ICS 03.060
A 11
备案号

JR

中华人民共和国金融行业标准

JR/T 0112—2014

证券期货业信息系统审计规范

Information system audit standard for securities and futures industry

2014-12-26 发布　　2014-12-26 实施

中国证券监督管理委员会　　发布

目　次

前　言

本标准按照GB/T 1.1-2009给出的规则起草。

本标准由全国金融标准化技术委员会（SAC/TC180）提出并归口。

本标准起草单位：中国证券监督管理委员会信息中心、上海证券交易所、深圳证券交易所、大连商品交易所、中国金融期货交易所、中证信息技术服务公司、国泰君安证券股份有限公司、海通证券股份有限公司、国信证券股份有限公司、招商证券股份有限公司、嘉实基金管理有限公司、南方基金管理有限公司、鲁证期货股份有限公司、国泰君安期货有限公司。

本标准主要起草人：张野、刘铁斌、王东明、陈炜、俞枫、沈云明、李海军、温军成、金浦芳、赵磊、王欣、吕德旭、周桉、周光增、李艳、李杰、舒春林、康明涛、路冰。

证券期货业信息系统审计规范规范

1 范围

本标准规定了证券期货业信息系统审计工作的要求。

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

2 规范性引用文件

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

JR/T 0059—2010 证券期货经营机构信息系统备份能力标准

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 0099—2012 证券期货业信息系统运维管理规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

信息系统审计 information system audit

核心机构和经营机构根据国家及行业信息系统相关规范和标准，对信息系统规划、建设、运维和应急等活动进行自我检查和评价，判断系统运行的安全性、系统建设的合规性和系统应用绩效，提出整改建议，并持续跟踪落实整改情况。

3.2

审计项 audit item

信息系统规划、建设、运维和应急等活动的关键控制点，来自于国家及行业相关技术规范和标准要求，用于判断系统运行的安全性、系统建设的合规性和系统应用绩效。

3.3

专业能力 professional competence

个人从事信息系统审计所必备的学识、技术和能力，由学历认定、资格考试、职业技能鉴定等方式进行评价。

3.4

第三方审计机构 third party audit institutions

熟悉证券期货业信息安全法规、规范、标准和指引，具有国家、行业认可的相关资质和必要能力，并在审计过程中能够客观、公正、独立地从事审计活动的机构。

4 审计目的

核心机构和经营机构自觉贯彻落实国家及行业信息系统建设、安全运行、绩效考核相关规范和标准，通过查找突出的风险隐患，有针对性的采取防范和改进措施，提高信息安全保障水平、系统建设合规性和应用绩效。

5 审计内容

证券期货业信息系统审计包括3个方面，分别是系统运行安全审计、系统建设合规审计和系统应用绩效审计。核心机构应开展系统运行安全审计、系统建设合规审计和系统应用绩效审计。经营机构应开展系统运行安全审计，并可视情况开展系统建设合规审计、系统应用绩效审计。

系统运行安全审计重点关注系统运维风险，通过审查和评估交易、结算、行情、通信等重要业务信息系统的安全性，及时发现运行风险隐患。系统运行安全审计的内容见附录A，其中期货公司类别是《期货公司信息技术管理指引》评级结果。审计项来自于国家和行业颁布的信息安全法规、规范、标准和指引，主要包括组织管理、机房管理、网络管理、主机和系统管理、运维管理等方面。

系统建设合规审计重点关注违法违规风险，通过审查和评估在采购电子产品、建设信息系统项目、运行维护信息系统等活动中，本机构负责采购的人员、项目建设人员、系统运维人员等是否存在贪污受贿、徇私舞弊、玩忽职守等行为，及时发现违法违规等风险隐患。系统建设合规审计的内容见附录B。审计项来自于通行的信息系统招投标制度、财务预算制度等，主要包括需求论证、预算制定、项目立项、项目采购、项目招标、商务谈判、供应商管理、合同管理、项目验收、钱款支付等方面。

系统应用绩效审计重点关注信息系统能否有效发挥作用，通过审查和评估已建成信息系统的经济效益和使用情况，及时发现资源浪费等风险隐患。系统应用绩效审计的内容见附录C。审计项来自于通行的信息系统绩效评价方法，主要包括系统功能、性能是否达到项目预期目标、经费使用是否合理有效等方面。

附录A、附录B、附录C将根据国家和行业信息安全法规、规范、标准和指引，每年适时更新，保持与现行规定的一致性。核心机构和经营机构应以最新的审计项汇总为基础，开展信息系统审计工作。

6 审计机构

核心机构和经营机构应指定内审部门负责信息系统审计工作，并合理配备具有专业能力的审计人员。内审部门可以根据实际需要聘请具有专业能力的外部专家协助开展信息系统审计工作，可以聘请第三方审计机构协助开展信息系统审计工作，第三方机构的员工必须是正式员工。

核心机构和经营机构的信息技术部门等相关部门应配合内审部门开展信息系统审计工作。

7 审计过程

7.1 审计准备阶段

7.1.1 审计立项

核心机构和经营机构的内审部门应每年开展一次信息系统审计，并将信息系统审计列入年度审计工作计划中，同时报董事会或者高级管理层批准。

信息系统审计计划应包括下列基本内容：

a) 审计工作目标；

b) 审计实施时间；

c) 需要的审计资源；

d) 后续审计安排。

7.1.2 组建审计组

内审部门负责组建审计组，确定审计组组长和成员。审计组成员不得少于2人，其中内审部门人员不得少于1人。

审计组成员应保持独立性和客观性，被审计部门应回避。

审计组组长、审计组成员应具有相关专业能力，并通过定期后续相关培训加以保持和提高。审计组组长应具有信息系统审计工作经验。

审计组成员应履行保密义务，对于实施信息系统审计所获取的信息保密。

7.1.3 制定审计方案

审计组组长应以风险评估为基础，在审计实施前编制审计方案，并报内审部门负责人批准。

审计方案应包括下列基本内容：

a) 被审计部门的名称；
b) 审计目标和范围；
c) 审计内容和重点；
d) 审计程序和方法；
e) 审计组成员的组成及分工；
f) 审计起止日期；
g) 对专家和外部审计工作结果的利用；
h) 其他有关内容。

7.1.4 编制工作底稿

审计组成员对审计方案确定的审计事项，均应编制审计工作底稿。

审计工作底稿应包括以下内容：

a) 被审计部门的名称；
b) 审计事项及其起止日期；
c) 审计程序的执行过程及结果记录；
d) 审计结论、意见及建议；
e) 审计人员姓名和审计日期；
f) 复核人员姓名、复核意见、复核日期；
g) 审计证据的数量及清单；
h) 被审计部门意见、签字及盖章。

审计组应根据被审计部门、审计事项的具体情况，确定选取审计对象的抽样方法，并选取审计对象。

7.2 审计实施阶段

7.2.1 通知被审计部门

审计组应在实施审计10个工作日前，向信息技术部门等被审计部门送达审计通知书。

审计通知书应包括下列内容：

i) 被审计部门名称；
j) 审计范围和审计内容；
k) 审计起止日期；

l) 需要被审计部门提供的资料及其他必要的协助要求；
m) 审计组组长及审计组成员名单。

7.2.2 审计组进场

审计组进驻被审计部门时，应召开有内审部门负责人、审计组组长、审计组成员、被审计部门负责人、被审计部门有关人员参加的进场会议，安排审计工作有关事项。

审计组组长应说明审计目标、审计范围、审计内容、审计重点、审计程序、起止日期等，并提出需要协助、配合审计的有关事项和要求。

被审计部门应汇报相关情况，并提供审计通知书中所列的相关资料，配合审计组开展信息系统审计工作。

7.2.3 实施审计方案

审计组根据实际情况和工作需要，通过访谈、问卷调查等方式，进一步了解被审计部门信息系统有关情况。调查对象一般包括相关业务部门负责人、信息技术部门负责人、信息技术部门相关业务负责人、机房管理员、系统管理员、网络管理员、数据库管理员、安全管理员等相关人员。

审计组应按照审计方案，对信息系统的合规性、可靠性、安全性和绩效等进行评估，并确保不影响系统的正常稳定运行。

审计组应依据不同的审计事项及其审计目标，获取不同种类的审计证据。审计证据主要包括相关制度、日志文件、配置文件、运维记录、测评报告、商业合同等。

审计组应将获取的审计证据名称、来源、内容等完整、清晰地记录于审计工作底稿中。

被审计单位应提供承诺书，承诺相关材料的真实性、完整性、准确性。

审计工作底稿应经审计组组长或其指定人员复核。

审计证据应客观充足，使得重复审计可获得同样结果。当审计人员认为无法获取充足审计证据时，应记录审计证据不足这一事实。

7.2.4 审计结果沟通

现场审计结束前，审计组应就审计发现的问题、审计结论、审计意见和建议与相关业务部门负责人、信息技术部门负责人进行认真、充分的沟通，听取其意见。

审计组应当将结果沟通的有关书面或电子材料作为审计工作底稿的一部分。

7.3 审计终结阶段

7.3.1 撰写审计报告

现场审计结束后，审计组应对取得的审计证据进行综合分析，并撰写审计报告（草稿）。审计报告（草稿）可参考覆盖附录A、附录B、附录C内容的外部审计结果。

审计报告（草稿）主要包括下列内容：

a) 审计概况，包括审计目标、审计范围、审计内容及重点、审计方法、审计程序及起止时间等；
b) 审计依据，即实施审计所依据的相关规范和标准等；
c) 审计问题，即对被审计部门信息技术相关活动所发现的主要问题；
d) 审计结论，即根据已查明的事实，对被审计部门信息技术相关活动的评价；
e) 审计意见和建议，即针对审计发现的主要问题提出的处理意见和改进建议。

审计组应向被审计部门提交审计报告（草稿）。被审计部门应自收到审计报告（草稿）之日起10个工作日内，提出书面反馈意见；在规定期限内没有提出意见的，视同无异议。

被审计部门对审计报告（草稿）有异议的，审计组应研究、核实，并考虑是否需要修改审计报告（草稿）。

审计报告（草稿）经审计组集体讨论，并应通过内审部门对审计报告质量的分级复核程序，由审计组组长及相关报告审核人员审核后定稿。

7.3.2 提交报告

现场审计结束后，审计组应将审计报告、审计工作底稿等相关材料报送内审部门。采用聘请外部专家或第三方审计机构协助开展审计工作的，应将外聘人员或机构的审计工作底稿等相关材料报送内审部门。

核心机构和经营机构的内审部门应向董事会或高级管理层提交审计报告，并抄送有关部门。

8 审计结果应用

8.1 整改方案

当被审计部门基于成本或者其他方面考虑，决定对审计发现的问题不采取纠正措施并做出书面说明时，核心机构和经营机构的内审部门负责人应向董事会或者高级管理层报告。

核心机构和经营机构的被审计部门应对审计中发现的问题，制定有效可行的整改方案，明确进度安排。

审计组应对被审计部门制定的整改方案进行评审。如有必要，核心机构和经营机构的被审计部门应组织由审计组组长、审计组主要成员、相关业务部门负责人、信息技术部门负责人、信息技术部门相关人员、有关专家参加的整改方案评审会议，对整改方案进行评审。

8.2 落实整改

被审计部门应按照整改方案，尽快对审计发现的风险隐患进行整改，并在与审计部门约定的期限内提供审计整改报告。

核心机构和经营机构的内审部门应对审计发现的问题的整改情况进行跟踪监督，可在规定期限内，或者与被审计部门约定的期限内实施后续审计。

内审部门负责人如果初步认定被审计部门对审计发现的问题已采取了有效的纠正措施，可要求内审人员及时对整改措施进行核查，或将后续审计作为下次审计工作的一部分。

内审部门对被审计部门实施后续审计，审计过程与新设审计项目相同，参照本规范第7章对审计过程的规定实施。

9 建档保存

9.1 保存范围

审计工作结束后，审计组应整理相关材料，并建立、保管审计档案。下列材料应归入审计档案：

a) 审计方案、审计通知书；
b) 审计工作底稿、审计报告；
c) 整改方案；
d) 后续审计工作底稿、后续审计报告；
e) 其他相关材料。

9.2 保存期限

审计档案应至少保存5年。

附 录 A
（规范性附录）
系统安全审计项汇总

A.1 核心机构系统运行安全审计项汇总

A.1.1 组织管理

A.1.1.1 安全管理制度

A.1.1.1.1 管理制度

本项要求包括：

a) 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。
b) 是否建立安全管理制度，覆盖安全策略的制定、实施、检查、评估、改进等全过程。
c) 是否形成由安全策略、管理制度、操作规程等构成的全面的信息安全管理制度体系。（本项适用于：信息系统等级保护三级系统）
d) 是否对安全管理人员或操作人员执行的日常管理操作建立操作规程。
e) 是否制定覆盖运维工作各个环节的、体系化的运维管理制度和操作流程。运维管理制度包括但不限于：机房管理、网络与系统管理、数据和介质管理、交付管理、测试管理、配置管理、安全管理、值班管理、监控管理、文档管理、设备和软件管理、供应商管理、关联单位关系管理、检查审计等制度。运维操作流程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。
f) 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。

A.1.1.1.2 制定和发布

本项要求包括：

a) 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。
b) 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。
c) 安全管理制度是否具有统一的格式，并进行版本控制。（本项适用于：信息系统等级保护三级系统）
d) 是否建立信息发布管理审核制度；安全管理制度是否通过正式、有效的方式发布。
e) 安全管理制度是否注明发布范围，并对收发文进行登记。（本项适用于：信息系统等级保护三级系统）
f) 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。（本项适用于：定为信息系统等级保护三级系统的证券交易所交易系统、证券交易所通信系统、开放式基金登记结算系统、证券登记结算系统）

A.1.1.1.3 评审和修订

本项要求包括：

a) 信息安全领导小组是否负责定期组织相关部门和相关人员对安全管理制度体系的合理性和适用性进行审定；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。（本项适用于：信息系统等级保护三级系统）
b) 是否定期或不定期对安全管理制度进行检查和审定，对存在不足或需要改进的安全管理制度进行修订。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。
c) 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。（本项适用于：定为信息系统等级保护三级系统的证券交易所交易系统、证券交易所通信系统、开放式基金登记结算系统、证券登记结算系统）
d) 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。（本项适用于：定为信息系统等级保护三级系统的证券交易所交易系统、证券交易所通信系统、开放式基金登记结算系统、证券登记结算系统）
e) 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.1.1.2 安全管理机构

A.1.1.2.1 机构设置

本项要求包括：
a) 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。
b) 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.1.1.2.2 岗位设置

本项要求包括：
a) 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。
b) 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。
c) 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。（本项适用于：信息系统等级保护三级系统）
d) 是否合理设置运维岗位，规定岗位职责及技能要求，并符合如下要求：
   1) 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；
   2) 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。
e) 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。
f) 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.1.1.2.3 人员配备

本项要求包括：
a) 是否配备系统管理员、网络管理员、安全管理员等；每个岗位应有备岗。
b) 安全管理员是否禁止兼任网络管理员、系统管理员、数据库管理员。（本项适用于：信息系统等级保护二级系统）

c) 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。
d) 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。
e) 关键事务岗位是否配备多人共同管理。（本项适用于：信息系统等级保护三级系统）
f) 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。
g) 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。
h) 是否有应急技术支援队伍。

A.1.1.2.4 授权和审批

本项要求包括：

a) 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。
b) 是否针对关键活动建立审批流程，并由批准人签字确认。（本项适用于：信息系统等级保护二级系统）
c) 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。（本项适用于：信息系统等级保护三级系统）
d) 是否定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息；每年至少审查一次审批事项。（本项适用于：信息系统等级保护三级系统）
e) 是否记录审批过程并保存审批文档。（本项适用于：信息系统等级保护三级系统）
f) 权限分配是否有审批和完整的记录，权限设置后应复核。
g) 是否按照最小安全访问原则分配用户权限。
h) 是否建立权限分配表，对用户的访问权限进行合理分配，对文件系统访问权限进行合理设置，编制文档并保持更新。
i) 是否在用户账户变化时，同时变更或撤销其权限。
j) 是否定期检查权限设置的有效性。

A.1.1.2.5 供应商管理

本项要求包括：

a) 是否确保安全服务商的选择符合国家、行业的有关规定。
b) 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。
c) 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。
d) 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。
e) 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。
f) 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，明确供应商应接受证券期货行业监管部门的信息安全延伸检查。
g) 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。
h) 是否加强运维外包服务管理，主要包括：
   1) 与外包公司及外包人员签订保密协议；

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

A.1.1.2.6 关联单位关系管理

本项要求包括：

a) 是否加强各类管理人员之间、组织内部机构之间以及信息安全职能部门内部的合作与沟通。（本项适用于：信息系统等级保护二级系统）
b) 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。
c) 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。（本项适用于：信息系统等级保护三级系统）
d) 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。（本项适用于：信息系统等级保护三级系统）
e) 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。（本项适用于：信息系统等级保护三级系统）
f) 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。
g) 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。
h) 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。
i) 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。
j) 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。

A.1.1.2.7 审核和检查

本项要求包括：

a) 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；全面安全检查应至少每年一次。（本项适用于：信息系统等级保护三级系统）
b) 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。（本项适用于：信息系统等级保护三级系统）
c) 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。（本项适用于：信息系统等级保护三级系统）
d) 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.1.1.3 经费和人员管理

A.1.1.3.1 经费投入

本项要求包括：

a) 最近三个财政年度IT投入平均数额是否不少于最近三个财政年度平均净利润的6%或不少于最近三个财政年度平均营业收入的3%，取二者数额较大者。
b) 是否制定信息系统运行维护年度预算计划，每年进行核算。预算和核算应接受监督和审计。
c) 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。
d) 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。
e) 安全建设的投入是否超过IT总投入的15%。
f) 是否对资金的使用进行绩效考核。

A.1.1.3.2 人员录用

本项要求包括：

a) 是否指定或授权专门的部门或人员负责人员录用。
b) 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。
c) 是否与开发、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。
d) 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。（本项适用于：信息系统等级保护三级系统）

A.1.1.3.3 人员离岗

本项要求包括：

a) 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。
b) 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。
c) 是否办理严格的调离手续。（本项适用于：信息系统等级保护二级系统）
d) 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。（本项适用于：信息系统等级保护三级系统）

A.1.1.3.4 人员考核

本项要求包括：

a) 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应至少每年一次。
b) 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。（本项适用于：信息系统等级保护三级系统）
c) 是否对考核结果进行记录并保存。（本项适用于：信息系统等级保护三级系统）
d) 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。（本项适用于：定为信息系统等级保护三级系统的证券交易所交易系统、证券交易所通信系统、开放式基金登记结算系统、证券登记结算系统）

A.1.1.3.5 教育和培训

本项要求包括：

a) 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。
b) 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。
c) 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。
d) 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。（本项适用于：信息系统等级保护三级系统）

A.1.1.3.6 外部人员访问管理

本项要求包括：
a) 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。
b) 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。（本项适用于：信息系统等级保护三级系统）

A.1.2 机房管理

A.1.2.1 基础保障

A.1.2.1.1 物理位置的选择

本项要求包括：
a) 机房和办公场地是否选择具有防震、防风和防雨等能力的建筑：
   1) 应具有机房或机房所在建筑物符合当地抗震要求的相关证明；
   2) 机房外墙壁应没有对外的窗户。否则，应采用双层固定窗，并作密封、防水处理。
b) 机房场地是否避免设在建筑物的高层或地下室，以及用水设备的下层或隔壁：（本项适用于：信息系统等级保护三级系统）
   1) 机房场地不宜设在建筑物顶层，如果不可避免，应采取有效的防水措施。机房场地设在建筑物地下室的，应采取有效的防水措施；
   2) 机房场地设在建筑物高层的，应对设备采取有效固定措施；
   3) 如果机房周围有用水设备，应当有防渗水和疏导措施。

A.1.2.1.2 防雷击

本项要求包括：
a) 机房或机房所在大楼，是否设计并安装防雷击措施，防雷措施应至少包括避雷针或避雷器等。
b) 机房是否设置交流电源地线。
c) 是否设置防雷保安器，防止感应雷。（本项适用于：信息系统等级保护三级系统）

