（一）信息技术治理

序号	审计项	审计项修订建议	审计程序	审计程序修订建议
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。	检查公司网络~~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。
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。	检查~~运维~~值班管理相关制度，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。
1.1.31		是否对其收集的用户信息严格保密，并建立健全用户信息保护制度。		a）访谈如何对关于数据管理制度中对用户信息的保护的； b）检查用于信息保护制度。
1.2 评审修订				
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；	a)访谈网络~~信息~~安全领导小组负责人，询问网络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；
2 供应商管理				
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。	检查涉及证券期货交易、行情、开户、结算等软件产品或技术服务的采购合同，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。
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。	检查外包商及外包人员服务的评估报告，确认定期对外包商及外包人员的服务质量进行了评估。

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。	检查应急预案或相关文档，确认有外包服务意外终止的应急措施。
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。		b)检查合作与沟通的会议纪要或来往函件，判断是否定期与关联单位进行合作与沟通。	b)检查合作与沟通记录：如合作备忘、会议纪要、框架协议、合同、邮件往来记录。~~的会议纪要或来往函件，判断是否定期与关联单位进行合作与沟通。~~
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；	~~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；~~ a)检查相关合同或聘书，判断是否与信息安全专业机构建立合作关系或聘请信息安全专家作为安全顾问，指导信息安全建设，参与安全规划和安全评审等；
4 经费管理				
4.3	是否落实软件采购经费，做好软件正版化工作。		b)检查软件采购经费说明，是否按照预算执行。	b)检查软件采购记录，是否落实软件正版化采购计划。~~经费说明，是否按照预算执行。~~
5.2 人员考核				
5.2.3	是否对考核结果进行记录并保存。	是否对考核结果进行记录并保存。（适用于等级保护三级系统）	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；	a)检查是否对关键岗位人员的安全审查和技能考核结果进行记录；
5.4 人员录用				

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。	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。（适用于等级保护三级系统）		
6 组织管理				
6.1 岗位设置				
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。	查阅公司的岗位职责说明书~~正式发文~~，是否设立机房管理负责人。
6.2 机构设置				
6.2.5		是否制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任。		a）访谈是否制定安全管理制度和操作规程，并查阅内容。 b）查阅网络安全负责人的任命记录，是否明确其岗位职责。

（二）机房管理

序号	审计项	审计项修订建议	审计程序	审计程序修订建议
8 机房运维				
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；	a)审阅机房管理制度或~~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；

（三）网络管理

序号	审计项	审计项修订建议	审计程序	审计程序修订建议
1 安全管理				

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。	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。（适用于等级保护三级系统）	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。	~~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。~~ a)访谈安全管理员，询问是否定期检查恶意代码库的升级情况，对截获的危险病毒或恶意代码是否及时分析处理； b)检查是否具有恶意代码检测记录、恶意代码库升级记录和分析报告； c)检查升级记录是否记录升级时间、升级版本等内容。
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。		b)检查边界和关键网络设备的安全审计记录。	b)检查边界和关键网络设备的安全日志~~审计记录~~。
3 访问控制				

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。		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）。	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)测试~~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）； d)检查是否有其他措施，防止外部网络用户连接内部网络。
4 结构安全				
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；	~~a)检查网络设计或验收文档，查看带宽设计容量；~~
6 网络运维				
6.14		是否采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月。		a）核查设备是否开启了日志记录或安全审计功能。 b）应核查是否部署了综合安全审计系统或类似功能的系统平台。 c）应核查网络日志留存是否大于6个月。

（四）运维管理

序号	审计项	审计项修订建议	审计程序	审计程序修订建议
4 日常操作				
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。	抽查~~检查~~一年内~~全部~~注册邮箱账号的审批情况。
6 数据和介质管理				

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。		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；	b)检查介质使用管理记录，查看其是否记录介质归档和查询~~使用~~等情况；
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。	a） 查看存储介质管理制度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（规定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，对保密性较高的存储介质未经批准不得自行销毁）； b)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。
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。	a)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； b)访谈资产管理员，询问是否定期对离线存储介质的完整性（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。

