一品牌或单一来源采购的书面说明材料、验收记录表、入库单等。	是□ 否□ 不适用□	
5	**项目招标**			
5.1	**招标制度**			
5.1.1	项目是否有使用人、招标人、审批人职责分离的制度,其中使用人只负责需求、配置及初步询 价;招标人应为专门工作小组或委员会,负责招标采购及谈判；审批人员不参与采购。	检查招标管理制度是否规定了使用人、招标人、审批人职责分离，其中使用人只负责需求、配置及初步询价；招标人应为专门工作小组或委员会，负责招标采购；审批人员不参与采购。	是□ 否□ 不适用□	
5.1.2	标书制定及审批是否合规,标书中是否明确评标标准或打分标准；审批流程是否完善，审批流 程中应确定招标公告发布渠道及时间。	a)检查招标管理制度是否符合《中华人民共和国招标投标法》及有关规定，是否有关于招标文件制定和审批流程的规定； b)检查招标文件制定和审批是否按照招标管理制度实施； c)检查招标文件是否明确评标标准和方法。	是□ 否□ 不适用□	
5.1.3	项目审批人员构成是否合理，是否履职尽责。	a)检查招标管理制度是否规定项目审批人员构成； b)检查审批人员是否符合项目审批人员构成规定； c)检查审批记录是否有审批人员的签字。	是□ 否□ 不适用□	

表 I.2　信息系统建设合规审计底稿（续）

序号	审计项	审计程序	审计结论	备注
5.2	**招标公告**			
5.2.1	项目是否在规定时间段在指定媒体等公开渠道发布招标公告。	检查招标公告，判断项目是否在规定时间段在指定媒体等公开渠道发布招标公告	是□ 否□ 不适用□	
5.3	**发送招标邀请**			
5.3.1	投标人的资质是否符合标书要求。	a)检查招标文件、投标文件，投标人的资质是否符合招标文件要求； b)检查投标人资质审核记录，是否按照招标要求规定进行检查。	是□ 否□ 不适用□	
5.3.2	项目是否进行市场询价。	检查采购询价记录，判断项目是否进行市场询价过程。	是□ 否□ 不适用□	
5.4	**委托代理机构招标**			
5.4.1	是否有代理机构选择程序。	a)检查采购管理规定是否有招标代理机构选择程序，对招标代理机构的资质是否有要求； b)检查是否按照招标代理机构选择程序执行。	是□ 否□ 不适用□	
5.4.2	代理机构是否有相关资质。	检查代理机构资质证书，判断代理机构是否有委托招标项目所要求的资质。	是□ 否□ 不适用□	
5.4.3	选择的代理机构是否经过项目管理委员会审批。	检查代理机构资质证书，判断代理机构是否有委托招标项目所要求的资质。	是□ 否□ 不适用□	
5.5	**开标、评标、中标现场流程（委托招标除外）**			
5.5.1	开标、评标、中标现场流程是否符合《中华人民共和国招标投标法》等法律法规。	a)检查开标、评标流程是否符合《中华人民共和国招标投标法实施条例》等法律法规的规定； b)检查相关开标、评标的记录。	是□ 否□ 不适用□	
5.5.2	评标委员会人员构成是否合理。	a)检查采购管理规定是否有关于评标委员会人员构成的规定； b)检查评标记录，判断评标委员会人员构成是否符合规定。	是□ 否□ 不适用□	
5.5.3	是否采取相关保密措施，缩小知悉范围。	检查是否按照制度规定执行保密措施，如签署评标专家承诺书等。	是□ 否□ 不适用□	