A.1.2.1.3 防火

本项要求包括：
a) 机房是否设置灭火设备和火灾自动报警系统。机房的火灾自动报警系统应向当地公安消防部门备案。（本项适用于：信息系统等级保护二级系统）
b) 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应向当地公安消防部门备案。（本项适用于：信息系统等级保护三级系统）

c) 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。（本项适用于：信息系统等级保护三级系统）
d) 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。（本项适用于：信息系统等级保护三级系统）
e) 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.1.2.1.4 防水和防潮

本项要求包括：

a) 水管安装，是否穿过机房屋顶和活动地板下；
   1) 与机房设备无关的水管不得穿过机房屋顶和活动地板下；
   2) 机房屋顶和活动地板下铺有水管的，应采取有效防护措施。
b) 是否采取措施防止雨水通过机房窗户、屋顶和墙壁渗透。
c) 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。
d) 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。（本项适用于：信息系统等级保护三级系统）

A.1.2.1.5 防静电

本项要求包括：

a) 关键设备应采用必要的接地防静电措施。（本项适用于：信息系统等级保护二级系统）
b) 主要设备是否采用必要的接地防静电措施。（本项适用于：信息系统等级保护三级系统）
c) 机房是否采用防静电地板。（本项适用于：信息系统等级保护三级系统）
d) 是否采用静电消除器等装置，减少静电的产生。（本项适用于：定为信息系统等级保护三级系统的证券交易所交易系统、证券交易所通信系统）

A.1.2.1.6 空调

本项要求包括：

a) 机房是否设置温、湿度自动调节设施，使机房温、湿度的变化在设备运行所允许的范围之内：
   1) 开机时机房温度应控制在 22℃-24℃；
   2) 开机时机房相对湿度应控制在 40%-55%。
b) 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。
c) 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.1.2.1.7 电力供应

本项要求包括：

a) 是否在机房供电线路上配置稳压器和过电压防护设备。
b) 是否提供短期的备用电力供应，至少满足主要设备在断电情况下的正常运行要求。
   1) 机房应配备 UPS，UPS 实际供电能力能够满足主要设备在断电情况下正常运行 2 个小时以上；
   2) 机房应自备或租用发电机，能够保障持续供电。
c) 是否提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求；机房应配备 UPS，UPS 实际供电能力能够满足设备在断电情况下正常运行 2 个小时以上。（本项适用于：定为信息系统等级保护三级系统的证券交易所交易系统、证券交易所通信系统）
d) 是否采用双路市电，双路市电应能实现自动切换。（本项适用于：信息系统等级保护三级系统）

A.1.2.1.8 电磁防护

本项要求包括：

a) 电源线和通信线缆是否隔离铺设，避免互相干扰。电源线和通信线缆应铺设在不同的桥架或管道，避免互相干扰。

b) 是否采用接地方式防止外界电磁干扰和设备寄生耦合干扰：（本项适用于：信息系统等级保护三级系统）

   1) 机房或机房所在的大楼必须有接地措施，并且接地电阻必须小于 1 欧姆；

   2) 机房验收报告应提供合格的检测结果。

c) 是否对关键设备和磁介质实施电磁屏蔽。（本项适用于：信息系统等级保护三级系统）

A.1.2.2 机房运维

A.1.2.2.1 物理访问控制

本项要求包括：

a) 机房出入口是否安排专人值守，控制、鉴别和记录进入的人员；

   1) 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；

   2) 没有门禁系统的机房，应当安排专人控制、鉴别和记录人员的进出；

   3) 有门禁系统的机房，应当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。

b) 机房出入口是否安排专人值守并配置电子门禁系统，控制、鉴别和记录进入的人员：（本项适用于：定为信息系统等级保护三级系统的证券交易所交易系统、证券交易所通信系统）

   1) 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；

   2) 应当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。

c) 需进入机房的来访人员是否经过申请和审批流程，并限制和监控其活动范围；

   1) 来访人员进入机房，应有审批流程，记录带进带出的设备、进出时间、工作内容，并有专人陪同其在限定的范围内工作；

   2) 机房出入口应有视频监控，监控记录至少保存 3 个月。

d) 是否对机房划分区域进行管理，区域和区域之间设置物理隔离装置，在重要区域前设置交付或安装等过渡区域：（本项适用于：信息系统等级保护三级系统）

   1) 机房应当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；

   2) 机房应当设置专门的过渡区域，用于设备的交付或安装；

   3) 重要区域包括：主机房、辅助区、支持区等功能区域。

e) 重要区域是否配置第二道电子门禁系统，控制、鉴别和记录进入的人员。（本项适用于：定为信息系统等级保护三级系统的证券交易所交易系统、证券交易所通信系统）

A.1.2.2.2 防盗窃和防破坏

本项要求包括：

a) 是否将主要设备放置在机房内。

b) 是否将设备或主要部件进行固定，并设置明显的不易除去的标记；

   1) 主要设备应当安装、固定在机柜内或机架上；

   2) 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。

c) 是否将通信线缆铺设在隐蔽处，可铺设在地下或管道中；通信线缆可铺设在管道或线槽、线架中。
d) 是否对介质分类标识，存储在介质库或档案室中。
e) 主机房应安装必要的防盗报警设施。（本项适用于：信息系统等级保护二级系统）
f) 是否利用光、电等技术设置机房防盗报警系统。（本项适用于：信息系统等级保护三级系统）
g) 是否对机房设置监控报警系统：（本项适用于：信息系统等级保护三级系统）
   1) 应至少对机房的出入口、操作台等区域进行摄像监控；
   2) 监控录像记录至少保存 3 个月。

A.1.2.2.3 机房管理

本项要求包括：
a) 是否指定专门的部门或人员定期对机房供配电、空调、温湿度控制等设施进行维护管理；
   1) 应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；
   2) 应每年对防盗报警、防雷、消防等装置进行检测维护并保存相关维护记录。
b) 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。
c) 是否加强对办公环境的保密性管理，包括工作人员调离办公室应立即交还该办公室钥匙和不在办公区接待来访人员等。（本项适用于：信息系统等级保护二级系统）
d) 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。
e) 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。（本项适用于：信息系统等级保护三级系统）
f) 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。（本项适用于：定为信息系统等级保护三级系统的证券交易所交易系统、证券交易所通信系统、开放式基金登记结算系统、证券登记结算系统）
g) 是否指定机房管理负责人。
h) 是否确保机房环境整洁和安全，包括：
   1) 应定期检查防水、防雷、防火、防潮、防尘、防鼠、防静电、防电磁辐射等措施的有效性；
   2) 应保持机房环境卫生，采取防尘措施，定期进行除尘处理；
   3) 交易时间内不得进行机房施工、保洁操作。
i) 是否对设备和人员出入进行严格管理，包括：
   1) 应指定人员负责控制、鉴别和记录设备和人员的进出情况，记录进出人员、进出时间、工作内容，并留存记录至少 90 天；
   2) 机房出入口的监控录像至少保存 90 天；
   3) 外来人员进入机房应经过申请和审批流程，并限制和监控其活动范围，并有专人陪同；
   4) 外来设备未经批准不得接入生产环境。
j) 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.1.2.2.4 用电安全

本项要求包括：
a) 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。

b) 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。
c) 是否在危险性高的位置张贴相应的用电安全操作方法、警示及指引。
d) 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。
e) 未经审批是否禁止接入其他用电设备。

A.1.2.2.5 机房消防

本项要求包括：
a) 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。
b) 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。
c) 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。
d) 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。
e) 是否定期进行消防设施的使用培训和演习。

A.1.3 网络管理

A.1.3.1 网络安全

A.1.3.1.1 结构安全

本项要求包括：
a) 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%。
b) 是否保证接入网络和核心网络的带宽满足业务高峰期需要。（本项适用于：信息系统等级保护二级系统）
c) 是否保证网络各个部分的带宽满足业务高峰期需要。（本项适用于：信息系统等级保护三级系统）
d) 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。（本项适用于：信息系统等级保护三级系统）
e) 是否绘制与当前运行情况相符的网络拓扑结构图；应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。
f) 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。
g) 是否提供关键网络设备、通信线路和数据处理系统的硬件冗余，保证系统的可用性。（本项适用于：信息系统等级保护二级系统）
h) 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，重要网段与其他网段之间采取可靠的技术隔离手段。（本项适用于：信息系统等级保护三级系统）
i) 是否按照对业务服务的重要次序来指定带宽分配优先级别，保证在网络发生拥堵的时候优先保护重要主机。应对所有业务确定重要性、优先级，制定业务相关带宽分配原则及相应的带宽控制策略，根据安全需求，采取网络 QoS 或专用带宽管理设备等措施。（本项适用于：信息系统等级保护三级系统）

j) 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。（本项适用于：信息系统等级保护三级系统）
k) 通信带宽是否保持在历史流量峰值的 4 倍以上。
l) 重要线路是否至少具有一条以上的备份线路。
m) 与交易业务相关的系统是否在行业专网上部署。

A.1.3.1.2 访问控制

本项要求包括：

a) 网络边界是否部署访问控制设备并启用访问控制功能。
b) 是否针对数据流提供明确的允许/拒绝访问的访问控制策略，控制力度达到网段级。网络边界访问控制设备应设定过滤规则集。规则集应涵盖对所有出入边界的数据包的处理方式，对于没有明确定义的数据包，应缺省拒绝。（本项适用于：信息系统等级保护二级系统）
c) 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。（本项适用于：信息系统等级保护三级系统）
d) 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。
e) 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。
f) 是否对进出网络的信息内容进行过滤，实现对应用层 HTTP、FTP、TELNET、SMTP、POP3 等协议命令级的控制；对通过互联网传输的信息内容进行过滤，实现对应用层 HTTP、FTP、TELNET、SMTP、POP3 等通用性协议命令级控制。（本项适用于：信息系统等级保护三级系统）
g) 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。（本项适用于：信息系统等级保护三级系统）
h) 是否限制网络最大流量数及网络连接数。（本项适用于：信息系统等级保护三级系统）
i) 重要网段是否采取技术手段防止地址欺骗。（本项适用于：信息系统等级保护三级系统）
j) 是否制定网络访问控制策略，应合理设置网络隔离设施上的访问控制列表，关闭与业务无关的端口；编制文档并保持更新；访问控制策略的变更应履行审批手续。

A.1.3.1.3 安全审计

本项要求包括：

a) 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) 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。
c) 是否能够根据记录数据进行分析，并生成审计报表。（本项适用于：信息系统等级保护三级系统）
d) 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。（本项适用于：信息系统等级保护三级系统）
e) 是否定期检查网络设备的用户、口令及权限设置的正确性。
f) 是否留存网络访问日志。

A.1.3.1.4 边界完整性检查

本项要求包括：

a) 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，准确定出位置，并对其进行有效阻断。（本项适用于：信息系统等级保护二级系统）
b) 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。（本项适用于：信息系统等级保护三级系统）
c) 是否能够对内部网络用户私自联到外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。（本项适用于：信息系统等级保护三级系统）
d) 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.1.3.1.5 入侵防范

本项要求包括：
a) 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。
b) 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应提供报警。（本项适用于：信息系统等级保护三级系统）

A.1.3.1.6 恶意代码防范

本项要求包括：
a) 是否在网络边界处对恶意代码进行检测和清除：（本项适用于：信息系统等级保护三级系统）
   1) 在不严重影响网络性能和业务的情况下，应在网络边界部署恶意代码检测系统；
   2) 如果部署了主机恶意代码检测系统，可选择安装部署网络边界恶意代码检测系统。
b) 是否维护恶意代码库的升级和检测系统的更新。

A.1.3.1.7 网络设备防护

本项要求包括：
a) 是否对登录网络设备的用户进行身份鉴别；应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。
b) 是否对网络设备的管理员登录地址进行限制。
c) 网络设备用户的标识是否唯一。
d) 身份鉴别信息是否具有不易被冒用的特点，口令是否有复杂度要求并定期更换；
   1) 口令应符合以下条件：数字、字母、符号混排，无规律的方式；
   2) 管理员用户口令的长度至少为 12 位；
   3) 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；
   4) 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。
e) 是否具有登录失败处理功能，是否采取结束会话、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。
f) 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。
g) 主要网络设备是否对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别：（本项适用于：信息系统等级保护三级系统）
   1) 通过本地控制台管理主要网络设备时，应采用一种或一种以上身份鉴别技术；
   2) 以远程方式登录主要网络设备，应采用两种或两种以上组合的鉴别技术进行身份鉴别。

h) 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。（本项适用于：信息系统等级保护三级系统）

A.1.4 主机和系统管理

A.1.4.1 主机安全

A.1.4.1.1 身份鉴别

本项要求包括：

a) 是否对登录操作系统和数据库系统的用户进行身份标识和鉴别。
b) 操作系统和数据库系统管理用户身份标识是否具有不易被冒用的特点，口令应有复杂度要求并定期更换；
   1) 口令应符合以下条件：数字、字母、符号混排，无规律的方式；
   2) 口令的长度至少为 12 位；
   3) 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；
   4) 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。
c) 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。
d) 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。
e) 是否为操作系统和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：
   1) 应为操作系统的不同用户分配不同的用户名；
   2) 应为数据库系统的不同用户分配不同的用户名。
f) 是否采用两种或两种以上组合的鉴别技术对管理用户进行身份鉴别：（本项适用于：信息系统等级保护三级系统）
   1) 通过本地控制台管理主机设备时，应采用一种或一种以上身份鉴别技术；
   2) 以远程方式登录主机设备，应采用两种或两种以上组合的鉴别技术进行身份鉴别。

A.1.4.1.2 访问控制

本项要求包括：

a) 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。
b) 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。
c) 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。
   1) 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；
   2) 系统无法重命名的特殊默认账户，可不重命名。
d) 是否及时删除多余的、过期的账户，避免共享账户的存在。
e) 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。（本项适用于：信息系统等级保护三级系统）

A.1.4.1.3 安全审计

本项要求包括：

a) 审计范围是否覆盖到服务器上的每个操作系统用户和数据库用户；应在保证系统运行安全和效率的前提，启用系统审计或采用第三方安全审计产品实现审计要求。（本项适用于：信息系统等级保护二级系统）

b) 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。
c) 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。
d) 是否保护审计记录，避免受到未预期的删除、修改或覆盖等。审计记录应至少保存6个月。
e) 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和数据库用户；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。（本项适用于：信息系统等级保护三级系统）
f) 是否能够根据记录数据进行分析，并生成审计报表。（本项适用于：信息系统等级保护三级系统）
g) 是否保护审计进程，避免受到未预期的中断。（本项适用于：信息系统等级保护三级系统）

A.1.4.1.4 入侵防范

本项要求包括：

a) 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，应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。
b) 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。（本项适用于：信息系统等级保护三级系统）
c) 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，应停止有关服务，并提供报警。（本项适用于：信息系统等级保护三级系统）

A.1.4.1.5 恶意代码防范

本项要求包括：

a) 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；
   1) 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；
   2) 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。
b) 是否支持防恶意代码软件的统一管理。
c) 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。（本项适用于：信息系统等级保护三级系统）

A.1.4.1.6 资源控制

本项要求包括：

a) 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。
b) 是否根据安全策略设置登录终端的操作超时锁定。
c) 是否限制单个用户对系统资源的最大或最小使用限度。
d) 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。（本项适用于：信息系统等级保护三级系统）
e) 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。（本项适用于：信息系统等级保护三级系统）

A.1.4.2 应用安全

A.1.4.2.1 结构安全

本项要求包括：

a) 交易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。

b) 处理能力是否至少具有历史交易峰值 4 倍以上的峰值处理能力和日处理能力。

A.1.4.2.2 身份鉴别

本项要求包括：

a) 是否提供专用的登录控制模块对登录用户进行身份标识和鉴别。

b) 是否提供用户身份标识唯一和鉴别信息复杂度检查功能，保证应用系统中不存在重复用户身份标识，身份鉴别信息不易被冒用。

c) 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。

d) 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。

e) 是否对同一用户采用两种或两种以上组合的鉴别技术实现用户身份鉴别：（本项适用于：信息系统等级保护三级系统）

   1) 管理用户通过受控本地控制台管理应用系统时，应采用一种或一种以上身份鉴别技术；

   2) 管理用户以远程方式登录应用系统，应采用两种或两种以上组合的鉴别技术进行身份鉴别；

   3) 面向互联网服务的系统应当提供两种或两种以上组合的鉴别技术供用户选择。

A.1.4.2.3 访问控制

本项要求包括：

a) 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、数据库表等客体的访问，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。

b) 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。

c) 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。

d) 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。

e) 核心系统是否有授权管理功能。

A.1.4.2.4 安全审计

本项要求包括：

a) 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。

b) 是否采取有效措施防止删除、修改或覆盖审计记录。（本项适用于：信息系统等级保护二级系统）

c) 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。审计记录应至少保存 6 个月。

d) 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。（本项适用于：信息系统等级保护三级系统）

e) 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。（本项适用于：信息系统等级保护三级系统）

A.1.4.2.5 通信完整性

本项要求包括：

a) 通过互联网、卫星网进行通信时，是否采用校验码技术保证通信过程中数据的完整性。（本项适用于：信息系统等级保护二级系统）
b) 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。（本项适用于：信息系统等级保护三级系统）
c) 是否能够检测到鉴别信息和重要业务数据在传输过程中完整性受到破坏。（本项适用于：信息系统等级保护二级系统）
d) 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。（本项适用于：信息系统等级保护三级系统）

A.1.4.2.6 通信保密性

本项要求包括：

a) 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。
b) 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。

A.1.4.2.7 抗抵赖

本项要求包括：

a) 是否具有在请求的情况下为数据原发者或接收者提供数据原发证据的功能;应用系统的操作与管理记录，至少应记录操作时间、操作人员及操作类型、操作内容等信息。交易系统应能够记录用户交易行为数据，至少包括业务流水号、账户名、IP 地址、交易指令等信息。（本项适用于：信息系统等级保护三级系统）
b) 是否具有在请求的情况下为数据原发者或接收者提供数据接收证据的功能。应用系统的操作与管理记录，至少应记录操作时间、操作人员及操作类型、操作内容等信息。交易系统应能够记录用户交易行为数据，至少包括业务流水号、账户名、IP 地址、交易指令等信息。（本项适用于：信息系统等级保护三级系统）

A.1.4.2.8 软件容错

本项要求包括：

a) 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。
b) 在故障发生时，应用系统是否能够继续提供一部分功能，确保能够实施必要的措施。（本项适用于：信息系统等级保护二级系统）
c) 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。（本项适用于：信息系统等级保护三级系统）

A.1.4.2.9 资源控制

本项要求包括：

a) 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，另一方是否能够自动结束会话。用户登录应用系统后在规定的时间内未执行任何操作，应自动退出系统。

b) 是否能够对系统的最大并发会话连接数进行限制。
c) 是否能够对单个账户的多重并发会话进行限制。
d) 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。（本项适用于：信息系统等级保护三级系统）
e) 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。（本项适用于：信息系统等级保护三级系统）
f) 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。（本项适用于：信息系统等级保护三级系统）
g) 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。（本项适用于：信息系统等级保护三级系统）

A.1.4.3 数据安全及备份恢复

A.1.4.3.1 数据完整性

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存储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。（本项适用于：信息系统等级保护三级系统）

A.1.4.3.2 数据保密性

本项要求包括：

a) 是否采用加密或其他保护措施实现鉴别信息的存储保密性。（本项适用于：信息系统等级保护二级系统）
b) 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。（本项适用于：信息系统等级保护三级系统）

A.1.5 运维管理

A.1.5.1 系统建设管理

A.1.5.1.1 系统定级

本项要求包括：

a) 是否明确信息系统的边界和安全保护等级。
b) 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。
c) 是否确保信息系统的定级结果经过相关部门的批准。
d) 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。（本项适用于：信息系统等级保护三级系统）
e) 定级结果是否经过相关部门批准，由证信办出具定级审核意见。