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。	~~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。~~（证券交易所、期货交易所、中国结算、核心机构删除）		
6.12		是否采取数据分类、重要数据备份和加密等措施。		a）应检查组织是否将数据保护纳入到安全制度中。 b）是否使用数据脱敏、数据加密、访问控制、数据销毁等技术手段与产品保护敏感信息。 c）是否通过内部信息安全手段（如堡垒机、终端安全管理、PKI 加密体系的应用等）来加强数据安全体系建设。
6.13		在中华人民共和国境内运营中收集和产生的个人信息和重要数据是否在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估。		a）访谈是否有数据向境外提供。 b）查阅向境外提供的数据是否有相应的评估机构。
6.14		收集、使用个人信息，是否遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。		查阅相关记录，是否能够说明机构在收集和使用个人信息时，被用户同意。

6.15		是否采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。在发生或者可能发生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。		a）访谈是否存在个人信息安全事件发生。 b）查阅是否制定个人信息安全事件补救措施，以及相关报告流程。
11 应急准备				
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。	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电力故障、消防、空调故障等应急预案进行演练。
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。	a）检查是否规定每年审查应急预案； b）检查应急预案审查或更新记录，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。
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。	检查应急预案评估或更新记录报告，判断是否每年至少进行一次评估。

11.44		是否通过多渠道、多手段、多方式收集网络安全信息，实时监测以下情形，并将重要监测信息报送证信办。 （1）大规模病毒爆发、大范围网络攻击； （2）台风、地震、暴雨、火灾等自然灾害； （3）行业重要信息系统上线或重大变更； （4）行业重要信息系统存在重大安全、容量或性能隐患； （5）行业重要基础设施（如：证联网、电力、通信、托管机房）遭到破坏； （6）其他适用情形。		a)访谈系统运维负责人，询问是否通过多渠道、多手段、多方式收集网络安全信息；请相关人员列举采用的渠道、手段及方式名称。 b)如有重要检测信息，检查是否有将重要监测信息报送证信办的记录。
11.45		是否对进入Ⅲ、Ⅳ级应急准备状态定义有明确条件。		检查应急预案，判断是否对进入Ⅲ、Ⅳ级应急准备状态定义有明确条件。

11.46		证信办启动行业网络安全事件Ⅰ级应急准备状态后，网络安全事件应急指挥机构及相关人员是否保持24小时通信联络畅通，加强网络安全事件监测和事态发展信息搜集工作，重点确认关键信息系统及基础设施是否受影响，组织指导信息技术支撑队伍、相关运行单位开展应急处置或准备、风险评估和控制工作，并定期将重要情况报证信办。		a）检查应急预案，Ⅰ级准备是否要求网络安全事件应急指挥机构及相关人员保持24小时通信联络畅通； b）检查应急预案，Ⅰ级准备是否要求加强网络安全事件监测和事态发展信息搜集工作，重点确认关键信息系统及基础设施是否受影响，组织指导信息技术支撑队伍、相关运行单位开展应急处置或准备、风险评估和控制工作； c）检查应急预案，Ⅰ级准备是否要求定期将重要情况报证信办，并检查相关记录文档。
11.47		证信办启动行业网络安全事件Ⅱ级应急准备状态后，网络安全事件应急指挥机构是否启动相应应急预案，组织开展应急准备工作，做好风险评估、应急准备和风险控制工作。关键岗位安排人员是否实行24小时通信联络畅通，相关人员保持通信联络畅通。		a）检查应急预案，Ⅱ级应急准备是否要求关键岗位安排人员24小时通信联络畅通，相关人员保持通信联络畅通； b）检查应急预案，Ⅱ级应急准备是否要求网络安全事件应急指挥机构启动相应应急预案，组织开展应急准备工作，做好风险评估、应急准备和风险控制工作。
11.48		是否有详细的Ⅲ、Ⅳ级应急预案。		检查应急预案，判断是否有详细的Ⅲ、Ⅳ级应急准备状态的启动条件。
11.49		应急预案是否有明确的Ⅲ、Ⅳ级应急准备状态结束条件。		检查应急预案，判断是否有明确的应急准备状态结束条件。
9 应急处置				