表 I.2　信息系统建设合规审计底稿（续）

序号	审计项	审计程序	审计结论	备注
5.6	**中标公示**			
5.6.1	是否在规定时间段在指定媒体等公开渠道发布中标公示。	a)检查采购管理规定是否有对中标通知的规定； b)检查是否向中标人发出中标通知书，并同时将中标结果通知所有未中标的投标人。	是□ 否□ 不适用□	
6	**商务谈判**			
6.1	**谈判人员**			
6.1.1	是否由专门工作小组或委员会负责商务谈判。	检查采购管理规定是否包括成立专门工作小组或委员会的要求。	是□ 否□ 不适用□	
6.1.2	项目是否有谈判人员名单及其职责说明。	a)检查采购管理规定是否有谈判小组成员构成及职责说明。 b)检查谈判小组人员名单是否符合谈判小组人员构成的规定。	是□ 否□ 不适用□	
6.1.3	项目是否有谈判人员签字的相关记录。	检查会议纪要和谈判小组人员名单，确认是否有谈判人员签字的谈判记录。	是□ 否□ 不适用□	
6.2	**谈判内容**			
6.2.1	项目谈判前是否有明确谈判程序、谈判内容、合同草案条款，并经法律、财务等部门一致通过的记 录。	a)检查采购管理规定是否有需要在谈判前制定谈判程序、谈判内容的规定； b)检查合同草案条款，确定谈判前是否有合同草案条款。	是□ 否□ 不适用□	
6.3	**谈判过程**			
6.3.1	项目是否有标书、情况说明等相关书面材料。	检查谈判材料是否包含标书、合同草案、供应商报价明细等文档。	是□ 否□ 不适用□	
6.3.2	如有低于标书要求项，是否有相关书面材料。	检查是否有低于标书要求项的相关情况说明材料。	是□ 否□ 不适用□	
6.4	**结果记录**			
6.4.1	项目是否有谈判纪要等相关记录，并由全体谈判人员签字。	a)检查谈判纪要是否由全体谈判人员签字； b)检查谈判纪要，谈判小组是否从质量和服务均能满足采购文件实质性响应要求的供应商中，按照最后报价由低到高的顺序提出3名以上成交候选人。	是□ 否□ 不适用□	

表 I.2 信息系统建设合规审计底稿（续）

7	**供应商管理**			
7.1	**供应商列表建立**			
7.1.1	是否制定供应商列表管理制度。	检查是否制定了供应商管理的相关制度。	是□ 否□ 不适用□	
7.1.2	可选供应商的相关材料是否齐备。	按照供应商管理相关规定，检查相关材料是否齐备。	是□ 否□ 不适用□	
7.1.3	可选供应商数量是否达到一定规模。	a)检查供应商管理相关规定是否对供应商的数量进行了要求； b)检查可选供应商列表是否按照供应商管理相关规定，数量达到一定规模。	是□ 否□ 不适用□	
7.2	**供应商列表调整**			
7.2.1	是否有供应商列表调整策略。	检查供应商管理相关制度是否有合格供应商列表调整策略。	是□ 否□ 不适用□	
7.2.2	是否定期要求供应商提供相关资质，在工商管理网站上进行验证。	a)检查供应商管理相关规定是否定期要求供应商提供相关资质。 b)检查在工商局网站对供应商相关资质进行验证的记录。	是□ 否□ 不适用□	
7.2.3	是否制定供应商评价方法，并定期评估供应商的专业能力和服务水平。	a)检查供应商管理相关规定是否制定供应商定期评价方法。 b)检查评估记录，判断是否按规定定期评估供应商的专业能力和服务水平。	是□ 否□ 不适用□	
8	**合同管理**			
8.1	**合同制度体系**			
8.1.1	是否有合同管理制度、流程。	检查合同管理办法是否有合同管理制度、流程。	是□ 否□ 不适用□	
8.1.2	管理制度及流程是否覆盖了合同准备、签订、执行、变更、终止等各个生命周期的重要阶段。	检查合同管理办法是否覆盖了合同准备、签订、执行、变更、监督等各生命周期的重要阶段。	是□ 否□ 不适用□	
8.2	**合同合规性**			
8.2.1	是否按照制度规定，有财务、法律等部门审核通过的记录。	检查合同条款是否有财务、法律等部门审核通过的记录。	是□ 否□ 不适用□	