A.1.5.1.2 方案设计

本项要求包括：

a) 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。
b) 是否以书面形式描述对系统的安全保护要求、策略和措施等内容，形成系统的安全方案。（本项适用于：信息系统等级保护二级系统）
c) 是否对安全方案进行细化，形成能指导安全系统建设、安全产品采购和使用的详细设计方案。（本项适用于：信息系统等级保护二级系统）

d) 是否组织相关部门和有关安全技术专家对安全设计方案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。（本项适用于：信息系统等级保护二级系统）
e) 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。（本项适用于：信息系统等级保护三级系统）
f) 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。（本项适用于：信息系统等级保护三级系统）
g) 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。（本项适用于：信息系统等级保护三级系统）
h) 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。（本项适用于：信息系统等级保护三级系统）
i) 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。
j) 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.1.5.1.3 产品采购和使用

本项要求包括：

a) 是否确保安全产品采购和使用符合国家的有关规定。
b) 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。
c) 是否指定或授权专门的部门负责产品的采购。
d) 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。（本项适用于：信息系统等级保护三级系统）

A.1.5.1.4 自行软件开发

本项要求包括：

a) 开发环境是否与实际运行环境物理分离。（本项适用于：信息系统等级保护二级系统）
b) 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。
c) 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。
d) 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。应保证同一组件或子系统的开发人员和测试人员分离。（本项适用于：信息系统等级保护三级系统）
e) 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。（本项适用于：信息系统等级保护三级系统）
f) 是否对程序资源库的修改、更新、发布进行授权和批准。（本项适用于：信息系统等级保护三级系统）
g) 开发人员是否为专职人员，开发人员的开发活动是否受到控制、监视和审查。（本项适用于：定为信息系统等级保护三级系统的证券交易所交易系统、证券交易所通信系统）
h) 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。

A.1.5.1.5 外包软件开发

本项要求包括：

a) 是否根据开发要求测试软件质量。
b) 是否确保提供软件设计的相关文档和使用指南。
c) 是否在软件安装之前检测软件包中可能存在的恶意代码。
d) 要求开发单位提供软件源代码，并审查软件中可能存在的后门。

A.1.5.1.6 工程实施

本项要求包括：
a) 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。
b) 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。
c) 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。（本项适用于：信息系统等级保护三级系统）

A.1.5.1.7 系统交付

本项要求包括：
a) 是否向用户提供系统建设文档和运行维护所需文档。
b) 是否书面规定系统交付的控制方法和人员行为准则。（本项适用于：信息系统等级保护三级系统）
c) 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。（本项适用于：信息系统等级保护三级系统）
d) 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。
e) 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。
f) 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。
g) 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。

A.1.5.1.8 测试验收

本项要求包括：
a) 是否对系统进行安全性测试验收。（本项适用于：信息系统等级保护二级系统）
b) 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。
c) 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。
d) 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。（本项适用于：信息系统等级保护三级系统）
e) 是否书面规定系统测试验收的控制方法和人员行为准则。（本项适用于：信息系统等级保护三级系统）
f) 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。（本项适用于：信息系统等级保护三级系统）
g) 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。
h) 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。

i) 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。模拟环境应与生产环境进行有效隔离，不得对生产环境进行干扰。
j) 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。
k) 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。
l) 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。
m) 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。
n) 是否提前发布生产环境测试的系统测试公告。
o) 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。
p) 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。
q) 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。
r) 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。
s) 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。
t) 测试后是否恢复生产环境并验证恢复的有效性。
u) 是否禁止交易时段使用生产环境进行测试。
v) 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.1.5.1.9 系统备案

本项要求包括：
a) 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。（本项适用于：信息系统等级保护三级系统）
b) 是否将系统等级及相关材料报证监会证信办备案。
c) 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.1.5.1.10 等级测评

本项要求包括：
a) 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。（本项适用于：信息系统等级保护三级系统）
b) 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。（本项适用于：信息系统等级保护三级系统）
c) 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。（本项适用于：信息系统等级保护三级系统）
d) 是否指定或授权专门的部门或人员负责等级测评的管理。（本项适用于：信息系统等级保护三级系统）
e) 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.1.5.2 系统运维管理

A.1.5.2.1 值班管理

本项要求包括：

a) 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。
b) 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。
c) 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。
d) 是否制定交接班流程，并严格执行，留存记录。
e) 是否设置运维值班电话，并保持畅通。

A.1.5.2.2 文档管理

本项要求包括：

a) 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。
b) 是否明确文档管理的责任人。
c) 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。
d) 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。
e) 是否对超范围、超权限使用文档时，保存相关审批、使用记录。

A.1.5.2.3 资产管理

本项要求包括：

a) 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。
b) 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。
c) 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。（本项适用于：信息系统等级保护三级系统）
d) 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。（本项适用于：信息系统等级保护三级系统）

A.1.5.2.4 数据与介质管理

本项要求包括：

a) 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。
b) 是否对介质归档和查询等过程进行记录，并根据存档介质的目录清单定期盘点。（本项适用于：信息系统等级保护二级系统）
c) 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。
d) 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。
e) 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。

f) 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，应按国家相关规定另行处理。
g) 是否根据数据备份的需要对某些介质实行异地存储，存储地的环境要求和管理方法应与本地相同。（本项适用于：信息系统等级保护三级系统）
h) 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。（本项适用于：信息系统等级保护三级系统）
i) 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。
j) 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。
k) 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。
l) 在线数据管理，是否做到如下要求：
   1) 交易业务系统数据应至少每交易日备份一次；
   2) 交易业务系统历史数据至少保留一年；
   3) 未经授权不得访问、复制；
   4) 对数据的修改应通过审批，双岗操作并记录操作日志。
m) 离线数据管理，是否做到如下要求：
   1) 离线数据不得更改；
   2) 应至少每季度对核心交易业务系统的备份数据进行一次有效性验证，如发现问题应采取措施修复备份数据，并查明原因；
   3) 离线数据的调阅、复制、传输、查询，应按照拟定的流程办理审批手续，并进行登记；
   4) 备份数据带离存储环境时应采取必要的安全措施。
n) 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。
o) 离线备份介质是否在本地机房、同城、异地安全可靠存放。
p) 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。
q) 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。
r) 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。

A.1.5.2.5 设备和软件管理

本项要求包括：

a) 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。
b) 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。
c) 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。
d) 信息处理设备是否经过审批才能带离机房或办公地点。
e) 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。（本项适用于：信息系统等级保护三级系统）
f) 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。

g) 是否明确设备和软件管理责任人。
h) 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。
i) 是否编制信息系统设备清单，主要包括设备名称、设备编号、入库时间、设备主要参数、设备序列号、设备状态、设备保修期、设备位置、设备用途和设备使用责任人等内容，并保留设备启用、转移、维修、报废等过程的记录。
j) 是否使用正版软件并保存软件授权证书和许可协议，应编制软件清单，主要包括软件名称、软件编号、入库时间、软件版本，授权和许可情况、软件序列号、软件状态、软件维护期、软件安装设备、用途和使用责任人等内容，并保留软件启用、转移、升级、报废等过程的记录。
k) 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。
l) 是否对外送设备的维修进行严格管理，防止数据泄露。
m) 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.1.5.2.6 变更管理

本项要求包括：

a) 是否确认系统中要发生的变更，并制定相应的变更方案；重要系统变更前应制定详细的变更方案、失败恢复方案、专项应急预案。
b) 系统发生重要变更前，是否向主管领导申请，审批后方可实施变更，并在实施后向相关人员通告。（本项适用于：信息系统等级保护二级系统）
c) 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。（本项适用于：信息系统等级保护三级系统）
d) 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。（本项适用于：信息系统等级保护三级系统）
e) 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。（本项适用于：信息系统等级保护三级系统）
f) 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。（本项适用于：定为信息系统等级保护三级系统的证券交易所交易系统、证券交易所通信系统、开放式基金登记结算系统、证券登记结算系统）
g) 是否建立系统变更流程，对信息系统的变更活动进行规范。
h) 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。
i) 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。
j) 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。
k) 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。
l) 是否按照测试方案，组织变更前后的测试，测试后应提交测试记录或报告。
m) 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。
n) 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。
o) 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。

p) 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。

A.1.5.2.7 配置管理

本项要求包括：

a) 是否制定配置管理流程，明确配置管理负责人。
b) 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。
c) 配置库中配置项的属性是否至少包括以下信息。
   1) 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；
   2) 配置项编号应唯一；
   3) 配置项的添加、修改、替换、删除应有变更记录；
   4) 应保存配置项历史记录，确保与事件管理、问题管理、变更管理等流程记录的关联性。
d) 是否定期对配置库进行备份。
e) 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。

A.1.5.2.8 日常操作

本项要求包括：

a) 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。
b) 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。
c) 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。
d) 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。
e) 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。
f) 是否对核心交易业务系统设置独立的操作和监控环境，与开发、测试等其他操作环境严格分离。
g) 注册邮箱账号是否经过审批。

A.1.5.2.9 口令管理

用户和口令管理是否符合如下要求：

1) 不得设置弱口令，若系统条件允许，口令应采用数字、字母、符号混排且无规律的方式，管理员口令长度原则上不低于 12 位；核心交易业务系统应提示并阻止用户使用弱口令登录；
2) 应每季度对管理员口令进行修改，更新的管理员口令至少 5 次内不能重复；
3) 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；
4) 应重点加强对匿名/默认用户的管理，防止被非法使用；
5) 应及时注销不再使用的账户；
6) 应明确责任人，负责统一保管、安全存放管理员口令，不得泄漏。

A.1.5.2.10 数据库管理

本项要求包括：

a) 是否保持数据库的可用性，及时维护、更新软件。
b) 是否负责数据库的参数配置、调优，编制文档并保持更新。
c) 是否定期对数据库容量进行检查和评估，形成评估报告。
d) 是否负责管理数据库、表、索引、存储过程，数据库的升级、优化、扩容、迁移。
e) 是否定期检查数据库的用户、口令及权限设置的正确性。

A.1.5.2.11 督促检查

本项要求包括：

a) 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。
b) 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。
c) 是否每季组织开展内部检查，形成检查报告。
d) 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。
e) 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。
f) 是否对检查和审计的结果采取纠正性和预防性的措施。
g) 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.1.5.2.12 监控分析

本项要求包括：

a) 是否应采取监控措施，配备监控和报警工具，对影响信息系统正常运行的关键对象，包括机房环境、网络、通信线路、主机、存储、数据库、核心交易业务相关的应用系统、安全设备等进行监控，形成记录并妥善保存。报警方式可包括声光、电话、短信、邮件等。
b) 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。（本项适用于：信息系统等级保护三级系统）
c) 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。（本项适用于：信息系统等级保护三级系统）
d) 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，应开启自动监控系统和自动报警系统。
e) 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。
f) 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。
g) 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。
h) 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。
i) 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。
j) 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。

k) 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。
l) 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。
m) 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。
n) 门户网站监控指标是否包括网页内容、日均访问量等。
o) 是否针对不同系统设置合理的监测频度。
p) 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。
q) 是否保存监控产生的日志，保存时间不少于一年。
r) 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。应至少每季度全面评估监控日志和操作记录，分析异常情况，形成评估报告。

A.1.5.2.13 网络安全管理

本项要求包括：

a) 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。
b) 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。
c) 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；应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。
d) 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；
   1) 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；
   2) 实施漏洞扫描或漏洞修补前，应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；
   3) 漏洞扫描或漏洞修补后应进行验证测试，以保证网络系统的正常运行。
e) 是否保证所有与外部系统的连接均得到授权和批准。
f) 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；应在配置变更前、变更后分别对网络设备的配置文件进行备份。（本项适用于：信息系统等级保护三级系统）
g) 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。（本项适用于：信息系统等级保护三级系统）
h) 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。（本项适用于：信息系统等级保护三级系统）
i) 是否合理设置安全域，绘制网络拓扑图，并保持更新。
j) 是否配置、调优网络系统的参数。
k) 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。
l) 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；应正确设置安全设备的接口参数和过滤规则。
m) 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。

n) 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，特殊紧急情况下应采取限制登录 IP、数字证书或动态口令认证、全程监控等措施，在操作完成后应及时关闭，并对维护过程进行监控并留存记录。
o) 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。
p) 是否禁止通过无线网络对交易业务网进行网络管理。
q) 计算机网络跳线是否整齐干净，跳线标识清晰。
r) 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。
s) 是否保持网络设备的可用性，及时维修、更换故障设备。
t) 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.1.5.2.14 系统安全管理

本项要求包括：

a) 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。
b) 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。
c) 是否安装系统的最新补丁程序，在安装系统补丁前，应首先充分评估并在测试环境中测试通过，并对重要文件进行备份后，方可实施系统补丁程序的安装；持续跟踪厂商提供的系统升级更新情况，应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。
d) 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。
e) 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。
f) 是否至少每月对运行日志和审计数据进行分析。
g) 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，权限设定应当遵循最小授权原则。（本项适用于：信息系统等级保护三级系统）
h) 是否定期进行漏洞扫描，对发现的系统安全漏洞及时进行修补：（本项适用于：定为信息系统等级保护三级系统的证券交易所交易系统、证券交易所通信系统、开放式基金登记结算系统、证券登记结算系统）
    1) 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；
    2) 实施漏洞扫描或漏洞修补前，应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；
    3) 漏洞扫描或漏洞修补后应进行验证测试，以保证系统的正常运行。
i) 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。（本项适用于：定为信息系统等级保护三级系统的证券交易所交易系统、证券交易所通信系统、开放式基金登记结算系统、证券登记结算系统）
j) 系统管理是否包括：
    1) 应保持系统的可用性，及时维修、更换故障设备和更新软件；
    2) 应负责应用系统、操作系统的参数配置、调优，编制文档并保持更新；
    3) 应定期对系统容量进行检查和评估，形成评估报告；
    4) 应负责管理系统和应用程序服务进程，并关闭与业务无关的服务；

5) 应定期检查应用系统、操作系统的用户、口令及权限设置的正确性。

k) 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。

l) 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.1.5.2.15 恶意代码防范

本项要求包括：

a) 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。

b) 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。

c) 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。

d) 是否定期检查信息系统内各种产品的恶意代码库的升级情况并进行记录，对主机防病毒产品、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及时分析处理，并形成书面的报表和总结汇报。（本项适用于：信息系统等级保护三级系统）

e) 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.1.5.2.16 密码管理

本项要求包括：

a) 是否使用符合国家密码管理规定的密码技术和产品。（本项适用于：信息系统等级保护二级系统）

b) 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。（本项适用于：信息系统等级保护三级系统）

A.1.5.2.17 备份与恢复管理

本项要求包括：

a) 是否识别需要定期备份的重要业务信息、系统数据及软件系统等。

b) 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。

c) 是否根据数据的重要性及其对系统运行的影响，制定数据的备份策略和恢复策略，备份策略指明备份数据的放置场所、文件命名规则、介质替换频率和数据离站运输方法。

d) 是否建立控制数据备份和恢复过程的程序，对备份过程进行记录，所有文件和记录应妥善保存。（本项适用于：信息系统等级保护三级系统）

e) 是否定期执行恢复程序，检查和测试备份介质的有效性，确保可以在恢复程序规定的时间内完成备份的恢复。（本项适用于：信息系统等级保护三级系统）

f) 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。

g) 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。

h) 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。

i) 2015 年底前，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。

j) 2015 年底前，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。
k) 2015 年底前，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。
l) 2015 年底前，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。
m) 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。
n) 在主用设备故障时，是否能实时切换到备份系统，自动隔离并保留故障设备以备事后调查。
o) 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。（本项适用于：信息系统等级保护三级系统）
p) 备份中心是否能够同时支持会员单位备份系统的接入。
q) 是否制定信息系统备份能力建设工作计划。
r) 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。

A.1.5.2.18 事件与问题管理

本项要求包括：

a) 是否对安全检查情况进行评估，形成评估报告。
b) 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。
c) 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。
d) 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。
e) 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。
f) 是否每月回顾、分析事件处理记录，完成事件分析报告。
g) 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。
h) 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。
i) 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。
j) 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。
k) 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。

A.1.5.2.19 网站安全

本项要求包括：

a) 是否对网站内容进行 24 小时实时监控。
b) 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。
c) 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。

A.1.5.2.20 软件正版化

本项要求包括：

a) 是否明确部门或责任人，负责本单位软件正版化工作。
b) 是否落实软件采购经费，做好软件正版化工作。
c) 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。

d) 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。
e) 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。
f) 是否每年对软件正版化情况开展自查。
g) 操作系统软件是否有授权（服务器）。
h) 操作系统是否有授权（办公计算机）。
i) 数据库软件是否有授权。
j) 杀毒软件是否有授权。
k) 办公文字处理软件是否有授权。
l) 办公专业处理软件是否有授权。
m) 应用服务器软件是否有授权。
n) 专用业务软件是否有授权。
o) 是否制定了软件正版化计划。

A.1.5.3 应急处置

A.1.5.3.1 应急准备

本项要求包括：

a) 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。
b) 是否对系统相关的人员进行应急预案培训，应急预案的培训应至少每年举办一次。
c) 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。（本项适用于：信息系统等级保护三级系统）
d) 是否定期对应急预案进行演练，根据不同的应急恢复内容，确定演练的周期；应至少每年对应急预案进行演练。（本项适用于：信息系统等级保护三级系统）
e) 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。（本项适用于：信息系统等级保护三级系统）
f) 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。（本项适用于：信息系统等级保护三级系统）（本项适用于：定为信息系统等级保护三级系统的证券交易所交易系统、证券交易所通信系统、开放式基金登记结算系统、证券登记结算系统）
g) 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。
h) 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。
i) 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。
j) 是否制定了网络与信息安全事件应急预案，内容至少包括：
    1) 应急预案编制的目的和依据；
    2) 应急预案的适用范围；
    3) 应急处置的组织体系及职责；
    4) 预防措施、保障措施与应急准备；
    5) 预警监测、处置和信息报送；
    6) 网络与信息安全事件的分级分类；

7） 网络与信息安全事件的报告流程；
8） 网络与信息安全事件处置的一般原则；
9） 网络与信息安全事件处置的具体方案；
10） 网络与信息安全事件内部调查处理以及分析总结的要求。

k） 应急预案是否符合如下要求：
1） 网络与信息安全事件处置的具体方案应包括各种可能发生的技术故障的应急处置流程、报告流程等；
2） 应针对各种技术故障拟定统一的解释口径和通知公告模板；
3） 应每年至少进行一次评估，并及时修订；
4） 应根据应急演练的情况进行评估和更新；
5） 应向证信办报备；
6） 在应急预案发生重大变化时，应及时重新报备。

l） 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。

m） 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。

n） 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。

o） 是否建立有效的应急通讯联络系统，确保信息畅通。

p） 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。

q） 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。

r） 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。

s） 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。

t） 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。

u） 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。

v） 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。

w） 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。

x） 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。

y） 是否每半年至少组织一次网络与信息安全应急演练。

z） 是否记录演练情况，演练记录至少保存两年。

aa） 是否对演练中发现的问题进行改进。

bb） 是否每年向证信办报告年度应急演练情况。

cc） 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。

dd) 交易所对集中交易系统存在安全隐患、可能引发行业技术风险的证券公司是否予以警告、限期整改以及取消其集中交易通道等处置，并报备中国证券业协会及证信办。（本项适用于：证券交易所）

A.1.5.3.2 应急处置

本项要求包括：

a) 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。
b) 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。
c) 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。
d) 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。
e) 是否记录并保存所有报告的安全弱点和可疑事件，分析事件原因，监督事态发展，采取措施避免安全事件发生。（本项适用于：信息系统等级保护二级系统）
f) 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。（本项适用于：信息系统等级保护三级系统）
g) 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。（本项适用于：信息系统等级保护三级系统）
h) 是否做好应急处置的相关记录，保留有关证据。
i) 是否对造成系统中断和造成信息泄密的安全事件应采用不同的处理程序和报告程序。（本项适用于：信息系统等级保护三级系统）
j) 是否对证券期货行业内通报的重大安全隐患，应立即进行专项安全检查。
k) 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。
l) 是否在应急处置中注意保证工作人员的人身安全。
m) 是否在应急处置结束前，保证专人 24 小时值班。
n) 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。
o) 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。