9.14		网络安全事件发生后，是否首先通过电话报告事件情况（受话人要做好电话记录），并随即填写《网络安全事件情况报告书》传真上报。		a)访谈系统运维负责人，询问网络安全事件发生后，本单位是否首先通过电话报告事件情况（受话人要做好电话记录），并随即填写《网络安全事件情况报告书》传真上报。 b)检查电话记录及《网络安全事件情况报告书》。
9.15		重要信息系统发生可能导致交易中断、严重缓慢，或者已经导致交易中断、严重缓慢的重大故障后，是否立即向办公厅值班室、相关业务部门和证信办报告，并每隔30分钟至少上报一次，直至信息系统恢复正常运行；如有重要情况应立即报告，且应同时向相关单位通报情况。		a)访谈系统运维负责人，询问重要信息系统发生可能导致交易中断、严重缓慢，或者已经导致交易中断、严重缓慢的重大故障后，本单位是否首先通过电话报告事件情况（受话人要做好电话记录），并随即填写《网络安全事件情况报告书》传真上报。 b)检查电话记录及《网络安全事件情况报告书》。
9.16		如发生其他技术故障，影响投资者正常业务办理，原则上30分钟内无法恢复业务正常运行的，是否立即报告办公厅值班室、相关业务部门和证信办，并每隔1小时至少上报一次，直至业务和信息系统恢复正常运行；如有重要情况应立即报告。		a)访谈系统运维负责人，询问影响投资者正常业务办理，原则上30分钟内无法恢复业务正常运行的，是否立即报告办公厅值班室、相关业务部门和证信办，并每隔1小时至少上报一次，直至业务和信息系统恢复正常运行； b)访谈系统运维负责人，询问重要情况是否立即报告办公厅值班室、相关业务部门和证信办； c)检查报告记录。

9.17		发生数据损毁或泄露的事件，是否立即报告办公厅值班室、相关业务部门和证信办，		a）访谈系统运维负责人，询问发生数据损毁或泄露的事件是否立即报告办公厅值班室、相关业务部门和证信办； b）检查报告记录。
9.18		涉及到计算机犯罪的事件，是否立即报告办公厅值班室、相关业务部门和证信办，同时应当报告当地公安网监部门。在事件解决前，如有重要情况应立即报告。		a）访谈系统运维负责人，询问涉及到计算机犯罪的事件是否立即报告办公厅值班室、相关业务部门和证信办； b）访谈系统运维负责人，在事件解决前，如有重要情况是否立即报告办公厅值班室、相关业务部门和证信办； c）检查报告记录。

9.19		集中交易系统发生故障，可能导致或已经造成交易中断或严重缓慢，是否立即报告公司住所地证监局，受影响的当事单位分支机构应当报告所在地证监局，每隔30分钟至少上报一次，直至信息系统恢复正常运行；如有重要情况应立即报告。证券公司根据受影响情况向相关证券交易场所报告，期货公司根据受影响情况向相关期货交易所报告。故障影响到登记结算业务时，同时向中国证券登记结算公司报告；影响到转融通业务时，同时向中国证券金融公司进行报告；影响到其他机构的，应及时向有关机构进行通报，报告要求同交易所。		a)访谈系统运维负责人，询问集中交易系统发生可能导致或已经造成交易中断或严重缓慢的，是否要求立即报告公司住地证监局，受影响分支机构报告所在地证监局，每隔30分钟至少上报一次，直至信息系统恢复正常运行。如有重要情况是否立即报告。 b)证券公司：访谈系统运维负责人，根据受影响情况是否向相关证券交易场所报告；故障影响到登记结算业务时，是否同时向中国证券登记结算公司报告；影响到转融通业务时，是否同时向中国证券金融公司进行报告；影响到其他机构的，是否及时向有关机构进行通报，报告要求同交易所。 c）期货公司：访谈系统运维负责人，根据受影响情况是否向相关期货交易所报告。故障影响到登记结算业务时，是否同时向中国证券登记结算公司报告；影响到转融通业务时，是否同时向中国证券金融公司进行报告；影响到其他机构的，是否及时向有关机构进行通报，报告要求同交易所。 d)检查报告记录。

9.20		证券期货经营机构总部的其他信息系统（包括但不限于网上交易系统，银证、银期、银基系统，融资融券系统）、证券期货投资咨询机构的信息系统发生网络安全事件，影响投资者正常业务办理，原则上30分钟内无法恢复业务正常运行的，是否立即报告公司住所地证监局，分支机构是否报告所在地证监局。		a）访谈系统运维负责人，询问总部的其他信息系统（包括但不限于网上交易系统，银证、银期、银基系统，融资融券系统）、证券期货投资咨询机构的信息系统发生网络安全事件，影响投资者正常业务办理，原则上30分钟内无法恢复业务正常运行，原则上30分钟内无法恢复业务正常运行的，是否要求立即报告公司住地证监局，受影响分支机构报告所在地证监局。 b）检查报告记录。
9.21		证券期货营业部发生网络安全事件，影响投资者正常业务办理，原则上30分钟内无法恢复业务正常运行的，是否立即报告所在地证监局和公司总部。		a）访谈系统运维负责人，询问证券期货营业部发生网络安全事件，影响投资者正常业务办理，原则上30分钟内无法恢复业务正常运行的，是否立即报告所在地证监局和公司总部。 b）检查报告记录。
9.22		发生数据损毁或泄露的事件，是否立即报告住所地证监局。		a）访谈系统运维负责人，询问发生数据损毁或泄露的事件时，是否立即报告住所地证监局。 b）检查报告记录。