表 I.2　信息系统建设合规审计底稿（续）

序号	审计项	审计程序	审计结论	备注
8.3	**合同签订前**			
8.3.1	合同协商过程是否有完整的记录，例如：经双方认可的会议纪要、录音、录像、邮件等材料。	检查经双方认可的会议纪要、录音、录像、邮件等材料，判断合同协商过程记录是否完整。	是□ 否□ 不适用□	
8.3.2	合同制度中是否具有防范被篡改的控制机制。	检查合同管理办法是否具有防范被篡改的控制机制，如合同复核机制，骑缝章等。	是□ 否□ 不适用□	
8.4	**合同履行**			
8.4.1	是否有项目合同履约情况定期检查机制。	a)检查是否有合同履约情况定期检查机制。 b)审阅合同履约情况定期检查记录。	是□ 否□ 不适用□	
8.4.2	是否有保密协议签订内容。	检查合同是否有保密条款。	是□ 否□ 不适用□	
8.4.3	是否有安全手段进行敏感信息保护。	检查记录、日志等，判断是否采用人员陪同、监控等安全手段进行敏感信息保护。	是□ 否□ 不适用□	
9	**项目验收**			
9.1	**成立验收小组**			
9.1.1	验收小组和招标小组成员是否相同。	检查采购小组名单、验收小组名单，判断采购小组成员和验收小组成员是否不完全相同。	是□ 否□ 不适用□	
9.1.2	验收小组是否签名廉洁承诺书。	检查验收小组成员是否签署廉洁承诺书。	是□ 否□ 不适用□	
9.2	**验收过程**			
9.2.1	合同是否有相关具体指标，且与验收表单一致。	检查合同、测试验收报告是否有相关具体指标，验收结果是否达到合同要求。	是□ 否□ 不适用□	
9.2.2	相关测试报告是否齐备，测试报告应包括功能、性能和压力测试等。	根据合同约定，检查测试验收报告是否包括功能、性能、压力测试等。	是□ 否□ 不适用□	
9.2.3	是否有合同变更记录和验收记录。	a)检查合同是否有完整的变更记录； b)检查验收报告与变更后合同是否相符。	是□ 否□ 不适用□	

表 I.2　信息系统建设合规审计底稿（续）

序号	审计项	审计程序	审计结论	备注
9.4	**系统上线**			
9.4.1	系统上线是否经过合理审批流程。	a)检查是否有关于系统上线审批流程的规定； b)检查是否按照制度规定执行系统上线审批流程。	是□ 否□ 不适用□	
9.4.2	信息系统项目开发技术文档是否保存完整。	检查归档的技术文档是否完整，包括项目需求说明书、项目计划书、设计开发文档等。	是□ 否□ 不适用□	
10	**钱款支付**			
10.1	**支付条件**			
10.1.1	项目费用是否有合同支付记录及相关审批手续。	a)检查项目费用支付是否有制度流程； b)检查合同支付审批记录是否符合支付制度流程的规定。	是□ 否□ 不适用□	

附 录 J
（规范性附录）
信息系统应用绩效审计底稿

表J.1至表J.2给出了信息系统应用绩效审计的程序、内容及相关记录要求。

表J.1 信息系统应用绩效审计底稿

被审计部门：	索引号：JXSJ
审计主题：绩效审计	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 J.1　系统应用绩效审计底稿（续）

审计证据列表：

表J.2　信息系统应用绩效审计底稿

序号	审计项	审计程序	审计结论	备注
1	**系统建设**			
1.1	**项目提出**			
1.1.1	项目建设目标、建设内容是否明确。	a)检查项目计划书或建设方案是否包括项目背景即开展本项目的原因； b)检查项目计划书或建设方案是否包括项目概述即项目的名称及其核心内容； c)检查项目计划书或建设方案是否包括项目目标即项目要解决的问题和要达到的效果。	是□ 否□ 不适用□	
1.1.2	项目的设立是否符合相关的政策、文件要求。	a)检查项目相关材料是否包括项目合规性分析即是否符合监管要求； b)检查项目相关材料是否包括项目实施的必要性分析，即项目实施对完成业务任务或促进发展的意义与作用。	是□ 否□ 不适用□	
1.2	**项目验收**			
1.2.1	目标完成率（实际完成的功能模块数/预定完成的功能模块数×100%）是否符合预期。	a)检查测试验收报告，根据报告计算目标完成率(实际完成的任务数或功能模块数/预定完成的任务数或功能模块数×100%)； b)对照业务需求说明书,目标完成率是否符合预期。	是□ 否□ 不适用□	
1.2.2	根据项目的监理报告或第三方评测报告，建设项目总体质量是否符合预期。	检查项目监理报告、第三方评测报告或项目验收报告，对照业务需求说明书判断建设项目总体质量是否符合预期。	是□ 否□ 不适用□	
1.2.3	建设项目是否如期完成上线。	检查项目计划书、项目验收报告、上线申请单或启用报告比较计划上线或启用时间和实际上线或启用时间是否一致。	是□ 否□ 不适用□	
1.2.4	建设项目如果没有如期上线，是否有合理的理由。	检查项目总结报告是否有项目未如期上线的合理理由。	是□ 否□ 不适用□	
1.2.5	预算的建设资金与实际的建设资金的差距是否合理。	核对预决算文档和付款记录，分析预算的建设资金与实际的建设资金的差距是否有充分理由。	是□ 否□ 不适用□	
1.2.6	预算的建设资金与实际的建设资金如果有较大差距，是否有合理的理由。	核对合同、项目阶段性总结报告或项目结项报告、项目计划书，分析预算的建设资金与实际的建设资金的差距是否有合理理由，并经相关审批。	是□ 否□ 不适用□	
1.2.7	预算的运营资金与实际的运营资金的差距是否合理。	核对维保合同、项目运营报告年度维保立项、项目计划书或项目立项报告预算的运营资金与实际的运营资金的差距是否合理。	是□ 否□ 不适用□	