A.1.5.3.3 调查处理

本项要求包括：

a) 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。事件总结报告内容应当包括：
   1) 事件基本情况，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；
   2) 应急处置情况，包括事件报告的情况、采取的措施及效果；
   3) 事件调查情况，包括事件原因、事件级别、责任认定和结论；
   4) 事件处理情况，包括事件暴露出的问题及采取的整改措施，责任追究情况。

b) 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。
c) 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。
d) 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。
e) 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。
f) 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。
g) 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.2 证券公司系统运行安全审计项汇总

A.2.1 组织管理

A.2.1.1 安全管理制度

A.2.1.1.1 管理制度

本项要求包括：
a) 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。
b) 是否建立安全管理制度，覆盖安全策略的制定、实施、检查、评估、改进等全过程。
c) 是否形成由安全策略、管理制度、操作规程等构成的全面的信息安全管理制度体系。（本项适用于：信息系统等级保护三级系统）
d) 是否对安全管理人员或操作人员执行的日常管理操作建立操作规程。
e) 是否制定覆盖运维工作各个环节的、体系化的运维管理制度和操作流程。运维管理制度包括但不限于：机房管理、网络与系统管理、数据和介质管理、交付管理、测试管理、配置管理、安全管理、值班管理、监控管理、文档管理、设备和软件管理、供应商管理、关联单位关系管理、检查审计等制度。运维操作流程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。
f) 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。

A.2.1.1.2 制定和发布

本项要求包括：
a) 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。
b) 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。
c) 安全管理制度是否具有统一的格式，并进行版本控制。（本项适用于：信息系统等级保护三级系统）
d) 是否建立信息发布管理审核制度；安全管理制度是否通过正式、有效的方式发布。
e) 安全管理制度是否注明发布范围，并对收发文进行登记。（本项适用于：信息系统等级保护三级系统）

A.2.1.1.3 评审和修订

本项要求包括：

a) 信息安全领导小组是否负责定期组织相关部门和相关人员对安全管理制度体系的合理性和适用性进行审定；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。（本项适用于：信息系统等级保护三级系统）

b) 是否定期或不定期对安全管理制度进行检查和审定，对存在不足或需要改进的安全管理制度进行修订。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。

c) 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.2.1.2 安全管理机构

A.2.1.2.1 机构设置

本项要求包括：

a) 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。

b) 是否设立 IT 治理委员会或类似机构，负责公司 IT 治理工作。

c) IT 治理委员是否包括公司 IT 治理直接责任人、IT 总监、IT 部门负责人、相关业务负责人、财务负责人、内部控制负责人以及部分技术骨干等人员，其中 IT 人员的比例是否在 30%以上。

d) IT 治理委员会是否履行以下职责：

1) 拟订公司 IT 治理目标和 IT 治理工作计划；
2) 审议公司 IT 发展规划；
3) 审议公司年度 IT 工作计划和 IT 预算；
4) 审议公司重大 IT 项目立项、投入和优先级；
5) 审议公司 IT 管理制度和重要流程；
6) 制订与 IT 治理相关的培训和教育工作计划；
7) 检查所拟订和审议事项的落实和执行情况；
8) 组织评估公司 IT 重大事项并提出处置意见；
9) 向公司管理层报告 IT 治理状况。

e) 是否建立集中交易运营管理组织，负责集中交易系统的运行和管理。

A.2.1.2.2 岗位设置

本项要求包括：

a) 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。

b) 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。

c) 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。（本项适用于：信息系统等级保护三级系统）

d) 是否合理设置运维岗位，规定岗位职责及技能要求，并符合如下要求：

1) 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；
2) 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。

e) 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。

f) 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。
g) 是否实现集中交易业务运作与技术支持之间的相互隔离，电脑人员、会计人员之间及与其他业务人员之间职责不得相互交叉。
h) 开展集中交易的证券公司是否实现前台业务操作、中台业务管理以及后台业务支持三者之间的隔离。

A.2.1.2.3 人员配备

本项要求包括：

a) 是否配备系统管理员、网络管理员、安全管理员等；每个岗位应有备岗。
b) 安全管理员是否禁止兼任网络管理员、系统管理员、数据库管理员。（本项适用于：信息系统等级保护二级系统）
c) 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。
d) 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。
e) 关键事务岗位是否配备多人共同管理。（本项适用于：信息系统等级保护三级系统）
f) 公司是否配备足够的信息技术人员，公司的 IT 工作人员总数不少于公司员工总人数的 6%。
g) 核心网络的管理是否设置专职、双岗网络管理员，实行网络分级管理；网络管理员应具备相应的素质和技能，持有相应的资格证书。
h) 是否有应急技术支援队伍。
i) 第三方存管系统安全稳定运行的第一责任人是否为总部主要负责人。
j) 是否指定专门的技术联络员，具体负责与监管机构、技术协调小组、第三方存管相关参与方之间的对口联络。
k) A 型证券营业部是否至少配备一名专职技术人员；B 型证券营业部是否至少配备一名兼职技术人员；营业部是否制定顶岗、备岗等相关制度，确保在交易时间内有技术人员值守；专职技术人员和兼职技术人员是否具有计算机相关专业学历或从事信息技术工作 1 年以上。

A.2.1.2.4 授权和审批

本项要求包括：

a) 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。
b) 是否针对关键活动建立审批流程，并由批准人签字确认。（本项适用于：信息系统等级保护二级系统）
c) 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。（本项适用于：信息系统等级保护三级系统）
d) 是否定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息；每年至少审查一次审批事项。（本项适用于：信息系统等级保护三级系统）
e) 是否记录审批过程并保存审批文档。（本项适用于：信息系统等级保护三级系统）
f) 权限分配是否有审批和完整的记录，权限设置后应复核。
g) 是否按照最小安全访问原则分配用户权限。
h) 是否建立权限分配表，对用户的访问权限进行合理分配，对文件系统访问权限进行合理设置，编制文档并保持更新。
i) 是否在用户账户变化时，同时变更或撤销其权限。
j) 是否定期检查权限设置的有效性。

k) 对集中交易系统中的前瞻性功能，若确需做技术模拟和前期准备的，是否建立和实施严格的内部审批程序，技术上须具备禁止启用手段，并由内部稽核部门实行严密监控。
l) 集中交易系统安全管理是否在系统管理和业务操作的各层面建立相应的操作权限制约机制：
   1) 实行权限集中管理，统一授权；
   2) 在权限体系中支持前台业务操作、中台业务管理与后台业务支持的分离。
m) 是否禁止开发、测试和运营人员未经授权访问、修改非职责范围内的网上证券信息系统。

A.2.1.2.5 供应商管理

本项要求包括：

a) 是否确保安全服务商的选择符合国家、行业的有关规定。
b) 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。
c) 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。
d) 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。
e) 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。
f) 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，明确供应商应接受证券期货行业监管部门的信息安全延伸检查。
g) 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。
h) 是否加强运维外包服务管理，主要包括：
   1) 与外包公司及外包人员签订保密协议；
   2) 明确外包公司应当承担的责任及追究方式；
   3) 明确界定外包人员的工作职责、活动范围、操作权限；
   4) 对外包人员工作情况进行监督和检查，并保留相应记录；
   5) 对驻场外包人员的入场和离场进行管理；
   6) 定期评估外包的服务质量；制定外包服务意外终止的应急措施。
i) 是否建立产品提供、系统开发和运营服务厂商的退出机制，以保障其退出之后集中交易系统的持续运行和系统重要数据的安全。
j) 根据需要可外包 B 型和 C 型证券营业部的信息系统运维工作。运维外包是否满足但不限于以下要求：
   1) B 型证券营业部至少配备一名兼职技术人员，并制定顶岗、备岗等相关制度，确保在交易时间内有技术人员值守。专职技术人员和兼职技术人员应具有计算机相关专业学历或从事信息技术工作 1 年以上。
   2) 与外包服务提供单位签订外包合同与保密协议，确保信息系统安全运行、风险可控。
   3) 不得授予外包人员业务系统操作权限。

A.2.1.2.6 关联单位关系管理

本项要求包括：

a) 是否加强各类管理人员之间、组织内部机构之间以及信息安全职能部门内部的合作与沟通。（本项适用于：信息系统等级保护二级系统）

b) 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。
c) 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。（本项适用于：信息系统等级保护三级系统）
d) 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。（本项适用于：信息系统等级保护三级系统）
e) 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。（本项适用于：信息系统等级保护三级系统）
f) 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。
g) 各参与方需要进行第三方存管系统联调或升级时，是否提前至少 5 个工作日通知相关参与方。
h) 各参与方对第三方存管系统提出重大的新业务或管理需求时，是否为相关参与方留有充足的技术准备时间，原则上不少于 30 个工作日。
i) 各相关参与方之间是否相互提供与第三方存管系统相关的信息，包括但不限于：广域网接入设备及端口类型、相关网络拓扑结构及必要参数、主机类型与配置、相关系统参数、技术接口协议、系统运行性能测试报告、主要应急预案及相关联系人等。
j) 是否在对相关网络及设备做重大变更时提前告知相关参与方，以免对方运行监控人采取不必要的操作。
k) 如涉及第三方（指除证券公司及其客户以外的任何一方），是否与第三方签订保密协议和服务级别协议，并明确责任，采取措施（如第三方维护时只提供临时密码等）防止通过第三方泄露用户信息。

A.2.1.2.7 客户关系管理

本项要求包括：

a) 是否在与客户签订的服务合同、经纪合同及补充协议、风险揭示书等中载明，客户使用网上交易可能面临的风险、公司采取的风险控制措施、客户应采取的风险控制措施以及相关风险对应的责任承担（如防止用于网上交易的计算机或手机终端感染木马、病毒，以免被恶意程序窃取口令；加强帐号、口令的保护，不使用简单口令、定期修改口令、输入口令时防止他人偷看、不对他人泄露口令等）。
b) 是否在门户网站或固定营业场所公告短信服务号码、移动证券门户网站地址等信息，提醒客户防范他人利用移动通讯设备进行欺诈。
c) 是否根据移动证券业务的网络延迟时间、链路稳定状况、信号衰减程度等风险因素，对行情或交易数据可能出现明显滞后或产生数据丢失的情况，事先对客户进行风险提示。
d) 是否尽可能使用统一的网上证券服务电话、域名、短信号码等，并应在与投资者签订的协议或合同中明确告知客户使用网上证券信息系统的合法途径、意外事件的处理办法，以及证券公司联系方式等。
e) 是否根据投资者需要开启或关闭网上交易方式。

A.2.1.2.8 审核和检查

本项要求包括：

a) 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。安全检查应至少每季度一次。
b) 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；全面安全检查应至少每年一次。（本项适用于：信息系统等级保护三级系统）
c) 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。（本项适用于：信息系统等级保护三级系统）
d) 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。（本项适用于：信息系统等级保护三级系统）

A.2.1.3 经费和人员管理

A.2.1.3.1 经费投入

本项要求包括：

a) 最近三个财政年度IT投入平均数额是否不少于最近三个财政年度平均净利润的6%或不少于最近三个财政年度平均营业收入的3%，取二者数额较大者。
b) 是否制定信息系统运行维护年度预算计划，每年进行核算。预算和核算应接受监督和审计。
c) 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。
d) 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。

A.2.1.3.2 人员录用

本项要求包括：

a) 是否指定或授权专门的部门或人员负责人员录用。
b) 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。
c) 是否与开发、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。
d) 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。（本项适用于：信息系统等级保护三级系统）

A.2.1.3.3 人员离岗

本项要求包括：

a) 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。
b) 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。
c) 是否办理严格的调离手续。（本项适用于：信息系统等级保护二级系统）
d) 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。（本项适用于：信息系统等级保护三级系统）

A.2.1.3.4 人员考核

本项要求包括：

a) 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应至少每年一次。
b) 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。（本项适用于：信息系统等级保护三级系统）
c) 是否对考核结果进行记录并保存。（本项适用于：信息系统等级保护三级系统）

A.2.1.3.5 教育和培训

本项要求包括：

a) 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。
b) 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。
c) 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。
d) 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。（本项适用于：信息系统等级保护三级系统）
e) 对各重要岗位的人员上岗是否有相应的资质要求和必要的上岗培训，对重要岗位人员建立轮岗制度和定期培训制度。

A.2.1.3.6 外部人员访问管理

本项要求包括：

a) 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。
b) 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。（本项适用于：信息系统等级保护三级系统）

A.2.2 机房管理

A.2.2.1 基础保障

A.2.2.1.1 物理位置的选择

本项要求包括：

a) 机房和办公场地是否选择具有防震、防风和防雨等能力的建筑：
   1) 应具有机房或机房所在建筑物符合当地抗震要求的相关证明；
   2) 机房外墙壁应没有对外的窗户。否则，应采用双层固定窗，并作密封、防水处理。
b) 机房场地是否避免设在建筑物的高层或地下室，以及用水设备的下层或隔壁：（本项适用于：信息系统等级保护三级系统）
   1) 机房场地不宜设在建筑物顶层，如果不可避免，应采取有效的防水措施。机房场地设在建筑物地下室的，应采取有效的防水措施；
   2) 机房场地设在建筑物高层的，应对设备采取有效固定措施；
   3) 如果机房周围有用水设备，应当有防渗水和疏导措施。
c) 证券营业部机房选址是否远离产生粉尘、油烟、有害气体以及具有腐蚀性、易燃、易爆物品的工厂、仓库等场所。

A.2.2.1.2 防雷击

本项要求包括：

a) 机房或机房所在大楼，是否设计并安装防雷击措施，防雷措施应至少包括避雷针或避雷器等。
b) 机房是否设置交流电源地线。
c) 是否设置防雷保安器，防止感应雷。（本项适用于：信息系统等级保护三级系统）

A.2.2.1.3 防火

本项要求包括：

a) 机房是否设置灭火设备和火灾自动报警系统。机房的火灾自动报警系统应向当地公安消防部门备案。（本项适用于：信息系统等级保护二级系统）
b) 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应向当地公安消防部门备案。（本项适用于：信息系统等级保护三级系统）
c) 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。（本项适用于：信息系统等级保护三级系统）
d) 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。（本项适用于：信息系统等级保护三级系统）

A.2.2.1.4 防水和防潮

本项要求包括：

a) 水管安装，是否穿过机房屋顶和活动地板下；
   1) 与机房设备无关的水管不得穿过机房屋顶和活动地板下；
   2) 机房屋顶和活动地板下铺有水管的，应采取有效防护措施。
b) 是否采取措施防止雨水通过机房窗户、屋顶和墙壁渗透。
c) 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。
d) 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。（本项适用于：信息系统等级保护三级系统）

A.2.2.1.5 防静电

本项要求包括：

a) 关键设备应采用必要的接地防静电措施。（本项适用于：信息系统等级保护二级系统）
b) 主要设备是否采用必要的接地防静电措施。（本项适用于：信息系统等级保护三级系统）
c) 机房是否采用防静电地板。（本项适用于：信息系统等级保护三级系统）

A.2.2.1.6 空调

本项要求包括：

a) 机房是否设置温、湿度自动调节设施，使机房温、湿度的变化在设备运行所允许的范围之内：
   1) 开机时机房温度应控制在22℃-24℃；
   2) 开机时机房相对湿度应控制在40%-55%。
b) 是否安装独立的空调设备。
c) 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。
d) 证券营业部机房是否具备独立空调系统，使机房温度保持在23℃±5℃范围内。

A.2.2.1.7 电力供应

本项要求包括：

a) 是否在机房供电线路上配置稳压器和过电压防护设备。
b) 是否提供短期的备用电力供应，至少满足主要设备在断电情况下的正常运行要求。
   1) 机房应配备 UPS，UPS 实际供电能力能够满足主要设备在断电情况下正常运行 2 个小时以上；
   2) 机房应自备或租用发电机，能够保障持续供电。
c) 是否采用双路市电，双路市电应能实现自动切换。（本项适用于：信息系统等级保护三级系统）
d) 机房是否配备单独的配电柜。
e) 机房是否有独立于一般照明电的专用供配电线路。
f) 是否配置 UPS 电源，并不得将与业务无关的设备接入 UPS 电源。市电插座与 UPS 插座应严格区分，插座面板应有提示性的标识或标签。
g) A 型和 B 型证券营业部是否至少配备一种持续供电方式，在市电中断情况下，保证不低于 25%的现场交易终端或同等支持能力的其他交易终端在交易时间内持续工作，满足证券营业部客户现场交易需要。

A.2.2.1.8 电磁防护

本项要求包括：
a) 电源线和通信线缆是否隔离铺设，避免互相干扰。电源线和通信线缆应铺设在不同的桥架或管道，避免互相干扰。
b) 是否采用接地方式防止外界电磁干扰和设备寄生耦合干扰：（本项适用于：信息系统等级保护三级系统）
   1) 机房或机房所在的大楼必须有接地措施，并且接地电阻必须小于 1 欧姆；
   2) 机房验收报告应提供合格的检测结果。
c) 是否对关键设备和磁介质实施电磁屏蔽。（本项适用于：信息系统等级保护三级系统）

A.2.2.2 机房运维

A.2.2.2.1 物理访问控制

本项要求包括：
a) 机房出入口是否安排专人值守，控制、鉴别和记录进入的人员；
   1) 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；
   2) 没有门禁系统的机房，应当安排专人控制、鉴别和记录人员的进出；
   3) 有门禁系统的机房，应当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。
b) 需进入机房的来访人员是否经过申请和审批流程，并限制和监控其活动范围；
   1) 来访人员进入机房，应有审批流程，记录带进带出的设备、进出时间、工作内容，并有专人陪同其在限定的范围内工作；
   2) 机房出入口应有视频监控，监控记录至少保存 3 个月。
c) 是否对机房划分区域进行管理，区域和区域之间设置物理隔离装置，在重要区域前设置交付或安装等过渡区域：（本项适用于：信息系统等级保护三级系统）
   1) 机房应当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；
   2) 机房应当设置专门的过渡区域，用于设备的交付或安装；
   3) 重要区域包括：主机房、辅助区、支持区等功能区域。
d) 操作间与设备间是否分隔。

A.2.2.2.2 防盗窃和防破坏

本项要求包括：

a) 是否将主要设备放置在机房内。
b) 是否将设备或主要部件进行固定，并设置明显的不易除去的标记；
   1) 主要设备应当安装、固定在机柜内或机架上；
   2) 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。
c) 是否将通信线缆铺设在隐蔽处，可铺设在地下或管道中；通信线缆可铺设在管道或线槽、线架中。
d) 是否对介质分类标识，存储在介质库或档案室中。
e) 主机房应安装必要的防盗报警设施。（本项适用于：信息系统等级保护二级系统）
f) 是否利用光、电等技术设置机房防盗报警系统。（本项适用于：信息系统等级保护三级系统）
g) 是否对机房设置监控报警系统：（本项适用于：信息系统等级保护三级系统）
   1) 应至少对机房的出入口、操作台等区域进行摄像监控；
   2) 监控录像记录至少保存 3 个月。

A.2.2.2.3 机房管理

本项要求包括：

a) 是否指定专门的部门或人员定期对机房供配电、空调、温湿度控制等设施进行维护管理；
   1) 应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；
   2) 应每年对防盗报警、防雷、消防等装置进行检测维护并保存相关维护记录。
b) 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。
c) 是否加强对办公环境的保密性管理，包括工作人员调离办公室应立即交还该办公室钥匙和不在办公区接待来访人员等。（本项适用于：信息系统等级保护二级系统）
d) 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。
e) 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。（本项适用于：信息系统等级保护三级系统）
f) 是否指定机房管理负责人。
g) 是否确保机房环境整洁和安全，包括：
   1) 应定期检查防水、防雷、防火、防潮、防尘、防鼠、防静电、防电磁辐射等措施的有效性；
   2) 应保持机房环境卫生，采取防尘措施，定期进行除尘处理；
   3) 交易时间内不得进行机房施工、保洁操作。
h) 是否对设备和人员出入进行严格管理，包括：
   1) 应指定人员负责控制、鉴别和记录设备和人员的进出情况，记录进出人员、进出时间、工作内容，并留存记录至少 90 天；
   2) 机房出入口的监控录像至少保存 90 天；
   3) 外来人员进入机房应经过申请和审批流程，并限制和监控其活动范围，并有专人陪同；
   4) 外来设备未经批准不得接入生产环境。