9.23		持续报告是否填写《网络安全事件情况报告书》，内容包括：事件发生时间、地点、简要经过、影响范围初步评估、影响程度初步评估、影响人数初步评估、经济损失初步评估、后果初步判断、原因初步判断、事件性质初步判断、已采取的措施及效果、需要有关部门和单位协助处置的有关事宜、报告单位、签发人和报告时间、联系人与联系方式、与本事件有关的其他内容。		a)访谈系统运维负责人，持续报告时是否填写《网络安全事件情况报告书》，内容包括：事件发生时间、地点、简要经过、影响范围初步评估、影响程度初步评估、影响人数初步评估、经济损失初步评估、后果初步判断、原因初步判断、事件性质初步判断、已采取的措施及效果、需要有关部门和单位协助处置的有关事宜、报告单位、签发人和报告时间、联系人与联系方式、与本事件有关的其他内容。 b)检查报告记录。
9.24		各证券期货交易场所自行决策是否采取临时停市、技术性停牌措施时，是否及时向办公厅值班室、市场部、期货部、证信办报告。		a)访谈系统运维负责人，证券交易所采取临时停市、技术性停牌措施时，是否及时向办公厅值班室、市场部、期货部、证信办报告。 b)检查报告记录。
9.25		各证券期货交易场所决定采取临时停市、暂停交易以及调整开市收市时间等紧急措施时，是否通过本单位网站及相关媒体向市场发布公告，让投资者了解实际情况，稳定市场、媒体和投资者的预期和情绪。同时，密切关注网上舆情，指导会员做好舆论工作。		a)访谈系统运维负责人，证券期货交易场所采取临时停市、暂停交易以及调整开市收市时间等紧急措施时，是否通过本单位网站及相关媒体向市场发布公告。同时，是否密切关注网上舆情，指导会员做好舆论工作。 b)检查公告记录。

9.26		未经批准，是否未擅自发布相关信息。		a）访谈系统运维负责人，应急响应过程中是否有针对性地加强防范，防止事态蔓延措施。是否未经批准，不得擅自发布相关信息。 b）检查应急预案，是否有相关要求。
9.27		是否有针对性的采取措施，备份数据、保护设备、排查隐患，恢复受破坏的网络和信息系统，必要时可依法征用单位和个人的设备和资源，并按规定给予补偿。		a）访谈系统运维负责人，应急响应过程中是否有针对性的采取措施，备份数据、保护设备、排查隐患，恢复受破坏的网络和信息系统，必要时可依法征用单位和个人的设备和资源，并按规定给予补偿。 b）检查应急预案，是否有相关要求。
9.28		是否在应急恢复过程中应保留相关证据，做好应急处置的相关记录。对于人为破坏活动，配合有关部门调查取证工作。		a）访谈系统运维负责人，应急响应过程中是否保留相关证据，做好应急处置的相关记录。对于人为破坏活动，是否配合有关部门调查取证工作。 b）检查应急预案，是否有相关要求。
9.29		是否做好受影响公众的解释、疏导工作，防止发生群体性事件。必要时，请求公安机关协助维护现场秩序。		a）访谈系统运维负责人，应急响应过程中是否做好受影响公众的解释、疏导工作，防止发生群体性事件。必要时，请求公安机关协助维护现场秩序。 b）检查应急预案，是否有相关要求。
14 应急结束				
14.1		各证券、期货交易所和中国证券登记结算公司是否针对各种重大技术故障制定详细的应急预案，并预备相应的停市、暂停交易和恢复交易公告。		a）访谈系统运维负责人，是否制定详细的应急预案，并预备相应的停市、暂停交易和恢复交易公告。 b）检查应急预案相应内容。