表J.2 信息系统应用绩效审计底稿（续）

序号	审计项	审计程序	审计结论	备注
1.2.8	预算的运营资金与实际的运营资金如果有较大差距，是否有合理的理由。	核对维保合同、项目运营报告年度维保立项、项目计划书或项目立项报告预算的运营资金与实际的运营资金的差距是否合理，并经相关审批	是□ 否□ 不适用□	
1.3	**系统性能**			
1.3.1	系统故障时长（即一年内系统不能正常工作的时间）是否符合设计目标。	a)检查系统设计或建设报告中有无连续性指标； b)查阅运行记录或运行故障报告； c)是否有持续优化计划。	是□ 否□ 不适用□	
1.3.2	系统故障恢复时间（即系统发生故障后，经多长时间才能恢复系统的正常运转）是否合理。	a)提供故障中断及恢复时间； b)系统故障恢复时间是否满足行业规定。；	是□ 否□ 不适用□	
1.3.3	系统、设备实际使用时长是否合理。	a)提供设备上线或启用时间； b)对比设备管理办法或资产管理办法与设备实际使用时长。	是□ 否□ 不适用□	
1.3.4	系统实际处理能力与最大处理能力比值是否合理。	a)历史峰值与系统设计最大处理能力对比； b)经验证的系统最大处理能力与系统设计最大处理能力对比。	是□ 否□ 不适用□	
1.3.5	系统是否能快速扩展。	检查系统测试报告，判断系统是否可以根据业务需求升级或扩容。	是□ 否□ 不适用□	
1.3.6	网络带宽利用率每交易日峰值按月统计的平均值是否不超过 80%。	通过网络监控系统检查网络带宽利用率每交易日峰值按月统计的平均值是否不超过80%。	是□ 否□ 不适用□	
1.3.7	是否提高了数据共享水平。	访谈技术、业务主岗人员了解数据共享情况	是□ 否□ 不适用□	
2	**经济效益**			
2.1	**有形经济效益**			
2.1.1	项目完成产生的经济效益是否与立项报告的预期一致。	检查项目运营报告、可行性分析报告对比项目完成产生的经济收入是否符合设计目标。	是□ 否□ 不适用□	
2.2	**无形经济效益**			
2.2.1	项目建成后，组织机构是否得到优化调整。	检查项目运营报告或年度总结,项目建成后，组织机构是否得到优化调整。	是□ 否□ 不适用□	