A.2.2.2.4 用电安全

本项要求包括：

a) 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。
b) 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。
c) 是否在危险性高的位置张贴相应的用电安全操作方法、警示及指引。
d) 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。
e) 未经审批是否禁止接入其他用电设备。

A.2.2.2.5 机房消防

本项要求包括：

a) 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。
b) 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。
c) 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。
d) 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。
e) 是否定期进行消防设施的使用培训和演习。

A.2.3 网络管理

A.2.3.1 网络安全

A.2.3.1.1 结构安全

本项要求包括：

a) 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%。
b) 是否保证接入网络和核心网络的带宽满足业务高峰期需要。（本项适用于：信息系统等级保护二级系统）
c) 是否保证网络各个部分的带宽满足业务高峰期需要。（本项适用于：信息系统等级保护三级系统）
d) 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。（本项适用于：信息系统等级保护三级系统）
e) 是否绘制与当前运行情况相符的网络拓扑结构图；应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。
f) 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。
g) 是否提供关键网络设备、通信线路和数据处理系统的硬件冗余，保证系统的可用性。（本项适用于：信息系统等级保护二级系统）
h) 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，重要网段与其他网段之间采取可靠的技术隔离手段。（本项适用于：信息系统等级保护三级系统）

i) 是否按照对业务服务的重要次序来指定带宽分配优先级别，保证在网络发生拥堵的时候优先保护重要主机。应对所有业务确定重要性、优先级，制定业务相关带宽分配原则及相应的带宽控制策略，根据安全需求，采取网络 QoS 或专用带宽管理设备等措施。（本项适用于：信息系统等级保护三级系统）

j) 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。（本项适用于：信息系统等级保护三级系统）

k) 网上信息系统是否具备 2 个或 2 个以上的不同运营商的互联网接入。

l) 集中交易通信系统是否达到以下要求：中心机房与交易所的通信连接应做到地面线路和卫星通信相互备份，与中国证券登记结算公司的通信连接应有备份线路。

m) 集中交易通信系统是否达到以下要求：公司中心机房和各分支机构之间应建立多条、不同运营商、不同介质的通信通道（如 DDN、帧中继、卫星等），保证业务的连续性。

n) 主通信线路的带宽是否考虑充分的冗余，本地局域网的网络时延应小于 50ms。中介服务机构与其他参与方之间的通信线路，应根据承载的通信量保证足够的带宽。

o) 与证券营业部之间是否采用至少 2 条不同运营商或不同介质的通信线路，建立安全、可靠通信连接，且线路带宽能够满足证券营业部业务需要并留有冗余。网络通信设备应有冗余备份，保证发生故障时实现及时切换。

p) A 型和 B 型证券营业部的通信线路中是否有一条为地面数据专线。

q) 是否确保 A 型和 B 型证券营业部提供至少 2 种相互独立的行情揭示系统、委托方式。

A.2.3.1.2 访问控制

本项要求包括：

a) 网络边界是否部署访问控制设备并启用访问控制功能。

b) 是否针对数据流提供明确的允许/拒绝访问的访问控制策略，控制力度达到网段级。网络边界访问控制设备应设定过滤规则集。规则集应涵盖对所有出入边界的数据包的处理方式，对于没有明确定义的数据包，应缺省拒绝。（本项适用于：信息系统等级保护二级系统）

c) 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。（本项适用于：信息系统等级保护三级系统）

d) 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。

e) 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。

f) 是否对进出网络的信息内容进行过滤，实现对应用层 HTTP、FTP、TELNET、SMTP、POP3 等协议命令级的控制；对通过互联网传输的信息内容进行过滤，实现对应用层 HTTP、FTP、TELNET、SMTP、POP3 等通用性协议命令级控制。（本项适用于：信息系统等级保护三级系统）

g) 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。（本项适用于：信息系统等级保护三级系统）

h) 是否限制网络最大流量数及网络连接数。（本项适用于：信息系统等级保护三级系统）

i) 重要网段是否采取技术手段防止地址欺骗。（本项适用于：信息系统等级保护三级系统）

j) 是否制定网络访问控制策略，应合理设置网络隔离设施上的访问控制列表，关闭与业务无关的端口；编制文档并保持更新；访问控制策略的变更应履行审批手续。

k) 所有可配置的网络设备是否按最小安全访问原则设置访问控制权限，关闭不必要的端口及服务，妥善保管和定期更换网络设备的远程访问口令。

l) 对于来自互联网的访问是否采用可靠的身份认证、访问控制和安全审计措施，防止非法接入和非法访问。

m) 是否加强证券营业部网络配置、访问控制、安全审计等网络管理，确保证券营业部的网络设备按最小安全访问原则设置访问控制权限，每一次变更后及时更新备份网络设备的配置信息。

A.2.3.1.3 安全审计

本项要求包括：

a) 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) 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。

c) 是否能够根据记录数据进行分析，并生成审计报表。（本项适用于：信息系统等级保护三级系统）

d) 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。（本项适用于：信息系统等级保护三级系统）

e) 是否定期检查网络设备的用户、口令及权限设置的正确性。

f) 是否留存网络访问日志。

A.2.3.1.4 边界完整性检查

本项要求包括：

a) 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，准确定出位置，并对其进行有效阻断。（本项适用于：信息系统等级保护二级系统）

b) 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。（本项适用于：信息系统等级保护三级系统）

c) 是否能够对内部网络用户私自联到外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。（本项适用于：信息系统等级保护三级系统）

d) 是否定期检查安全隔离情况，确保各安全域之间有效隔离。

e) 是否确保证券营业部局域网与公司广域网、互联网实现有效隔离。

A.2.3.1.5 入侵防范

本项要求包括：

a) 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。

b) 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应提供报警。（本项适用于：信息系统等级保护三级系统）

A.2.3.1.6 恶意代码防范

本项要求包括：

a) 是否在网络边界处对恶意代码进行检测和清除：（本项适用于：信息系统等级保护三级系统）

   1) 在不严重影响网络性能和业务的情况下，应在网络边界部署恶意代码检测系统；

   2) 如果部署了主机恶意代码检测系统，可选择安装部署网络边界恶意代码检测系统。

b) 是否维护恶意代码库的升级和检测系统的更新。（本项适用于：信息系统等级保护三级系统）

A.2.3.1.7 网络设备防护

本项要求包括：

a) 是否对登录网络设备的用户进行身份鉴别；应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。
b) 是否对网络设备的管理员登录地址进行限制。
c) 网络设备用户的标识是否唯一。
d) 身份鉴别信息是否具有不易被冒用的特点，口令是否有复杂度要求并定期更换；
   1) 口令应符合以下条件：数字、字母、符号混排，无规律的方式；
   2) 管理员用户口令的长度至少为 12 位；
   3) 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；
   4) 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。
e) 是否具有登录失败处理功能，是否采取结束会话、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。
f) 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。
g) 主要网络设备是否对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别：（本项适用于：信息系统等级保护三级系统）
   1) 通过本地控制台管理主要网络设备时，应采用一种或一种以上身份鉴别技术；
   2) 以远程方式登录主要网络设备，应采用两种或两种以上组合的鉴别技术进行身份鉴别。
h) 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。（本项适用于：信息系统等级保护三级系统）

A.2.4 主机和系统管理

A.2.4.1 主机安全

A.2.4.1.1 身份鉴别

本项要求包括：

a) 是否对登录操作系统和数据库系统的用户进行身份标识和鉴别。
b) 操作系统和数据库系统管理用户身份标识是否具有不易被冒用的特点，口令应有复杂度要求并定期更换；
   1) 口令应符合以下条件：数字、字母、符号混排，无规律的方式；
   2) 口令的长度至少为 12 位；
   3) 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；
   4) 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。
c) 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。
d) 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。
e) 是否为操作系统和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：
   1) 应为操作系统的不同用户分配不同的用户名；
   2) 应为数据库系统的不同用户分配不同的用户名。
f) 是否采用两种或两种以上组合的鉴别技术对管理用户进行身份鉴别：（本项适用于：信息系统等级保护三级系统）

1) 通过本地控制台管理主机设备时，应采用一种或一种以上身份鉴别技术；
2) 以远程方式登录主机设备，应采用两种或两种以上组合的鉴别技术进行身份鉴别。

A.2.4.1.2 访问控制

本项要求包括：

a) 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。
b) 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。
c) 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。
   1) 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；
   2) 系统无法重命名的特殊默认账户，可不重命名。
d) 是否及时删除多余的、过期的账户，避免共享账户的存在。
e) 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。（本项适用于：信息系统等级保护三级系统）

A.2.4.1.3 安全审计

本项要求包括：

a) 审计范围是否覆盖到服务器上的每个操作系统用户和数据库用户;应在保证系统运行安全和效率的前提，启用系统审计或采用第三方安全审计产品实现审计要求。（本项适用于：信息系统等级保护二级系统）
b) 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。
c) 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。
d) 是否保护审计记录，避免受到未预期的删除、修改或覆盖等。审计记录应至少保存 6 个月。
e) 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和数据库用户;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。（本项适用于：信息系统等级保护三级系统）
f) 是否能够根据记录数据进行分析，并生成审计报表。（本项适用于：信息系统等级保护三级系统）
g) 是否保护审计进程，避免受到未预期的中断。（本项适用于：信息系统等级保护三级系统）
h) 集中交易系统是否具有完备的操作日志和错误报告。

A.2.4.1.4 入侵防范

本项要求包括：

a) 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，应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。
b) 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。（本项适用于：信息系统等级保护三级系统）
c) 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，应停止有关服务，并提供报警。（本项适用于：信息系统等级保护三级系统）

A.2.4.1.5 恶意代码防范

本项要求包括：

a) 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；
   1) 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；
   2) 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。
b) 是否支持防恶意代码软件的统一管理。
c) 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。（本项适用于：信息系统等级保护三级系统）

A.2.4.1.6 资源控制

本项要求包括：

a) 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。
b) 是否根据安全策略设置登录终端的操作超时锁定。
c) 是否限制单个用户对系统资源的最大或最小使用限度。
d) 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。（本项适用于：信息系统等级保护三级系统）
e) 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。（本项适用于：信息系统等级保护三级系统）

A.2.4.2 应用安全

A.2.4.2.1 结构安全

本项要求包括：

a) 集中交易系统的重要环节是否采取冗余备份措施，如报盘系统、重要的数据库服务器和中间件服务器等。
b) 集中交易系统是否保证系统的可扩展性与可维护性。
c) 集中交易系统是否具有动态加载、卸载功能，具有实现系统不停机维护的能力。
d) 集中交易系统是否在系统构架上支持前台操作与后台数据的分离。
e) 灾难备份中心与交易所之间的通信连接是否符合交易所的接入管理要求与技术标准；灾难备份中心与中心机房之间的通信连接除主用线路外、是否有备用线路；灾难备份中心与各分支机构之间是否建立通信连接。
f) 灾难备份中心的交易系统是否有足够的处理能力，确保届时能完全承担交易、清算及交收业务。
g) 网上信息系统服务端是否存在有效屏蔽系统技术错误信息的机制，不将系统产生的错误信息直接反馈给客户。
h) 与相关商业银行之间的第三方存管系统对接是否遵循总对总的原则，联接线路既可以采用银证直联，也可以通过相关中介服务机构进行联接。
i) 第三方存管系统的日处理能力是否达到最近一年内银证转账最大日处理量的5倍以上。
j) 各参与方是否在其第三方存管系统内部实现有效隔离，以确保与不同业务对象之间的业务和数据不会发生相互影响。
k) 第三方存管系统全年实际可用性是否达到99.9%，单次故障停机时间是否不超过60分钟。
l) 各参与方第三方存管系统的前置机、加密设备、网络设备等硬件设备是否有冗余备份，当出现故障时，是否能在30分钟内完成备用设备的切换。

m) 是否部署有效的网上证券信息系统安全防护与监控子系统，包括防火墙，防病毒、防木马系统，入侵检测系统或入侵防护系统，并正确配置；是否加强相关系统的日志审查工作并根据实际情况及时调整，保证安全措施的持续有效。
n) 网上开展证券业务的网络系统、安全系统、应用系统等重要环节是否具备足够的冗余，以应对网站及网上交易可能出现的突发峰值。
o) 网上开展证券业务的网络系统、安全系统、应用系统等重要环节是否具备良好的可扩充性，以应对业务增长和市场的变化。
p) 网上证券信息系统各环节是否有可靠的热备或冷备措施，保证整个系统的高可用性。

A.2.4.2.2 身份鉴别

本项要求包括：
a) 是否提供专用的登录控制模块对登录用户进行身份标识和鉴别。
b) 是否提供用户身份标识唯一和鉴别信息复杂度检查功能，保证应用系统中不存在重复用户身份标识，身份鉴别信息不易被冒用。
c) 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。
d) 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。
e) 是否对同一用户采用两种或两种以上组合的鉴别技术实现用户身份鉴别：（本项适用于：信息系统等级保护三级系统）
   1) 管理用户通过受控本地控制台管理应用系统时，应采用一种或一种以上身份鉴别技术；
   2) 管理用户以远程方式登录应用系统，应采用两种或两种以上组合的鉴别技术进行身份鉴别；
   3) 面向互联网服务的系统应当提供两种或两种以上组合的鉴别技术供用户选择。
f) 网上信息系统服务端是否能向客户提供可证明服务端自身身份的信息，如提供预留验证信息服务，在网上交易客户登录时回显，帮助客户有效识别仿冒的网上交易信息系统，防范利用仿冒的网上交易信息系统进行诈骗活动。
g) 网上信息系统是否提供可靠的身份验证机制，除采用账号名、口令、验证码的身份认证方式外，是否向客户提供一种以上强度更高的身份认证方式供客户选择使用，如客户端电脑或手机特征码绑定、软硬件证书、动态口令等认证方式，确认客户的身份和登录的合法性，防止不法分子利用木马等黑客程序窃取客户账号和口令。
h) 集中交易系统是否能防止强力试探口令，并具有超时自动锁定功能。
i) 网上信息系统客户端是否能向客户提示最近一次登录的日期、时间、地址等信息。
j) 是否根据自身系统的特点和需求，结合试点工作案例以及其他金融企业成熟做法，制定“网上交易强身份认证系统”实施方案（以下简称实施方案）。实施方案应包括但不限于：组织保障机制、系统技术架构、产品选型方案、业务管理及服务支持体系设计、应急处置措施、实施计划及进度安排等方面内容。

A.2.4.2.3 访问控制

本项要求包括：
a) 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、数据库表等客体的访问，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。
b) 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。

c) 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。
d) 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。
e) 核心系统是否有授权管理功能。
f) 集中交易系统是否防止异常中断后非法进入系统。
g) 集中交易系统是否建立工作站点与功能操作相关联的全面安全控制机制。
h) 是否关闭网上信息系统所有与业务和维护无关的服务及端口，严格控制防火墙中的权限设置，确保按“最小权限原则”进行设置。
i) 对于网上信息系统的内部访问，是否严格限制访问源。
j) 特殊紧急情况下需要通过互联网进行远程操作时，是否通过限制登录 IP、使用数字证书或动态口令、全程监控等措施确保安全，并在操作完成后，及时关闭相关端口。
k) A 型、B 型、C 型营业部是否确保证券营业部加强计算机终端的管理，记录网卡地址，防止非法使用。未经许可，不得将客户和员工的自备计算机接入证券营业部网络。证券营业部提供无线网络服务的，证券公司应统一制定证券营业部无线网络使用规范，采取有效的无线网络准入控制措施，登记并记录无线接入设备的信息。

A.2.4.2.4 安全审计

本项要求包括：

a) 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。
b) 是否采取有效措施防止删除、修改或覆盖审计记录。（本项适用于：信息系统等级保护二级系统）
c) 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。审计记录应至少保存 6 个月。
d) 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。（本项适用于：信息系统等级保护三级系统）
e) 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。（本项适用于：信息系统等级保护三级系统）
f) 集中交易系统是否提供系统运行状态监控模块。
g) 集中交易系统是否提供数据接口，满足稽核、审计及技术监控等的要求。
h) 网上证券服务端是否对不完整、被篡改、重发的数据包进行监控，对登录、委托方式、品种、价格、数量、操作频率、转账等异常行为进行跟踪、监控和限制，记录其账号、IP 地址等相关信息，并通过短信、电话等方式及时提示客户，必要时进行用户临时锁定。监控和处置情况应形成记录备查。

A.2.4.2.5 通信完整性

本项要求包括：

a) 通过互联网、卫星网进行通信时，是否采用校验码技术保证通信过程中数据的完整性。（本项适用于：信息系统等级保护二级系统）
b) 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。（本项适用于：信息系统等级保护三级系统）
c) 是否能够检测到鉴别信息和重要业务数据在传输过程中完整性受到破坏。（本项适用于：信息系统等级保护二级系统）

d) 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。（本项适用于：信息系统等级保护三级系统）
e) 集中交易系统是否具有防止数据的重发攻击、篡改和伪造等功能。

A.2.4.2.6 通信保密性

本项要求包括：
a) 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。
b) 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。
c) 集中交易系统业务数据在通信网络上是否以加密方式传输。
d) 在交换的数据中，客户资金密码、银行结算账户密码等重要信息是否加密，不得以明文方式交换。
e) 网上客户端的客户身份信息和交易数据等重要数据传输是否采用国家信息安全机构认可的加密技术和加密强度，并最低达到 SSL 协议 128 位的加密强度。
f) 加解密是否在投资者与证券公司实际控制的设备中进行，不得存在任何中间环节对数据进行加解密。
g) 移动证券系统是否自主运营，实现数据从用户终端到网上证券服务端之间的加密传送和控制，并随着技术的发展，不断提高加密强度，完善认证算法。
h) 移动证券客户端是否具备一定加密强度的用户认证功能，保护客户账号和口令信息。
i) 门户网站中客户账号及口令，是否采用加密方式传输，并最低达到 SSL 协议 128 位的加密强度。

A.2.4.2.7 抗抵赖

本项要求包括：
a) 是否具有在请求的情况下为数据原发者或接收者提供数据原发证据的功能；应用系统的操作与管理记录，至少应记录操作时间、操作人员及操作类型、操作内容等信息。交易系统应能够记录用户交易行为数据，至少包括业务流水号、账户名、IP 地址、交易指令等信息。（本项适用于：信息系统等级保护三级系统）
b) 是否具有在请求的情况下为数据原发者或接收者提供数据接收证据的功能。应用系统的操作与管理记录，至少应记录操作时间、操作人员及操作类型、操作内容等信息。交易系统应能够记录用户交易行为数据，至少包括业务流水号、账户名、IP 地址、交易指令等信息。（本项适用于：信息系统等级保护三级系统）
c) 数据交换机制是否支持报文校验、动态密钥交换、数字签名等安全措施。
d) 网上证券信息系统未经证券公司授权，是否未与第三方进行任何形式的数据交换，并具备经过认证后仅向授权的第三方指定地址发送信息的功能。

A.2.4.2.8 软件容错

本项要求包括：
a) 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。
b) 在故障发生时，应用系统是否能够继续提供一部分功能，确保能够实施必要的措施。（本项适用于：信息系统等级保护二级系统）

c) 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。（本项适用于：信息系统等级保护三级系统）

A.2.4.2.9 资源控制

本项要求包括：

a) 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，另一方是否能够自动结束会话。用户登录应用系统后在规定的时间内未执行任何操作，应自动退出系统。
b) 是否能够对系统的最大并发会话连接数进行限制。
c) 是否能够对单个账户的多重并发会话进行限制。
d) 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。（本项适用于：信息系统等级保护三级系统）
e) 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。（本项适用于：信息系统等级保护三级系统）
f) 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。（本项适用于：信息系统等级保护三级系统）
g) 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。（本项适用于：信息系统等级保护三级系统）
h) 网上信息系统服务端是否监控并能够抵御连续猜测，避免攻击者通过群体大规模对合法证券账户进行非法用户登陆的请求，导致大量用户账户被异常锁定，正常用户无法登录。