14.2		建立有效的应急通讯系统，业务系统耦合度较高的所司之间是否设立24小时热线电话，专机专用、专人值守，确保信息畅通，指挥有效。		a）访谈系统运维负责人，是否建立有效的应急通讯系统，业务系统耦合度较高的所司之间应设立24小时热线电话，专机专用、专人值守，确保信息畅通，指挥有效。 b）检查热线电话信息。
14.3		是否充分利用各种传播媒介及其他有效的宣传形式，加强突发网络安全事件预防和处置的有关法律、法规和政策的宣传，开展网络安全基本知识和技能的宣传活动。		a）访谈系统运维负责人，是否充分利用各种传播媒介及其他有效的宣传形式，加强突发网络安全事件预防和处置的有关法律、法规和政策的宣传，开展网络安全基本知识和技能的宣传活动；并要求相关人员列举媒介及宣传形式。
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。	检查是否具有设计文档、软件使用指南或操作手册等。
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	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~~。

（五）重要系统

序号	审计项	审计项修订建议	审计程序	审计程序修订建议
3 主机管理				
3.1 身份鉴别				
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。	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。（适用于等级保护三级系统）		
3.2 访问控制				

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。	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（root 用户除外）、修改这些帐户的默认口令。
3.3 安全审计				
3.3.5	是否能够根据记录数据进行分析，并生成审计报表。	是否能够根据记录数据进行分析，并生成审计报表。（适用于等级保护三级系统）		
3.3.6	是否保护审计进程，避免受到未预期的中断。	是否保护审计进程，避免受到未预期的中断。（适用于等级保护三级系统）		
3.4 安全管理				
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。	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。（适用于等级保护三级系统）		

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。	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。（适用于等级保护三级系统）		
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。	a）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； 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。
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。	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。（适用于等级保护三级系统）		
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。	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。（适用于等级保护三级系统）		

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。	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。（适用于等级保护三级系统）		
4 系统管理				
4.1 系统架构				
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。	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。（适用于等级保护三级系统）		
4.2 系统建设				
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。	是否书面规定系统交付的控制方法和人员行为准则。（适用于等级保护三级系统）	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。	检查公司相关~~系统建设方面的~~管理制度，查看是否包括系统交付的控制方法和人员行为准则的规定。
4.3 测试验收				
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。	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。（适用于等级保护三级系统）		
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。	是否书面规定系统测试验收的控制方法和人员行为准则。（适用于等级保护三级系统）	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。	检查公司相关~~系统建设方面的~~管理制度，查看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
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。	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。（适用于等级保护三级系统）		
4.5 变更管理				

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。	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。（适用于等级保护三级系统）	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。	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。
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。	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。（适用于等级保护三级系统）	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。	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，查看其是否有审批记录~~主管领导的批准签字~~。
4.6 安全管理				
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。	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。（适用于等级保护三级系统）		
4.7 身份鉴别				
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。	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。（适用于等级保护三级系统）		
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。	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。（适用于等级保护三级系统）		
4.9 资源控制				

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。	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。（适用于等级保护三级系统）		
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。	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。（适用于等级保护三级系统）		
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。	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。（适用于等级保护三级系统）		
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。	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。（适用于等级保护三级系统）		
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。	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。（适用于等级保护三级系统）		
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。	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。（适用于等级保护三级系统）	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。	~~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。

4.12 安全审计				
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。	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。（适用于等级保护三级系统）		
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。	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。（适用于等级保护三级系统）		
1 交易系统				
1.2 安全审计				
1.2.5	是否能够根据记录数据进行分析，并生成审计报表。	是否能够根据记录数据进行分析，并生成审计报表。（适用于等级保护三级系统）		
1.2.6	是否保护审计进程，避免受到未预期的中断。	是否保护审计进程，避免受到未预期的中断。（适用于等级保护三级系统）		
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；	a)查看数据库维护、更新记录；~~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；~~
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；	a)查看公司数据库容量管理相关制度，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
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；	a)查看公司数据库容量管理相关制度，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；

（六）等级保护相关工作

序号	审计项	审计项修订建议	审计程序	审计程序修订建议
1 等级测评				
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。	~~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。~~ a）访谈安全管理员，是否针对系统发生变更时进行了等级保护测评工作； b）检查等级保护测评报告，是否根据测评报告进行相应的整改； c）未进行整改的是否有整改计划或不整改的充分理由。