表 J.2　信息系统应用绩效审计底稿（续）

序号	审计项	审计程序	审计结论	备注
2.2.2	项目建成后，业务处理流程和业务功能是否得到改善，包括冗余流程的删除和精简等。	对管理人员访谈项目建成后，业务处理流程和业务功能是否得到改善，包括冗余流程的删除和精简等。	是□ 否□ 不适用□	
2.2.3	项目建成后，是否提高了办事效率。	a)对管理人员及业务人员访谈是否项目建成后提高了办事效率； b)检查项目总结评价是否有相关数据说明。	是□ 否□ 不适用□	
2.2.4	是否达到国内或行业先进水平。	a)检查项目运营报告或第三方检验报告判断是否达到国家或行业先进水平； b)是否有相关奖励证书。	是□ 否□ 不适用□	
3	**用户满意度**			
3.1	**满意度调查**			
3.1.1	项目建成后，业务人员对系统功能、性能、可用性等是否认可。	对业务人员访谈或者查阅满意度调查表，业务人员对系统功能、性能、可用性等是否认可	是□ 否□ 不适用□	
3.1.2	项目建成后，IT 人员对系统功能、性能、可用性等是否认可。	对业务人员访谈或查阅满意度调查表，建成后 IT 及业务人员对系统功能、性能、可用性等是否认可	是□ 否□ 不适用□	
3.1.3	项目建成后，外部机构对系统功能、性能、可用性等是否认可。	对业务人员访谈或进行问卷调查项目建成后外部机构对系统功能、性对能、可用性等是否认可。	是□ 否□ 不适用□	
3.1.4	是否按用户的要求提供了相关的服务。	对业务人员访谈或进行问卷调查是否按用户的要求提供了相关的服务。	是□ 否□ 不适用□	
3.2	**投诉情况**			
3.2.1	是否有关于系统功能的投诉。	检查投诉记录是否未收到关于系统功能的投诉。	是□ 否□ 不适用□	
3.2.2	是否有关于系统性能的投诉。	检查投诉记录是否未收到关于系统性能的投诉。	是□ 否□ 不适用□	
3.3	**问题与事件管理**			
3.3.1	所有事件报告、服务请求和相关需求是否能得到及时处理。	a)查阅相关服务请求及需求是否有记录； b)所有事件处置报告、服务请求和相关需求的及时处理时间是否有制度流程规定； c)事件、服务请求、需求的及时响应率； d)事件、服务请求、需求的成功解决率。	是□ 否□ 不适用□	

表 J.2　信息系统应用绩效审计底稿（续）

序号	审计项	审计程序	审计结论	备注
3.3.2	是否可以有效避免重复问题的发生。	a)查阅是否有问题管理流程； b)所有问题处置是否有过程记录； c)解决问题的响应率及成功率； d)检查日志是否仍有重复问题发生。	是□ 否□ 不适用□	

附 录 K
（规范性附录）
信息系统托管审计底稿

表K.1至表K.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K.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 K.1　信息系统托管审计底稿（续）

审计证据列表：

表K.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L.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L.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 K.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 L.6-卫星通信情况”、“表 L.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 K.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 L.6-卫星通信情况”、“表 L.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 L.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 K.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 K.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 K.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 K.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 L.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 L.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 K.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 L.6-卫星通信情况”、“表 L.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 L.6-卫星通信情况”、“表 L.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□	

表 K.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
2.3.2	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□	
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 K.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 K.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 K.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 L.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 L.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□	
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□	

表 K.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
3.1.11	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L.6-卫星通信情况”、“表L.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L.6-卫星通信情况”、“表L.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□	
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□	

表 K.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
3.3.3	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□	
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□	

表 K.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
3.4.1.2	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□	
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□	

表 K.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
3.4.2.4	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□	
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□	

表 K.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
3.4.3.5	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□	
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□	

表 K.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	**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□	
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□	

表 K.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
3.5.8	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□	
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□	

表 K.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
3.5.15	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□	
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□	

表 K.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
3.5.20	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□	
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 L.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□	

表 K.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
4.1.4	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 L.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 L.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 L.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□	
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□	

表 K.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
4.2	**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 L.6-卫星通信情况”、“表 L.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 L.6-卫星通信情况”、“表 L.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□	
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□	

表 K.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
4.3.3	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□	
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□	

表 K.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
4.4.1.2	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□	
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□	

表 K.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
4.4.2.4	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□	
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□	

表 K.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
4.4.3.5	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□	
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□	

表 K.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
4.5.2	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□	
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□	

表 K.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
4.6.2	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□	
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□	

表 K.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
4.6.10	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□	
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□	

表 K.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
4.6.17	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□	
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□	

表 K.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
4.6.22	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□	
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□	

表 K.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
4.6.30	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□	
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□	

表 K.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
4.6.36	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 L
（规范性附录）
信息系统调查表