A.2.4.2.10 行情信息

本项要求包括：

a) 通过网上证券信息系统向客户提供证券交易行情信息的，是否提示行情源。
b) 向客户提供证券信息的，是否说明信息来源，并提示投资者对行情信息及证券信息等进行核实。

A.2.4.3 数据安全及备份恢复

A.2.4.3.1 数据完整性

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存储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。（本项适用于：信息系统等级保护三级系统）

A.2.4.3.2 数据保密性

本项要求包括：

a) 是否采用加密或其他保护措施实现鉴别信息的存储保密性。（本项适用于：信息系统等级保护二级系统）
b) 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。（本项适用于：信息系统等级保护三级系统）
c) 网上证券客户端在本地计算机储存客户账户、交易数据等重要信息时，是否提示客户，经客户确认后以加密方式存储。

A.2.4.3.3 备份和恢复

是否妥善保存客户开户资料、委托记录、交易记录和内部管理、业务经营有关的各项资料，不得隐匿、伪造、篡改或者毁损。审计步骤资料的保存期限不得少于20年。

A.2.5 运维管理

A.2.5.1 系统建设管理

A.2.5.1.1 系统定级

本项要求包括：

a) 是否明确信息系统的边界和安全保护等级。
b) 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。
c) 是否确保信息系统的定级结果经过相关部门的批准。
d) 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。（本项适用于：信息系统等级保护三级系统）
e) 定级结果是否经过相关部门批准，由住所地证监局出具定级审核意见。

A.2.5.1.2 方案设计

本项要求包括：

a) 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。
b) 是否以书面形式描述对系统的安全保护要求、策略和措施等内容，形成系统的安全方案。（本项适用于：信息系统等级保护二级系统）
c) 是否对安全方案进行细化，形成能指导安全系统建设、安全产品采购和使用的详细设计方案。（本项适用于：信息系统等级保护二级系统）
d) 是否组织相关部门和有关安全技术专家对安全设计方案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。（本项适用于：信息系统等级保护二级系统）
e) 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。（本项适用于：信息系统等级保护三级系统）
f) 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。（本项适用于：信息系统等级保护三级系统）
g) 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。（本项适用于：信息系统等级保护三级系统）
h) 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。（本项适用于：信息系统等级保护三级系统）
i) 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。
j) 是否按照 99.99%可用性和 7×24 小时连续性指标对集中交易系统进行整体设计。
k) 集中交易系统的功能设计与技术实现是否禁止对违规业务功能的设计与实现。
l) 网上证券客户端是否具备反调试能力。

A.2.5.1.3 产品采购和使用

本项要求包括：

a) 是否确保安全产品采购和使用符合国家的有关规定。
b) 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。

c) 是否指定或授权专门的部门负责产品的采购。
d) 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。（本项适用于：信息系统等级保护三级系统）

A.2.5.1.4 自行软件开发

本项要求包括：
a) 开发环境是否与实际运行环境物理分离。（本项适用于：信息系统等级保护二级系统）
b) 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。
c) 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。
d) 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。应保证同一组件或子系统的开发人员和测试人员分离。（本项适用于：信息系统等级保护三级系统）
e) 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。（本项适用于：信息系统等级保护三级系统）
f) 是否对程序资源库的修改、更新、发布进行授权和批准。（本项适用于：信息系统等级保护三级系统）

A.2.5.1.5 外包软件开发

本项要求包括：
a) 是否根据开发要求测试软件质量。
b) 是否确保提供软件设计的相关文档和使用指南。
c) 是否在软件安装之前检测软件包中可能存在的恶意代码。
d) 要求开发单位提供软件源代码，并审查软件中可能存在的后门。
e) 由证券公司组织定制开发的核心业务系统，是否要求开发商提供源代码或对源代码实行第三方托管。

A.2.5.1.6 工程实施

本项要求包括：
a) 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。
b) 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。
c) 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。（本项适用于：信息系统等级保护三级系统）
d) 网络承建集成商是否具有国家有关部门颁发的二级以上（含二级）计算机信息系统集成资质证书。

A.2.5.1.7 系统交付

本项要求包括：
a) 是否向用户提供系统建设文档和运行维护所需文档。
b) 是否书面规定系统交付的控制方法和人员行为准则。（本项适用于：信息系统等级保护三级系统）
c) 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。（本项适用于：信息系统等级保护三级系统）
d) 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。

e) 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。
f) 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。
g) 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。

A.2.5.1.8 测试验收

本项要求包括：

a) 是否对系统进行安全性测试验收。（本项适用于：信息系统等级保护二级系统）
b) 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。
c) 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。
d) 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。（本项适用于：信息系统等级保护三级系统）
e) 是否书面规定系统测试验收的控制方法和人员行为准则。（本项适用于：信息系统等级保护三级系统）
f) 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。（本项适用于：信息系统等级保护三级系统）
g) 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。
h) 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。
i) 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。模拟环境应与生产环境进行有效隔离，不得对生产环境进行干扰。
j) 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。
k) 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。
l) 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。
m) 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。
n) 是否提前发布生产环境测试的系统测试公告。
o) 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。
p) 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。
q) 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。
r) 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。
s) 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。
t) 测试后是否恢复生产环境并验证恢复的有效性。
u) 是否禁止交易时段使用生产环境进行测试。
v) 是否配备独立的测试系统，并与交易所测试系统联网，实现完整的交易测试环境。
w) 测试系统是否具有与主用系统相同的技术架构，物理上是否具有与主用系统完全独立的通讯、主机及操控系统。
x) 网上证券信息系统的管理、开发、测试是否与运营人员及生产环境分离。

A.2.5.1.9 系统备案

本项要求包括：

a) 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。（本项适用于：信息系统等级保护三级系统）
b) 经营机构是否将系统等级及相关材料报住所地证监局备案。
c) 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.2.5.1.10 等级测评

本项要求包括：

a) 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。（本项适用于：信息系统等级保护三级系统）
b) 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。（本项适用于：信息系统等级保护三级系统）
c) 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。（本项适用于：信息系统等级保护三级系统）
d) 是否指定或授权专门的部门或人员负责等级测评的管理。（本项适用于：信息系统等级保护三级系统）
e) 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.2.5.2 系统运维管理

A.2.5.2.1 值班管理

本项要求包括：

a) 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。
b) 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。
c) 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。
d) 是否制定交接班流程，并严格执行，留存记录。
e) 是否设置运维值班电话，并保持畅通。

A.2.5.2.2 文档管理

本项要求包括：

a) 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。
b) 是否明确文档管理的责任人。
c) 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。
d) 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。

e) 是否对超范围、超权限使用文档时，保存相关审批、使用记录。
f) 是否加强证券营业部技术文档的收集、更新、保管、借阅等管理，确保证券营业部根据信息系统的变更情况及时更新技术文档。证券营业部技术文档包括但不限于机房平面图、供配电图、网络拓扑图、信息点对照表、系统手册、应急预案、运维日志、设备维护档案等资料。

A.2.5.2.3 资产管理

本项要求包括：
a) 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。
b) 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。
c) 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。（本项适用于：信息系统等级保护三级系统）
d) 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。（本项适用于：信息系统等级保护三级系统）

A.2.5.2.4 数据与介质管理

本项要求包括：
a) 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。
b) 是否对介质归档和查询等过程进行记录，并根据存档介质的目录清单定期盘点。（本项适用于：信息系统等级保护二级系统）
c) 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。
d) 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。
e) 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。
f) 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，应按国家相关规定另行处理。
g) 是否根据数据备份的需要对某些介质实行异地存储，存储地的环境要求和管理方法应与本地相同。（本项适用于：信息系统等级保护三级系统）
h) 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。（本项适用于：信息系统等级保护三级系统）
i) 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。
j) 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。
k) 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。
l) 在线数据管理，是否做到如下要求：
   1) 交易业务系统数据应至少每交易日备份一次；
   2) 交易业务系统历史数据至少保留一年；
   3) 未经授权不得访问、复制；
   4) 对数据的修改应通过审批，双岗操作并记录操作日志。

m) 离线数据管理，是否做到如下要求：
   1) 离线数据不得更改；
   2) 应至少每季度对核心交易业务系统的备份数据进行一次有效性验证，如发现问题应采取措施修复备份数据，并查明原因；
   3) 离线数据的调阅、复制、传输、查询，应按照拟定的流程办理审批手续，并进行登记；
   4) 备份数据带离存储环境时应采取必要的安全措施。
n) 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。
o) 离线备份介质是否在本地机房、同城、异地安全可靠存放。
p) 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。
q) 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。
r) 是否保证信息系统日志的完备性，确保所有重大修改被完整地记录，确保开启审计留痕功能。证券公司信息系统日志应至少保存 15 年。
s) 是否加强证券营业部数据备份、存放、保密、调阅、销毁等数据管理，确保证券营业部指定专人负责数据管理，数据调阅须经审批，且不得对外泄露。

A.2.5.2.5 设备和软件管理

本项要求包括：

a) 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。
b) 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。
c) 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。
d) 信息处理设备是否经过审批才能带离机房或办公地点。
e) 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。（本项适用于：信息系统等级保护三级系统）
f) 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。
g) 是否明确设备和软件管理责任人。
h) 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。
i) 是否编制信息系统设备清单，主要包括设备名称、设备编号、入库时间、设备主要参数、设备序列号、设备状态、设备保修期、设备位置、设备用途和设备使用责任人等内容，并保留设备启用、转移、维修、报废等过程的记录。
j) 是否使用正版软件并保存软件授权证书和许可协议，应编制软件清单，主要包括软件名称、软件编号、入库时间、软件版本，授权和许可情况、软件序列号、软件状态、软件维护期、软件安装设备、用途和使用责任人等内容，并保留软件启用、转移、升级、报废等过程的记录。
k) 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。
l) 是否对外送设备的维修进行严格管理，防止数据泄露。
m) 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.2.5.2.6 变更管理

本项要求包括：

a) 是否确认系统中要发生的变更，并制定相应的变更方案；重要系统变更前应制定详细的变更方案、失败恢复方案、专项应急预案。
b) 系统发生重要变更前，是否向主管领导申请，审批后方可实施变更，并在实施后向相关人员通告。（本项适用于：信息系统等级保护二级系统）
c) 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。（本项适用于：信息系统等级保护三级系统）
d) 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。（本项适用于：信息系统等级保护三级系统）
e) 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。（本项适用于：信息系统等级保护三级系统）
f) 是否建立系统变更流程，对信息系统的变更活动进行规范。
g) 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。
h) 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。
i) 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。
j) 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。
k) 是否按照测试方案，组织变更前后的测试，测试后应提交测试记录或报告。
l) 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。
m) 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。

A.2.5.2.7 配置管理

本项要求包括：

a) 是否制定配置管理流程，明确配置管理负责人。
b) 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。
c) 配置库中配置项的属性是否至少包括以下信息。
    1) 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；
    2) 配置项编号应唯一；
    3) 配置项的添加、修改、替换、删除应有变更记录；
    4) 应保存配置项历史记录，确保与事件管理、问题管理、变更管理等流程记录的关联性。
d) 是否定期对配置库进行备份。
e) 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。

A.2.5.2.8 日常操作

本项要求包括：

a) 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。

b) 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。
c) 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。
d) 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。
e) 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。
f) 是否对核心交易业务系统设置独立的操作和监控环境，与开发、测试等其他操作环境严格分离。
g) 注册邮箱账号是否经过审批。
h) 各参与方在进行日终清算文件交换时，是否对日终清算文件的合法性和完整性进行校验。
i) 是否禁止通过互联网对网上证券信息系统（如防火墙、网络设备、服务器等）进行远程管理和日常维护等操作。特殊紧急情况下需要通过互联网进行远程操作时，是否通过限制登录 IP、使用数字证书或动态口令、全程监控等措施确保安全，并在操作完成后，及时关闭相关端口。

A.2.5.2.9 口令管理

本项要求包括：

a) 用户和口令管理是否符合如下要求：
   1) 不得设置弱口令，若系统条件允许，口令应采用数字、字母、符号混排且无规律的方式，管理员口令长度原则上不低于 12 位；核心交易业务系统应提示并阻止用户使用弱口令登录；
   2) 应每季度对管理员口令进行修改，更新的管理员口令至少 5 次内不能重复；
   3) 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；
   4) 应重点加强对匿名/默认用户的管理，防止被非法使用；
   5) 应及时注销不再使用的账户；
   6) 应明确责任人，负责统一保管、安全存放管理员口令，不得泄漏。
b) 集中交易系统安全管理是否帐户和口令专人专用，加强对缺省帐户和口令的管理。
c) 集中交易系统安全管理是否禁止为客户设置统一的、有规律的、易猜测的初始口令。
d) 是否防止用户使用简单口令，并能够抵御连续猜测等对客户账户恶意攻击行为。
e) 是否确保证券营业部关键系统和关键设备的管理员用户密码实行专人管理，采用不低于 8 位的复合密码，每半年至少更换一次。发生人员变动时应及时更新密码。

A.2.5.2.10 数据库管理

本项要求包括：

a) 是否保持数据库的可用性，及时维护、更新软件。
b) 是否负责数据库的参数配置、调优，编制文档并保持更新。
c) 是否定期对数据库容量进行检查和评估，形成评估报告。
d) 是否负责管理数据库、表、索引、存储过程，数据库的升级、优化、扩容、迁移。
e) 是否定期检查数据库的用户、口令及权限设置的正确性。
f) 是否严格限制人工对数据库操作的账户权限，并分别使用不同权限的账户执行查询、插入、更新、删除等操作。

A.2.5.2.11 终端信息

本项要求包括：

a) 向客户提供的交易终端软件，是否采取适当的技术，确保软件能够采集到客户交易终端电话号码、互联网通讯协议地址（IP 地址）、媒介访问控制地址（MAC 地址）以及其他能识别客户交易终端的特征代码。
b) 向客户提供的交易终端软件，是否采取适当的技术，确保软件能够采集到客户交易终端信息。由第三方提供交易终端软件的，应当建立软件认证许可制度，要求第三方采取适当的技术，确保软件能够采集到客户交易终端信息。客户交易终端软件应当具备先提醒升级、再自动升级为最新版本的功能。
c) 网上交易、语音交易、自助交易等外围信息系统是否逐笔记录交易委托、银证转账、密码修改、账户登录等操作的客户交易终端信息。集中交易系统还应当同时逐笔存储交易委托、银证转账等操作的客户交易终端信息。
d) 是否为证券交易所或登记结算机构采集客户交易终端信息提供相应的数据接口，并在相关技术规范发布之日起 12 个月内，完成信息系统的改造升级，改造后的信息系统应符合国家信息安全标准。
e) 是否按照本规定的要求建设、改造和维护相关信息系统，以妥善管理客户交易终端信息，并提供符合技术规范的查询接口。应当采取必要的技术手段，满足交易时段客户信息查询的需要。
f) 是否按照技术规范对客户的主要开户资料进行电子化，并妥善保存在信息系统中。应当按照技术规范在 18 个月内对新增账户实施开户资料电子化，存量的正常交易类账户应在 36 个月内完成开户资料电子化。
g) 是否妥善保存客户交易终端信息和开户资料电子化信息，保存期限不得少于 20 年。应妥善保存交易时段客户交易区的监控录像资料，保存期限不得少于 6 个月。
h) 是否采取可靠的措施，采集、记录、存储、报送与客户身份识别有关的信息，不得以任何理由拒绝承担相应职责。公司及其工作人员应当对客户交易终端信息予以保密，不得泄露。
i) 是否严格限制对客户交易终端信息的人工操作权限，明确查询权限和操作流程，建立日志文档并指定专人妥善保管。禁止任何人对客户交易终端信息进行隐匿、伪造、篡改或毁损。
j) 发生影响采集、记录、存储、报送客户交易终端信息安全的重大事件时，是否及时向公司住所地和事件发生地证监局报告，不得隐瞒。

A.2.5.2.12 督促检查

本项要求包括：

a) 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。
b) 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。
c) 是否每季组织开展内部检查，形成检查报告。
d) 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。
e) 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。
f) 是否对检查和审计的结果采取纠正性和预防性的措施。
g) 是否确保证券营业部至少每半年检查一次电力、机房空调、消防等设施，每季度选择非交易时间进行 UPS 电池的充放电测试，并详细记录。
h) 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.2.5.2.13 监控分析

本项要求包括：

a) 是否应采取监控措施，配备监控和报警工具，对影响信息系统正常运行的关键对象，包括机房环境、网络、通信线路、主机、存储、数据库、核心交易业务相关的应用系统、安全设备等进行监控，形成记录并妥善保存。报警方式可包括声光、电话、短信、邮件等。

b) 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。（本项适用于：信息系统等级保护三级系统）

c) 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。（本项适用于：信息系统等级保护三级系统）

d) 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，应开启自动监控系统和自动报警系统。

e) 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。

f) 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。

g) 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。

h) 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。

i) 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。

j) 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。

k) 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。

l) 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。

m) 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。

n) 门户网站监控指标是否包括网页内容、日均访问量等。

o) 是否针对不同系统设置合理的监测频度。

p) 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。

q) 是否保存监控产生的日志，保存时间不少于一年。

r) 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。应至少每季度全面评估监控日志和操作记录，分析异常情况，形成评估报告。

s) 是否通过多种技术手段加强对投资者账户异动情况的监控，如委托的方式、品种、价格、数量异常等，并及时提醒客户，以保护客户资产安全。

t) 是否定期评估可供客户使用的网上证券信息系统的资源状况，并根据实时监控信息、可预见的业务发展需求进行容量的需求预测，确保有充足的处理能力、存储容量和通讯带宽，满足业务增长的需要，保证网上证券服务的可用性，并能抵御一定程度的拒绝服务攻击和缓冲区溢出攻击。

u) 是否确保 A 型证券营业部具备完善的监控体系，对信息系统的运行环境、运行状况等进行定时监控和事后分析。

v) 是否确保 A 型和 B 型证券营业部对系统运维日志进行规范管理，日常操作及异常事件处理应在系统运维日志中详细记录。运维日志可采用电子文档或纸质件记录，并妥善保管，保留期限不少于 2 年。

A.2.5.2.14 网络安全管理

本项要求包括：

a) 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。

b) 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。

c) 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；应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。

d) 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；

1) 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；

2) 实施漏洞扫描或漏洞修补前，应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；

3) 漏洞扫描或漏洞修补后应进行验证测试，以保证网络系统的正常运行。

e) 是否保证所有与外部系统的连接均得到授权和批准。

f) 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；应在配置变更前、变更后分别对网络设备的配置文件进行备份。（本项适用于：信息系统等级保护三级系统）

g) 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。（本项适用于：信息系统等级保护三级系统）

h) 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。（本项适用于：信息系统等级保护三级系统）

i) 是否合理设置安全域，绘制网络拓扑图，并保持更新。

j) 是否配置、调优网络系统的参数。

k) 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。

l) 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；应正确设置安全设备的接口参数和过滤规则。

m) 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。

n) 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，特殊紧急情况下应采取限制登录 IP、数字证书或动态口令认证、全程监控等措施，在操作完成后应及时关闭，并对维护过程进行监控并留存记录。

o) 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。

p) 是否禁止通过无线网络对交易业务网进行网络管理。

q) 计算机网络跳线是否整齐干净，跳线标识清晰。

r) 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。

s) 是否保持网络设备的可用性，及时维修、更换故障设备。

t) 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.2.5.2.15 系统安全管理

本项要求包括：

a) 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。
b) 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。
c) 是否安装系统的最新补丁程序，在安装系统补丁前，应首先充分评估并在测试环境中测试通过，并对重要文件进行备份后，方可实施系统补丁程序的安装；持续跟踪厂商提供的系统升级更新情况，应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。
d) 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。
e) 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。
f) 是否至少每月对运行日志和审计数据进行分析。
g) 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，权限设定应当遵循最小授权原则。（本项适用于：信息系统等级保护三级系统）
h) 系统管理是否包括：
   1) 应保持系统的可用性，及时维修、更换故障设备和更新软件；
   2) 应负责应用系统、操作系统的参数配置、调优，编制文档并保持更新；
   3) 应定期对系统容量进行检查和评估，形成评估报告；
   4) 应负责管理系统和应用程序服务进程，并关闭与业务无关的服务；
   5) 应定期检查应用系统、操作系统的用户、口令及权限设置的正确性。
i) 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。
j) 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。
k) 是否对证券营业部安装使用的应用软件进行统一管理，证券营业部不得擅自安装与业务及技术维护无关的应用软件。
l) 客户使用的网上证券委托软件是否由证券公司管理和授权发布。
m) 是否对其授权第三方发布的证券委托软件进行审核、监管。
n) 是否采取有效措施对门户网站上提供下载的网上证券客户端软件程序进行保护，客户端软件程序编译封装、形成下载文件后，应安排专人对其进行严格的病毒扫描和木马检查，并通过专用安全手段传输至网站文件下载服务器。
o) 网上证券客户端是否具有唯一连接到本证券公司网上证券接入系统的保障机制。网上证券客户端应提供足够的识别信息，以保证网上证券服务端能够对发出连接请求的客户端与证券公司所提供下载的程序进行一致性验证。
p) 当客户访问网上证券服务端时，未经客户许可，是否禁止以任何方式在客户端系统中安装插件。
q) 是否建立确认机制以保证客户获得正确的移动证券客户端软件。
r) 安全风险评估是否包括漏洞扫描、攻击测试、病毒扫描、木马检测等，针对不同的威胁设置相应的检查频率。