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。	~~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。~~ a）访谈安全管理员，是否针对二级系统进行了每年的等级保护自查； b）检查等级保护自查报告，是否根据自查报告进行相应的整改； c）未进行整改的是否有整改计划或不整改的充分理由。

（七）应用绩效

序号	审计项	审计项修订建议	审计程序	审计程序修订建议
1 系统建设				
1.2 项目验收				
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。	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说明~~充分理由~~。
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。	核对预决算文档和付款记录~~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说明~~合理理由，并经相关审批~~。

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。	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决算文档和付款记录~~，预算的运营资金与实际的运营资金的差距是否~~合理~~有说明。
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。	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决算文档和付款记录~~，预算的运营资金与实际的运营资金的差距是否~~有说明合理，并经相关审批~~。
1.3 系统性能				
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。	检查系统~~设计测试~~报告，是否包含系统能扩展的相关说明~~判断系统是否可以根据业务需求升级或扩容~~。
2 经济效益				
2.2 无形经济效益				
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。	~~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。~~ 查看是否有第三方提供的相关证明材料。

（八）系统托管

序号	审计项	审计项修订建议	审计程序	审计程序修订建议
1.2 网络通信要求				
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。		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。	b）检查保密承诺书、或合同保密条款，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。

1.4 运维保障				
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。	查看委托合同、应急记录、或相关手册等，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。
2.2 网络通信				
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。		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。	b）检查保密承诺书、或合同保密条款，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。
2.4 运维保障				
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。	查看委托合同、应急记录、或相关手册等，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。
3.2 网络通信				
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。		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。	b）检查保密承诺书、或合同保密条款，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。
4.2 网络通信				

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。		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。	b）检查保密承诺书、或合同保密条款，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。

（九）信息系统建设采购工作

序号	审计项	审计项修订建议	审计程序	审计程序修订建议
1		是否按财政部要求建立健全采购决策管理职能与执行职能相分离的管理体制，成立集中采购管理委员会和集中采购日常管理机构。		参照《国有金融企业集中采购管理暂行规定》，访谈相关人员，了解采购管理体制，查看相关制度，判断是否按要求设立相关机构。
2		是否按财政部要求制定集中采购目录及限额标准。		查看集中采购目录及限额标准。
3		是否按财政部要求制定集中采购管理办法，明确集中采购范围、采购方式、采购的具体程序、内部监督检查主体及职责。		查看集中采购管理办法中是否有采购范围、采购方式、采购具体程序、内部监督检查及职责等内容。
4		单一来源采购项目是否适用于财政部和本单位集中采购管理办法列明的情形。		访谈相关人员，了解已完成的单一来源采购项目情况。查看单一来源采购项目文档，结合财政部要求和本单位采购制度，判断是否适用于单一来源采购方式的情形。

5		是否按财政部要求通过企业网站、招标代理机构网站或省级人民政府采购部门指定公开渠道，向社会披露公开招标或非公开招标的采购项目信息。涉及国家秘密和商业秘密的除外。		访谈相关人员，了解信息系统采购项目公示的流程。登录信息公示相关渠道，查看是否按照《国有金融企业集中采购管理暂行规定》第28条执行。
6		是否在开展大额项目采购时，向采购服务中心申请采购监理服务。		查看满足大额项目采购的相关材料，是否包含向采购服务中心提交的《采购监理服务申请表》以及由采购监理出具的监理报告。
7		是否及时报送采购监理专家，并按照采购服务中心安排积极开展采购监理服务。		查看向采购服务中心报送的监理专家名单的发文，以及监理专家参加采购监理活动的相关文档。
8		会管单位采用公开招标方式进行采购的，是否根据实际情况，从行业专家库中抽选评标委员会技术专家，参与公开招标的信息系统采购项目的评标活动。		查看公开招标的信息系统采购项目评标专家相关记录。
9		行业采购服务中心是否制定采购监理服务工作内部规范，加强对采购监理专家的管理。		访谈行业采购服务中心相关人员，了解采购监理开展情况，查看是否有采购监理服务相关制度规范。
10		是否将本单位信息系统采购制度按要求在证监会会内网信息平台进行公示。		查看已发布的信息系统采购制度，并登录证监会会内网信息平台查看公示文档，判断是否已对发布的制度全部进行公示。
11		是否在新制定或者修订信息系统采购制度后，及时在证监会会内网信息平台进行公示。		访谈相关人员，了解信息系统采购制度更新情况。登录证监会会内网信息平台查看公示文档，判断是否及时对公示文档进行更新。