表L.1至表L.10给出了信息系统调查的内容和要求

表L.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
合规审计部门的负责人（含副职）					
姓名	工作电话	手机	电子邮箱	职务	所在部门
指导和管理信息安全工作的委员会或领导小组组成人员					
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L.2　治理-经营与IT投入情况

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）							
其中:安全投入费用（万元）							

表L.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 L.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 L.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L.4　登记结算系统情况

基本情况			
信息系统全称			
所在机房名称			
登记结算系统处理能力			
压力测试日开户处理能力（万笔/日）		系统实际日开户处理能力（万笔/日）	
压力测试日证券过户处理能力（万笔/日）		系统实际日证券过户处理能力（万笔/日）	
压力测试日结算处理能力（万笔/日）		系统实际日结算处理能力（万笔/日）	
登记结算系统容量			
压力测试日委托处理容量（万笔/日）		系统实际日委托处理容量（万笔/日）	
压力测试日成交处理容量（万笔/日）		系统实际日成交处理容量（万笔/日）	
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（%）			

表 L.4　登记结算系统情况（续）

<table>
<tr><td colspan="11">系统备份能力</td></tr>
<tr><td colspan="2"></td><td colspan="3">故障应对能力</td><td colspan="3">灾难应对能力</td><td colspan="3">重大灾难应对能力</td></tr>
<tr><td colspan="2">信息系统恢复时间目标 RTO</td><td colspan="3">分钟</td><td colspan="3">小时</td><td colspan="3">天</td></tr>
<tr><td colspan="2">信息系统恢复点目标 RPO</td><td colspan="3">秒</td><td colspan="3">分钟</td><td colspan="3">小时</td></tr>
<tr><td colspan="11">数据备份情况（不同备份内容请逐一填写）</td></tr>
<tr><td>备份内容</td><td>备份方式</td><td>备份周期</td><td>备份介质</td><td>是否压缩</td><td>备份数据量（GB）</td><td>是否本地存放</td><td>同城存放地与主中心直线距离（km）</td><td>异地存放地与主中心直线距离（km）</td><td>有效性验证方式</td><td>验证周期</td></tr>
<tr><td></td><td></td><td></td><td></td><td>是□
否□</td><td></td><td>是□
否□</td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="11">软件开发情况</td></tr>
<tr><td>开发方式</td><td colspan="10">完全自主开发□　引进后自主开发□　联合开发□　外包开发□</td></tr>
<tr><td>源代码所有权</td><td colspan="4">有□　无□</td><td>源代码审查</td><td colspan="5">是□　否□</td></tr>
<tr><td>源代码保存机制</td><td colspan="10">开发商保存□　自主保存□　第三方托管□　无□</td></tr>
</table>

表 L.4　登记结算系统情况（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	
		门户网站	网页内容□ 日均访问量□	同上			
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L.5　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）			

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

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 L.5　重要信息系统情况（续）

软件开发情况							
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□						
源代码所有权	有□　无□		源代码审查	是□　否□			
源代码保存机制	开发商保存□　自主保存□　第三方托管□　无□						
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	
		门户网站（此项仅适应于门户网站审计）	网页内容□ 日均访问量□	同上			

表 L.5　重要信息系统情况（续）

门户网站防篡改措施（如有请填写）（此项仅适应于门户网站审计）			
防篡改系统品牌		防篡改系统厂商	
防篡改措施（请简述）			

身份认证方式（此项仅适应于网上业务系统审计）		
	HTTP	HTTPS
账号+静态密码	□	□
随机验证码	□	□
密码图形键盘（软键盘）	□	□
客户端电脑特征码绑定	□	□
硬件数字证书（第 1 代）	□	□
硬件数字证书（第 2 代）	□	□
软件数字证书	□	□
动态密码（口令）卡	□	□
身份认证方式	厂商	已发放数量（张/个）
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		

软件数字证书建设和管理情况（如有请填写）（此项仅适应于网上业务系统审计）				
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）
本机构自主生成□ 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 中心的分中心系统□ 无系统□		