A.2.5.2.16 恶意代码防范

本项要求包括：

a) 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。
b) 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。
c) 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。
d) 是否定期检查信息系统内各种产品的恶意代码库的升级情况并进行记录，对主机防病毒产品、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及时分析处理，并形成书面的报表和总结汇报。（本项适用于：信息系统等级保护三级系统）
e) 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。
f) 网上交易软件是否采取安全的密码输入方式，增强防御恶意程序窃取密码的功能。
g) 基于浏览器的网上证券下单网页是否使用 HTTPS 等加密方式与服务端交互，服务端应具备防范 SQL 注入式攻击、跨站脚本攻击等网页攻击的能力，同时关闭 HTTP 服务器的 Web 远程维护功能。
h) 是否建立定期的网上信息系统安全风险评估机制和整改的工作制度，及时发现 SQL 注入漏洞、弱口令账户、绕过验证、目录遍历、文件上传、跨站脚本、Session 欺骗、拒绝式服务攻击和缓冲区溢出等系统存在的安全隐患和漏洞，并进行改进和完善。风险评估应通过内部评估与外部评估相结合的方式进行。
i) 是否确保证券营业部及时更新系统补丁、升级系统安全防护软件，定期进行全面的病毒和木马检测，发现病毒和木马立即处理并报告。移动存储、外来电子文档、软件系统使用前应进行病毒和木马查杀。
j) 是否定期对网站程序代码进行全面检查和评估，并及时修补，避免各种漏洞的存在。

A.2.5.2.17 密码管理

本项要求包括：

a) 是否使用符合国家密码管理规定的密码技术和产品。（本项适用于：信息系统等级保护二级系统）
b) 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。（本项适用于：信息系统等级保护三级系统）
c) 网上证券信息系统采用的认证授权和加密体系是否通过国家信息安全机构的安全性测评，具备足够的强度和抗攻击能力，并根据在网上开展证券业务的安全性需要和信息技术的发展，定期检查、评估和及时调整。

A.2.5.2.18 备份与恢复管理

本项要求包括：

a) 是否识别需要定期备份的重要业务信息、系统数据及软件系统等。
b) 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。
c) 是否根据数据的重要性及其对系统运行的影响，制定数据的备份策略和恢复策略，备份策略指明备份数据的放置场所、文件命名规则、介质替换频率和数据离站运输方法。
d) 是否建立控制数据备份和恢复过程的程序，对备份过程进行记录，所有文件和记录应妥善保存。（本项适用于：信息系统等级保护三级系统）
e) 是否定期执行恢复程序，检查和测试备份介质的有效性，确保可以在恢复程序规定的时间内完成备份的恢复。（本项适用于：信息系统等级保护三级系统）

f) 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；每季度至少对数据备份进行一次有效性验证。
g) 除已具有冗余备份机制的网上交易系统外，实时信息系统与非实时信息系统的灾难应对能力是否达到《证券期货经营机构信息系统备份能力标准》第五级或重大灾难应对能力达到第六级要求。
h) 2015 年底前，除已具有冗余备份机制的网上交易系统外，实时信息系统与非实时信息系统的重大灾难应对能力是否达到《证券期货经营机构信息系统备份能力标准》第六级要求。
i) 集中交易系统（含第三方存管）、融资融券系统、网上交易系统、电话委托系统、移动证券系统等实时信息系统是否达到《证券期货经营机构信息系统备份能力标准》中故障应对能力的第三级要求。
j) 法人清算系统、门户网站系统等非实时信息系统是否满足《证券期货经营机构信息系统备份能力标准》中故障应对能力的第二级要求。
k) 是否制定信息系统备份能力建设工作计划。
l) 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。

A.2.5.2.19 业务连续性

是否制定在网上开展证券业务连续性计划，保证在网上开展证券业务的连续正常运营。在网上开展证券业务连续性计划应充分评估第三方服务供应商对业务连续性的影响，并应采取适当的预防措施。

A.2.5.2.20 事件与问题管理

本项要求包括：
a) 是否对安全检查情况进行评估，形成评估报告。
b) 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。
c) 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。
d) 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。
e) 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。
f) 是否每月回顾、分析事件处理记录，完成事件分析报告。
g) 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。
h) 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。
i) 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。
j) 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。
k) 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。

A.2.5.2.21 网站安全

本项要求包括：
a) 是否建立对门户网站内容的审核制度、完整的发布流程和监控机制。
b) 是否对网页内容进行监控，对有害信息进行过滤，防止网站出现不良信息。
c) 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。

d) 当网站上的页面内容、提供给投资者下载的客户端软件及其他文件被异常修改时，是否能自动告警或自动恢复，防止被捆绑木马程序。
e) 网上证券信息系统是否部署在中华人民共和国境内，满足技术审计、监管部门现场检查及中国司法机构调查取证等要求。部署网上证券信息系统的有形场所，应符合国家安全标准的有关要求。
f) 网上证券信息系统是否自主运营、自主管理。如涉及第三方（指除证券公司及其客户以外的任何一方），应与第三方签订保密协议和服务级别协议，并明确责任，采取措施防止通过第三方泄露用户信息。
g) 门户网站是否按照国家主管部门的有关规定办理 ICP 备案，在网站首页公布 ICP 备案号，并提供备案信息的链接。
h) 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。
i) 网上客户业务处理的日志是否单独存放。

A.2.5.2.22 软件正版化

本项要求包括：
a) 是否明确部门或责任人，负责本单位软件正版化工作。
b) 是否落实软件采购经费，做好软件正版化工作。
c) 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。
d) 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。
e) 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。
f) 是否每年对软件正版化情况开展自查。
g) 操作系统软件是否有授权（服务器）。
h) 操作系统是否有授权（办公计算机）。
i) 数据库软件是否有授权。
j) 杀毒软件是否有授权。
k) 办公文字处理软件是否有授权。
l) 办公专业处理软件是否有授权。
m) 应用服务器软件是否有授权。
n) 专用业务软件是否有授权。
o) 是否制定了软件正版化计划。

A.2.5.3 应急处置

A.2.5.3.1 应急准备

本项要求包括：
a) 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。
b) 是否对系统相关的人员进行应急预案培训，应急预案的培训应至少每年举办一次。
c) 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。（本项适用于：信息系统等级保护三级系统）
d) 是否定期对应急预案进行演练，根据不同的应急恢复内容，确定演练的周期；应至少每年对应急预案进行演练。（本项适用于：信息系统等级保护三级系统）

e) 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。（本项适用于：信息系统等级保护三级系统）

f) 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。

g) 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。

h) 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。

i) 是否制定了网络与信息安全事件应急预案，内容至少包括：

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

j) 应急预案是否符合如下要求：

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

k) 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。

l) 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。

m) 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。

n) 是否建立有效的应急通讯联络系统，确保信息畅通。

o) 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。

p) 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。

q) 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。

r) 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。

s) 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。
t) 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。
u) 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。
v) 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。
w) 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。
x) 是否每半年至少组织一次网络与信息安全应急演练。
y) 是否记录演练情况，演练记录至少保存两年。
z) 是否对演练中发现的问题进行改进。
aa) 是否每年向住所地证监局报告年度应急演练情况。
bb) 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。
cc) 是否定期组织灾难备份应急预案和应急计划的演练，至少每年二次，并根据演练的结果和发现的问题进行总结，对系统和应急方案进行优化及完善。
dd) 是否对集中交易系统实行年度例行安全评估，并将评估结果报备相关交易所。
ee) 是否制定了针对第三方存管系统完整的应急预案及应急协调预案，并定期组织演练及联合演练。
ff) 网上信息系统应急预案是否针对电力、通信等基础设施故障、计算机硬件或网络设备故障、操作系统或应用系统故障、操作系统或应用系统漏洞、病毒入侵、恶意攻击、误操作、不可抗力等可能的故障原因制定对应的应急恢复操作流程或步骤。
gg) 是否确保 A 型、B 型、C 型营业部每年至少进行两次应急演练，并留存演练记录。

A.2.5.3.2 应急处置

本项要求包括：

a) 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。
b) 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。
c) 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。
d) 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。
e) 是否记录并保存所有报告的安全弱点和可疑事件，分析事件原因，监督事态发展，采取措施避免安全事件发生。（本项适用于：信息系统等级保护二级系统）
f) 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。（本项适用于：信息系统等级保护三级系统）
g) 是否针对集中交易制定规范化的故障处理流程，建立详细的故障日志（包括故障发生的时间、范围、现象、处理结果和处理人员等内容）。
h) 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。（本项适用于：信息系统等级保护三级系统）
i) 是否做好应急处置的相关记录，保留有关证据。

j) 是否对造成系统中断和造成信息泄密的安全事件应采用不同的处理程序和报告程序。（本项适用于：信息系统等级保护三级系统）
k) 是否对证券期货行业内通报的重大安全隐患，应立即进行专项安全检查。
l) 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。
m) 是否在应急处置中注意保证工作人员的人身安全。
n) 是否在应急处置结束前，保证专人 24 小时值班。
o) 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。
p) 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。
q) 日终清算数据送达商业银行的时间要求为：非结息日的截止时间为次日凌晨 2:00，结息日的截止时间为次日凌晨 3:00。如需延迟，是否提前至少一小时通知商业银行。
r) 各参与方如果因网络故障等原因，无法通过第三方存管系统自动传送日终清算数据到相关参与方，是否及时通知对方，并以其他方式将数据及时送达对方。
s) 第三方存管各参与方是否建立并完善内部责任机制和协调机制，坚持信息安全事故问责制度，做好自动留痕和书面留痕工作，以便于责任事故的认定。
t) 发现假冒本公司网上证券服务的非法活动或者网上证券信息系统出现重大安全事件后，是否及时向监管部门、公安机关报告。在启动实施网上证券信息系统应急预案时应及时向投资者公告。对于假冒本公司的非法活动应及时通过证券公司网站、网上证券客户端、电话语音系统或短信平台等提醒投资者注意。
u) 营业部发生影响交易业务的技术故障时，证券公司是否立即启动应急预案，尽快恢复交易业务，并按有关要求及时上报公司和证券营业部所在地证监局。应急事件处理完成后，应以书面形式上报公司和证券营业部所在地证监局。

A.2.5.3.3 调查处理

本项要求包括：

a) 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。事件总结报告内容应当包括：
   1) 事件基本情况，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；
   2) 应急处置情况，包括事件报告的情况、采取的措施及效果；
   3) 事件调查情况，包括事件原因、事件级别、责任认定和结论；
   4) 事件处理情况，包括事件暴露出的问题及采取的整改措施，责任追究情况。
b) 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。
c) 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。
d) 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。

e) 是否向住所地中国证监会派出机构进行预警报告、应急报告和事件总结报告，分支机构应当向所在地中国证监会派出机构进行预警报告、应急报告和事件总结报告。事件总结报告同时抄送中国证券业协会。
f) 发生信息安全事件影响到证券期货交易业务时，是否同时向相关证券期货交易所进行应急报告和事件总结报告；影响到证券登记结算业务时，应当同时向中国证券登记结算公司进行应急报告和事件总结报告；影响到转融通业务时，应当同时向中国证券金融公司进行应急报告和事件总结报告；影响到其他机构的，应当及时向有关机构进行应急通报。
g) 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.3 基金管理公司系统运行安全审计项汇总

A.3.1 组织管理

A.3.1.1 安全管理制度

A.3.1.1.1 管理制度

本项要求包括：
a) 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。
b) 是否建立安全管理制度，覆盖安全策略的制定、实施、检查、评估、改进等全过程。
c) 是否形成由安全策略、管理制度、操作规程等构成的全面的信息安全管理制度体系。（本项适用于：信息系统等级保护三级系统）
d) 是否对安全管理人员或操作人员执行的日常管理操作建立操作规程。
e) 是否制定覆盖运维工作各个环节的、体系化的运维管理制度和操作流程。运维管理制度包括但不限于：机房管理、网络与系统管理、数据和介质管理、交付管理、测试管理、配置管理、安全管理、值班管理、监控管理、文档管理、设备和软件管理、供应商管理、关联单位关系管理、检查审计等制度。运维操作流程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。
f) 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。

A.3.1.1.2 制定和发布

本项要求包括：
a) 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。
b) 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。
c) 安全管理制度是否具有统一的格式，并进行版本控制。（本项适用于：信息系统等级保护三级系统）
d) 是否建立信息发布管理审核制度；安全管理制度是否通过正式、有效的方式发布。
e) 安全管理制度是否注明发布范围，并对收发文进行登记。（本项适用于：信息系统等级保护三级系统）

A.3.1.1.3 评审和修订

本项要求包括：

a) 信息安全领导小组是否负责定期组织相关部门和相关人员对安全管理制度体系的合理性和适用性进行审定；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。（本项适用于：信息系统等级保护三级系统）
b) 是否定期或不定期对安全管理制度进行检查和审定，对存在不足或需要改进的安全管理制度进行修订。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。
c) 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.3.1.2 安全管理机构

A.3.1.2.1 机构设置

本项要求包括：

a) 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。
b) 是否设立 IT 治理委员会或类似机构，负责公司 IT 治理工作。
c) IT 治理委员是否包括公司 IT 治理直接责任人、IT 总监、IT 部门负责人、相关业务负责人、财务负责人、内部控制负责人以及部分技术骨干等人员，其中 IT 人员的比例是否在 30%以上。
d) IT 治理委员会是否履行以下职责：
   1) 拟订公司 IT 治理目标和 IT 治理工作计划；
   2) 审议公司 IT 发展规划；
   3) 审议公司年度 IT 工作计划和 IT 预算；
   4) 审议公司重大 IT 项目立项、投入和优先级；
   5) 审议公司 IT 管理制度和重要流程；
   6) 制订与 IT 治理相关的培训和教育工作计划；
   7) 检查所拟订和审议事项的落实和执行情况；
   8) 组织评估公司 IT 重大事项并提出处置意见；
   9) 向公司管理层报告 IT 治理状况。

A.3.1.2.2 岗位设置

本项要求包括：

a) 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。
b) 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。
c) 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。（本项适用于：信息系统等级保护三级系统）
d) 是否合理设置运维岗位，规定岗位职责及技能要求，并符合如下要求：
   1) 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；
   2) 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。
e) 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。
f) 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.3.1.2.3 人员配备

本项要求包括：

a) 是否配备系统管理员、网络管理员、安全管理员等；每个岗位应有备岗。
b) 安全管理员是否禁止兼任网络管理员、系统管理员、数据库管理员。（本项适用于：信息系统等级保护二级系统）
c) 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。
d) 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。
e) 关键事务岗位是否配备多人共同管理。（本项适用于：信息系统等级保护三级系统）
f) 公司是否配备足够的信息技术人员，公司的 IT 工作人员总数不少于公司员工总人数的 6%。
g) 是否有应急技术支援队伍。

A.3.1.2.4 授权和审批

本项要求包括：

a) 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。
b) 是否针对关键活动建立审批流程，并由批准人签字确认。（本项适用于：信息系统等级保护二级系统）
c) 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。（本项适用于：信息系统等级保护三级系统）
d) 是否定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息；每年至少审查一次审批事项。（本项适用于：信息系统等级保护三级系统）
e) 是否记录审批过程并保存审批文档。（本项适用于：信息系统等级保护三级系统）
f) 权限分配是否有审批和完整的记录，权限设置后应复核。
g) 是否按照最小安全访问原则分配用户权限。
h) 是否建立权限分配表，对用户的访问权限进行合理分配，对文件系统访问权限进行合理设置，编制文档并保持更新。
i) 是否在用户账户变化时，同时变更或撤销其权限。
j) 是否定期检查权限设置的有效性。
k) 是否禁止基金销售机构业务人员和运行维护人员直接修改基金投资人交易数据和口令密码；因特殊原因需要修改的，是否履行严格的程序并且留痕。

A.3.1.2.5 供应商管理

本项要求包括：

a) 是否确保安全服务商的选择符合国家、行业的有关规定。
b) 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。
c) 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。
d) 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。
e) 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。
f) 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，明确供应商应接受证券期货行业监管部门的信息安全延伸检查。

g) 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。
h) 是否加强运维外包服务管理，主要包括：
   1) 与外包公司及外包人员签订保密协议；
   2) 明确外包公司应当承担的责任及追究方式；
   3) 明确界定外包人员的工作职责、活动范围、操作权限；
   4) 对外包人员工作情况进行监督和检查，并保留相应记录；
   5) 对驻场外包人员的入场和离场进行管理；
   6) 定期评估外包的服务质量；制定外包服务意外终止的应急措施。
i) 对于定制开发的核心业务系统，是否要求开发商提供源代码或对源代码实行第三方托管。

A.3.1.2.6 关联单位关系管理

本项要求包括：
a) 是否加强各类管理人员之间、组织内部机构之间以及信息安全职能部门内部的合作与沟通。(本项适用于：信息系统等级保护二级系统)
b) 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。
c) 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。（本项适用于：信息系统等级保护三级系统）
d) 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。（本项适用于：信息系统等级保护三级系统）
e) 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。（本项适用于：信息系统等级保护三级系统）
f) 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。

A.3.1.2.7 审核和检查

本项要求包括：
a) 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。安全检查应至少每季度一次。
b) 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；全面安全检查应至少每年一次。（本项适用于：信息系统等级保护三级系统）
c) 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。（本项适用于：信息系统等级保护三级系统）
d) 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。（本项适用于：信息系统等级保护三级系统）

A.3.1.3 经费和人员管理

A.3.1.3.1 经费投入

本项要求包括：

a) 最近三个财政年度IT投入平均数额是否不少于最近三个财政年度平均净利润的6%或不少于最近三个财政年度平均营业收入的3%，取二者数额较大者。
b) 是否制定信息系统运行维护年度预算计划，每年进行核算。预算和核算应接受监督和审计。
c) 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。
d) 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。

A.3.1.3.2 人员录用

本项要求包括：

a) 是否指定或授权专门的部门或人员负责人员录用。
b) 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。
c) 是否与开发、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。
d) 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。（本项适用于：信息系统等级保护三级系统）

A.3.1.3.3 人员离岗

本项要求包括：

a) 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。
b) 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。
c) 是否办理严格的调离手续。（本项适用于：信息系统等级保护二级系统）
d) 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。（本项适用于：信息系统等级保护三级系统）

A.3.1.3.4 人员考核

本项要求包括：

a) 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应至少每年一次。
b) 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。（本项适用于：信息系统等级保护三级系统）
c) 是否对考核结果进行记录并保存。（本项适用于：信息系统等级保护三级系统）