12		是否按要求提交上月已公示采购项目的《会管单位信息系统建设采购信息摘要表》。		查看信息系统建设采购信息摘要表，判断是否按要求向行业采购服务中心报送上月已公示项目采购信息摘要表。
13		行业采购服务中心是否按月将汇总后的会管单位信息系统采购活动统计表报送会相关单位和部门。		查看信息系统采购活动统计表报送情况，判断是否按月报送会管单位信息系统采购汇总信息。
14		行业采购服务中心是否按季度向相关部门报送信息系统采购项目工作专报。		访谈采购服务中心人员，了解是否按季度对采购信息进行分析。查阅采购工作情况专报。

（十）证联网信息安全

序号	审计项	审计项修订建议	审计程序	审计程序修订建议
1		是否制定证联网接入相关的网络和信息安全应急预案，并定期演练。		a）检查应急预案，查看是否有证联网接入相关的应急预案和处置方案；b）检查应急演练报告，查看是否定期进行证联网接入相关的应急演练。
2		是否在接入证联网的网络边界处部署设备或采取技术措施，按照权限最小化原则进行双向访问控制。		a）访谈网络管理员，在接入证联网的网络边界处部署的安全设备或采取的安全防护技术手段；b）检查接入证联网的边界设备是否按照实际访问和被访问的需求进行严格的访问控制。
3		是否做好公司内网、证联网和互联网的有效隔离。		查看网络拓扑图结构和设备配置文件，检查安全域划分情况，证联网接入区域是否与互联网区域、办公区域等是否采用防火墙等设备进行有效隔离。
4		是否禁止接入证联网的服务器或终端等设备访问互联网。		检查证联网接入服务器或终端等设备，尝试登录互联网网站，验证是否能够访问互联网。

5		是否对接入证联网的终端进行主机监控、移动介质管理和非授权外连管理。		a）访谈网络管理员，接入证联网的终端进行移动介质管理和非授权外联管理的技术手段； b）查看介质管理办法，是否对终端设备的移动介质和外连进行管理； c）随机抽查一台证联网接入终端是否禁止非授权移动介质接入和非法外连。
6		接入证联网的终端设备是否按照国家级行业发布的相关法律、法规、规定做好安全加固及防护工作		a）访谈系统运维负责人，询问证联网终端是否采取了安全加固及防护措施； b）随机抽查一台证联网接入终端，检查开机口令长度是否不少于 12 位、数字和字母相结合，是否定期对终端操作系统进行补丁升级，是否安装防病毒软件，并及时更新病毒定义库到最新版本
7		是否配置 NAT，隐藏内部服务器的实际 IP 地址。		检查接入证联网的边界设备，查看是否配置NAT。
8		证联网接入终端 IP 地址是否 NAT 转换为 41.x.x.224-41.x.x.239 范围内。		检查证联网接入设备配置，查看转换后的 IP 地址是否在 41.x.x.224-41.x.x.239 内。
9		是否监控证联网接入链路状态。		查看网管系统，检查证联网接入链路的状态。
10		证联网承建单位是否配备信息安全管理员，是否配备主、备岗。		检查证联网承建单位是否针对证联网配备了信息安全管理员及主备岗设置情况，或者信息安全管理员职责有覆盖到证联网相关设备和系统。
11		运管中心应定期组织各承建单位进行应急演练。		检查承建单位和运管中心应急演练记录。

12		是否与证联网设备和服务提供商签订安全保密协议，明确安全保密责任义务。		检查承建单位与设备和服务提供商签署的保密协议，查看是否对供应商在服务中可能涉及、接触到的相关业务数据的保密要求作出规定，列明泄密将承担的法律责任。
13		运管中心是否建立全网集中网管系统，实现全网运行状态监控。网络日志留存是否不少于六个月。		a）访谈运管中心网络管理员，证联网集中网管系统部署和监控情况。 b）检查证联网网管系统中网络日志是否至少保存六个月。
14		承建单位是否建立节点网管系统，实现本节点运行状态监控。网络日志留存是否不少于六个月。		a）访谈网络管理员，询问证联网节点网管系统部署和监控情况。 b）检查证联网网管系统中网络日志是否至少保存六个月。
15		运管中心是否按月出具证联网系统运行月报和网络安全报告。		检查运管中心证联网系统运行月报和网络安全报告。