表L.6　网络通信情况

地面通信情况			
基本情况			
	广域网	城域网（含局域网）	小计
地面线路数（条）			
带宽			

表 L.6　网络通信情况（续）

外联通信情况										
与其他交易所等市场核心机构通信情况										
1.与其他证券交易所及其下属机构的地面专线连接情况通信情况										
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	历史流量峰值	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□ 其他□		主□ 备□		DDN□ SDH□ MSTP□ ATM□ 局域网□ 裸光纤□ VPN(ADSL)□ 3G□ 电话拨号□ 其他□	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□ 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□

表 L.6　网络通信情况（续）

2.与登记结算公司（包括北京总部、上海、深圳、北京分公司）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	历史流量峰值	线路用途
1		同上		同上		同上	同上			同上
3.与其他期货交易所及期货信息技术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	历史流量峰值	线路用途
1		同上		同上		同上	同上			同上
4.与投保基金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	历史流量峰值	线路用途
1		同上		同上		同上	同上			同上
5.与证金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	历史流量峰值	线路用途
1		同上		同上		同上	同上			同上
6.与期保监控中心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	历史流量峰值	线路用途
1		同上		同上		同上	同上			同上
7.与资本市场监测中心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	历史流量峰值	线路用途
1		同上		同上		同上	同上			同上

表 L.6　网络通信情况（续）

与银行直接连接情况										
序号	通信本端	通信本端机房类型	银行名称	主备方式	运营商	连接类型	线路类型	带宽	历史流量峰值	线路用途
1		同上		同上		同上	同上			同上
与证监会、证监局监管机构地面专线连接情况（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	历史流量峰值	线路用途
1		同上		同上		同上	同上			同上
与会员单位直接连接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	历史流量峰值	线路用途
1		同上		同上		同上	同上			同上
与人民银行地面专线连接情况（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	历史流量峰值	线路用途
1		同上		同上		同上	同上			同上
与场外市场地面专线连接情况（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	历史流量峰值	线路用途
1		同上		同上		同上	同上			同上
与外汇交易中心地面专线连接情况（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	历史流量峰值	线路用途
1		同上		同上		同上	同上			同上

表 L.6　网络通信情况（续）

与境外市场地面专线连接情况（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	历史流量峰值	线路用途
1		同上		同上		同上	同上			同上
与其他金融机构地面专线连接情况（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	历史流量峰值	线路用途
1		同上		同上		同上	同上			同上
与其他外联单位地面专线连接情况（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	历史流量峰值	线路用途
1		同上		同上		同上	同上			同上
内部通信情况										
（一）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	历史流量峰值	线路用途
1		同上		同上		同上	同上			同上
（二）与本所通信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	历史流量峰值	线路用途
1		同上		同上		同上	同上			同上
（二）与本所信息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	历史流量峰值	线路用途
1		同上		同上		同上	同上			同上

表L.7　信息安全等级保护相关工作情况

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L.8　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			
是否专门针对生产系统故障开展了应急演练	是□　否□	是否对灾备系统切换进行应急演练	是□　否□
是否针对网络通信故障开展了应急演练	是□　否□	是否专门针对门户网站网页篡改开展了应急演练	是□　否□
是否专门针对病毒入侵、DDOS 攻击、渗透式攻击等开展了应急演练	是□　否□	是否专门针对网站仿冒开展了应急演练	是□　否□
是否专门针对消防等开展了应急演练	是□　否□	是否对新风、空调系统故障开展了应急演练	是□　否□
是否专门针对电力故障开展了应急演练	是□　否□		

组织市场各经营机构参加的应急演练情况		
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L.9　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 L.9　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 L.9　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L.9　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 L.9　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L.9 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 L.9　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L.10　重要信息系统商用密码使用情况

<table>
<tr><td colspan="7">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="2">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="2">是□　否□</td><td colspan="3">具有 CA 认证系统（发证）□　　具有 CA 认证系统（验证）□</td></tr>
<tr><td colspan="7">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="2"></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="2"></td></tr>
<tr><td>联系人</td><td colspan="2"></td><td>电话</td><td colspan="2"></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="2"></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="2"></td></tr>
<tr><td>专职密码安全员数量（个）</td><td colspan="5"></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>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 L.10　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 L.10　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 L.11 为表 L.10 的附表，表 L.11 需按信息系统分别填写。

表L.11　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 L.11　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 L.11　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L.12为表L.10的附表，表L.12需按密码服务系统分别填写。

表L.12　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 L.12 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）			