A.3.1.3.5 教育和培训

本项要求包括：

a) 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。
b) 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。
c) 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。

d) 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。（本项适用于：信息系统等级保护三级系统）

A.3.1.3.6 外部人员访问管理

本项要求包括：

a) 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。

b) 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。（本项适用于：信息系统等级保护三级系统）

A.3.2 机房管理

A.3.2.1 基础保障

A.3.2.1.1 物理位置的选择

本项要求包括：

a) 机房和办公场地是否选择具有防震、防风和防雨等能力的建筑：
   1) 应具有机房或机房所在建筑物符合当地抗震要求的相关证明；
   2) 机房外墙壁应没有对外的窗户。否则，应采用双层固定窗，并作密封、防水处理。

b) 机房场地是否避免设在建筑物的高层或地下室，以及用水设备的下层或隔壁：（本项适用于：信息系统等级保护三级系统）
   1) 机房场地不宜设在建筑物顶层，如果不可避免，应采取有效的防水措施。机房场地设在建筑物地下室的，应采取有效的防水措施；
   2) 机房场地设在建筑物高层的，应对设备采取有效固定措施；
   3) 如果机房周围有用水设备，应当有防渗水和疏导措施。

A.3.2.1.2 防雷击

本项要求包括：

a) 机房或机房所在大楼，是否设计并安装防雷击措施，防雷措施应至少包括避雷针或避雷器等。

b) 机房是否设置交流电源地线。

c) 是否设置防雷保安器，防止感应雷。（本项适用于：信息系统等级保护三级系统）

A.3.2.1.3 防火

本项要求包括：

a) 机房是否设置灭火设备和火灾自动报警系统。机房的火灾自动报警系统应向当地公安消防部门备案。（本项适用于：信息系统等级保护二级系统）

b) 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应向当地公安消防部门备案。（本项适用于：信息系统等级保护三级系统）

c) 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。（本项适用于：信息系统等级保护三级系统）

d) 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。（本项适用于：信息系统等级保护三级系统）

A.3.2.1.4 防水和防潮

本项要求包括：

a) 水管安装，是否穿过机房屋顶和活动地板下；
   1) 与机房设备无关的水管不得穿过机房屋顶和活动地板下；
   2) 机房屋顶和活动地板下铺有水管的，应采取有效防护措施。
b) 是否采取措施防止雨水通过机房窗户、屋顶和墙壁渗透。
c) 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。
d) 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。（本项适用于：信息系统等级保护三级系统）

A.3.2.1.5 防静电

本项要求包括：

a) 关键设备应采用必要的接地防静电措施。（本项适用于：信息系统等级保护二级系统）
b) 主要设备是否采用必要的接地防静电措施。（本项适用于：信息系统等级保护三级系统）
c) 机房是否采用防静电地板。（本项适用于：信息系统等级保护三级系统）

A.3.2.1.6 空调

本项要求包括：

a) 机房是否设置温、湿度自动调节设施，使机房温、湿度的变化在设备运行所允许的范围之内：
   1) 开机时机房温度应控制在 22℃-24℃；
   2) 开机时机房相对湿度应控制在 40%-55%。
b) 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。

A.3.2.1.7 电力供应

本项要求包括：

a) 是否在机房供电线路上配置稳压器和过电压防护设备。
b) 是否提供短期的备用电力供应，至少满足主要设备在断电情况下的正常运行要求。
   1) 机房应配备 UPS，UPS 实际供电能力能够满足主要设备在断电情况下正常运行 2 个小时以上；
   2) 机房应自备或租用发电机，能够保障持续供电。
c) 是否采用双路市电，双路市电应能实现自动切换。（本项适用于：信息系统等级保护三级系统）

A.3.2.1.8 电磁防护

本项要求包括：

a) 电源线和通信线缆是否隔离铺设，避免互相干扰。电源线和通信线缆应铺设在不同的桥架或管道，避免互相干扰。
b) 是否采用接地方式防止外界电磁干扰和设备寄生耦合干扰：（本项适用于：信息系统等级保护三级系统）
   1) 机房或机房所在的大楼必须有接地措施，并且接地电阻必须小于 1 欧姆；
   2) 机房验收报告应提供合格的检测结果。
c) 是否对关键设备和磁介质实施电磁屏蔽。（本项适用于：信息系统等级保护三级系统）

A.3.2.2 机房运维

A.3.2.2.1 物理访问控制

本项要求包括：

a) 机房出入口是否安排专人值守，控制、鉴别和记录进入的人员；
   1) 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；
   2) 没有门禁系统的机房，应当安排专人控制、鉴别和记录人员的进出；
   3) 有门禁系统的机房，应当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。
b) 需进入机房的来访人员是否经过申请和审批流程，并限制和监控其活动范围；
   1) 来访人员进入机房，应有审批流程，记录带进带出的设备、进出时间、工作内容，并有专人陪同其在限定的范围内工作；
   2) 机房出入口应有视频监控，监控记录至少保存 3 个月。
c) 是否对机房划分区域进行管理，区域和区域之间设置物理隔离装置，在重要区域前设置交付或安装等过渡区域：（本项适用于：信息系统等级保护三级系统）
   1) 机房应当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；
   2) 机房应当设置专门的过渡区域，用于设备的交付或安装；
   3) 重要区域包括：主机房、辅助区、支持区等功能区域。

A.3.2.2.2 防盗窃和防破坏

本项要求包括：

a) 是否将主要设备放置在机房内。
b) 是否将设备或主要部件进行固定，并设置明显的不易除去的标记；
   1) 主要设备应当安装、固定在机柜内或机架上；
   2) 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。
c) 是否将通信线缆铺设在隐蔽处，可铺设在地下或管道中；通信线缆可铺设在管道或线槽、线架中。
d) 是否对介质分类标识，存储在介质库或档案室中。
e) 主机房应安装必要的防盗报警设施。（本项适用于：信息系统等级保护二级系统）
f) 是否利用光、电等技术设置机房防盗报警系统。（本项适用于：信息系统等级保护三级系统）
g) 是否对机房设置监控报警系统：（本项适用于：信息系统等级保护三级系统）
   1) 应至少对机房的出入口、操作台等区域进行摄像监控；
   2) 监控录像记录至少保存 3 个月。

A.3.2.2.3 机房管理

本项要求包括：

a) 是否指定专门的部门或人员定期对机房供配电、空调、温湿度控制等设施进行维护管理；
   1) 应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；
   2) 应每年对防盗报警、防雷、消防等装置进行检测维护并保存相关维护记录。
b) 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。
c) 是否加强对办公环境的保密性管理，包括工作人员调离办公室应立即交还该办公室钥匙和不在办公区接待来访人员等。（本项适用于：信息系统等级保护二级系统）
d) 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。

e) 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。（本项适用于：信息系统等级保护三级系统）
f) 是否指定机房管理负责人。
g) 是否确保机房环境整洁和安全，包括：
   1) 应定期检查防水、防雷、防火、防潮、防尘、防鼠、防静电、防电磁辐射等措施的有效性；
   2) 应保持机房环境卫生，采取防尘措施，定期进行除尘处理；
   3) 交易时间内不得进行机房施工、保洁操作。
h) 是否对设备和人员出入进行严格管理，包括：
   1) 应指定人员负责控制、鉴别和记录设备和人员的进出情况，记录进出人员、进出时间、工作内容，并留存记录至少 90 天；
   2) 机房出入口的监控录像至少保存 90 天；
   3) 外来人员进入机房应经过申请和审批流程，并限制和监控其活动范围，并有专人陪同；
   4) 外来设备未经批准不得接入生产环境。

A.3.2.2.4 用电安全

本项要求包括：

a) 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。
b) 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。
c) 是否在危险性高的位置张贴相应的用电安全操作方法、警示及指引。
d) 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。
e) 未经审批是否禁止接入其他用电设备。

A.3.2.2.5 机房消防

本项要求包括：

a) 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。
b) 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。
c) 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。
d) 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。
e) 是否定期进行消防设施的使用培训和演习。

A.3.3 网络管理

A.3.3.1 网络安全

A.3.3.1.1 结构安全

本项要求包括：

a) 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%。
b) 是否保证接入网络和核心网络的带宽满足业务高峰期需要。（本项适用于：信息系统等级保护二级系统）
c) 是否保证网络各个部分的带宽满足业务高峰期需要。（本项适用于：信息系统等级保护三级系统）
d) 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。（本项适用于：信息系统等级保护三级系统）
e) 是否绘制与当前运行情况相符的网络拓扑结构图；应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。
f) 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。
g) 是否提供关键网络设备、通信线路和数据处理系统的硬件冗余，保证系统的可用性。（本项适用于：信息系统等级保护二级系统）
h) 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，重要网段与其他网段之间采取可靠的技术隔离手段。（本项适用于：信息系统等级保护三级系统）
i) 是否按照对业务服务的重要次序来指定带宽分配优先级别，保证在网络发生拥堵的时候优先保护重要主机。应对所有业务确定重要性、优先级，制定业务相关带宽分配原则及相应的带宽控制策略，根据安全需求，采取网络 QoS 或专用带宽管理设备等措施。（本项适用于：信息系统等级保护三级系统）
j) 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。（本项适用于：信息系统等级保护三级系统）

A.3.3.1.2 访问控制

本项要求包括：

a) 网络边界是否部署访问控制设备并启用访问控制功能。
b) 是否针对数据流提供明确的允许/拒绝访问的访问控制策略，控制力度达到网段级。网络边界访问控制设备应设定过滤规则集。规则集应涵盖对所有出入边界的数据包的处理方式，对于没有明确定义的数据包，应缺省拒绝。（本项适用于：信息系统等级保护二级系统）
c) 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。（本项适用于：信息系统等级保护三级系统）
d) 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。
e) 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。
f) 是否对进出网络的信息内容进行过滤，实现对应用层 HTTP、FTP、TELNET、SMTP、POP3 等协议命令级的控制；对通过互联网传输的信息内容进行过滤，实现对应用层 HTTP、FTP、TELNET、SMTP、POP3 等通用性协议命令级控制。（本项适用于：信息系统等级保护三级系统）
g) 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。（本项适用于：信息系统等级保护三级系统）
h) 是否限制网络最大流量数及网络连接数。（本项适用于：信息系统等级保护三级系统）
i) 重要网段是否采取技术手段防止地址欺骗。（本项适用于：信息系统等级保护三级系统）

j) 是否制定网络访问控制策略，应合理设置网络隔离设施上的访问控制列表，关闭与业务无关的端口；编制文档并保持更新；访问控制策略的变更应履行审批手续。

A.3.3.1.3 安全审计

本项要求包括：

a) 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) 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。
c) 是否能够根据记录数据进行分析，并生成审计报表。（本项适用于：信息系统等级保护三级系统）
d) 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。（本项适用于：信息系统等级保护三级系统）
e) 是否定期检查网络设备的用户、口令及权限设置的正确性。
f) 是否留存网络访问日志。

A.3.3.1.4 边界完整性检查

本项要求包括：

a) 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，准确定出位置，并对其进行有效阻断。（本项适用于：信息系统等级保护二级系统）
b) 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。（本项适用于：信息系统等级保护三级系统）
c) 是否能够对内部网络用户私自联到外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。（本项适用于：信息系统等级保护三级系统）
d) 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.3.3.1.5 入侵防范

本项要求包括：

a) 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。
b) 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应提供报警。（本项适用于：信息系统等级保护三级系统）

A.3.3.1.6 恶意代码防范

本项要求包括：

a) 是否在网络边界处对恶意代码进行检测和清除：（本项适用于：信息系统等级保护三级系统）
   1) 在不严重影响网络性能和业务的情况下，应在网络边界部署恶意代码检测系统；
   2) 如果部署了主机恶意代码检测系统，可选择安装部署网络边界恶意代码检测系统。
b) 是否维护恶意代码库的升级和检测系统的更新。（本项适用于：信息系统等级保护三级系统）

A.3.3.1.7 网络设备防护

本项要求包括：

a) 是否对登录网络设备的用户进行身份鉴别；应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。
b) 是否对网络设备的管理员登录地址进行限制。
c) 网络设备用户的标识是否唯一。
d) 身份鉴别信息是否具有不易被冒用的特点，口令是否有复杂度要求并定期更换；
   1) 口令应符合以下条件：数字、字母、符号混排，无规律的方式；
   2) 管理员用户口令的长度至少为 12 位；
   3) 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；
   4) 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。
e) 是否具有登录失败处理功能，是否采取结束会话、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。
f) 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。
g) 主要网络设备是否对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别：（本项适用于：信息系统等级保护三级系统）
   1) 通过本地控制台管理主要网络设备时，应采用一种或一种以上身份鉴别技术；
   2) 以远程方式登录主要网络设备，应采用两种或两种以上组合的鉴别技术进行身份鉴别。
h) 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。（本项适用于：信息系统等级保护三级系统）

A.3.4 主机和系统管理

A.3.4.1 主机安全

A.3.4.1.1 身份鉴别

本项要求包括：
a) 是否对登录操作系统和数据库系统的用户进行身份标识和鉴别。
b) 操作系统和数据库系统管理用户身份标识是否具有不易被冒用的特点，口令应有复杂度要求并定期更换；
   1) 口令应符合以下条件：数字、字母、符号混排，无规律的方式；
   2) 口令的长度至少为 12 位；
   3) 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；
   4) 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。
c) 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。
d) 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。
e) 是否为操作系统和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：
   1) 应为操作系统的不同用户分配不同的用户名；
   2) 应为数据库系统的不同用户分配不同的用户名。
f) 是否采用两种或两种以上组合的鉴别技术对管理用户进行身份鉴别：（本项适用于：信息系统等级保护三级系统）
   1) 通过本地控制台管理主机设备时，应采用一种或一种以上身份鉴别技术；
   2) 以远程方式登录主机设备，应采用两种或两种以上组合的鉴别技术进行身份鉴别。

A.3.4.1.2 访问控制

本项要求包括：

a) 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。
b) 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。
c) 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。
   1) 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；
   2) 系统无法重命名的特殊默认账户，可不重命名。
d) 是否及时删除多余的、过期的账户，避免共享账户的存在。
e) 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。（本项适用于：信息系统等级保护三级系统）

A.3.4.1.3 安全审计

本项要求包括：

a) 审计范围是否覆盖到服务器上的每个操作系统用户和数据库用户；应在保证系统运行安全和效率的前提，启用系统审计或采用第三方安全审计产品实现审计要求。（本项适用于：信息系统等级保护二级系统）
b) 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。
c) 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。
d) 是否保护审计记录，避免受到未预期的删除、修改或覆盖等。审计记录应至少保存 6 个月。
e) 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和数据库用户；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。（本项适用于：信息系统等级保护三级系统）
f) 是否能够根据记录数据进行分析，并生成审计报表。（本项适用于：信息系统等级保护三级系统）
g) 是否保护审计进程，避免受到未预期的中断。（本项适用于：信息系统等级保护三级系统）
h) 网上基金销售信息系统服务端是否能产生、记录并集中存储必要的日志信息，日志信息至少包含能识别服务请求方身份的内容，如，登录终端的 IP 地址、MAC 地址、手机号码和终端特征码等，并确保数据的可审计性，满足监管部门现场检查要求及司法机构调查取证的要求。

A.3.4.1.4 入侵防范

本项要求包括：

a) 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，应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。
b) 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。（本项适用于：信息系统等级保护三级系统）
c) 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，应停止有关服务，并提供报警。（本项适用于：信息系统等级保护三级系统）

A.3.4.1.5 恶意代码防范

本项要求包括：

a) 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；
   1) 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；
   2) 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。
b) 是否支持防恶意代码软件的统一管理。
c) 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。（本项适用于：信息系统等级保护三级系统）

A.3.4.1.6 资源控制

本项要求包括：

a) 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。
b) 是否根据安全策略设置登录终端的操作超时锁定。
c) 是否限制单个用户对系统资源的最大或最小使用限度。
d) 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。（本项适用于：信息系统等级保护三级系统）
e) 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。（本项适用于：信息系统等级保护三级系统）

A.3.4.2 应用安全

A.3.4.2.1 结构安全

本项要求包括：

a) 网上信息系统服务端是否存在有效屏蔽系统技术错误信息的机制，不将系统产生的错误信息直接反馈给客户。
b) 是否为基金投资人提供自助式前台系统失效时的备用服务措施或方案。

A.3.4.2.2 身份鉴别

本项要求包括：

a) 是否提供专用的登录控制模块对登录用户进行身份标识和鉴别。
b) 是否提供用户身份标识唯一和鉴别信息复杂度检查功能，保证应用系统中不存在重复用户身份标识，身份鉴别信息不易被冒用。
c) 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。
d) 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。
e) 是否对同一用户采用两种或两种以上组合的鉴别技术实现用户身份鉴别：（本项适用于：信息系统等级保护三级系统）
   1) 管理用户通过受控本地控制台管理应用系统时，应采用一种或一种以上身份鉴别技术；
   2) 管理用户以远程方式登录应用系统，应采用两种或两种以上组合的鉴别技术进行身份鉴别；
   3) 面向互联网服务的系统应当提供两种或两种以上组合的鉴别技术供用户选择。

f) 网上信息系统服务端是否能向客户提供可证明服务端自身身份的信息，如提供预留验证信息服务，在网上交易客户登录时回显，帮助客户有效识别仿冒的网上交易信息系统，防范利用仿冒的网上交易信息系统进行诈骗活动。
g) 网上信息系统是否提供可靠的身份验证机制，除采用账号名、口令、验证码的身份认证方式外，是否向客户提供一种以上强度更高的身份认证方式供客户选择使用，如客户端电脑或手机特征码绑定、软硬件证书、动态口令等认证方式，确认客户的身份和登录的合法性，防止不法分子利用木马等黑客程序窃取客户账号和口令。
h) 网上信息系统客户端是否能向客户提示最近一次登录的日期、时间、地址等信息。
i) 是否采取有效技术措施，识别与验证使用网上基金销售业务服务的投资者的真实、有效身份，并应依照与投资者签订的协议对投资者操作权限、资金转移或交易限额等实施有效管理。

A.3.4.2.3 访问控制

本项要求包括：

a) 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、数据库表等客体的访问，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。
b) 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。
c) 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。
d) 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。
e) 核心系统是否有授权管理功能。
f) 是否关闭网上信息系统所有与业务和维护无关的服务及端口，严格控制防火墙中的权限设置，确保按“最小权限原则”进行设置。
g) 对于网上信息系统的内部访问，是否严格限制访问源。
h) 特殊紧急情况下需要通过互联网进行远程操作时，是否通过限制登录 IP、使用数字证书或动态口令、全程监控等措施确保安全，并在操作完成后，及时关闭相关端口。

A.3.4.2.4 安全审计

本项要求包括：

a) 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。
b) 是否采取有效措施防止删除、修改或覆盖审计记录。（本项适用于：信息系统等级保护二级系统）
c) 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。审计记录应至少保存 6 个月。
d) 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。（本项适用于：信息系统等级保护三级系统）
e) 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。（本项适用于：信息系统等级保护三级系统）

A.3.4.2.5 通信完整性

本项要求包括：

a) 通过互联网、卫星网进行通信时，是否采用校验码技术保证通信过程中数据的完整性。（本项适用于：信息系统等级保护二级系统）

b) 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。（本项适用于：信息系统等级保护三级系统）
c) 是否能够检测到鉴别信息和重要业务数据在传输过程中完整性受到破坏。（本项适用于：信息系统等级保护二级系统）
d) 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。（本项适用于：信息系统等级保护三级系统）
e) 网上基金销售信息系统服务端是否具有对数据包被篡改、异常重发等情况的应对能力。

A.3.4.2.6 通信保密性

本项要求包括：

a) 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。
b) 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。
c) 网上客户端的客户身份信息和交易数据等重要数据传输是否采用国家信息安全机构认可的加密技术和加密强度，并最低达到 SSL 协议 128 位的加密强度。
d) 门户网站中客户账号及口令，是否采用加密方式传输，并最低达到 SSL 协议 128 位的加密强度。
e) 网上基金销售信息系统客户端如需与银行等支付系统进行数据通信时，是否使用数字加密技术（如数字证书方式）进行严格的数据加密处理防止数据被篡改。

A.3.4.2.7 抗抵赖

本项要求包括：

a) 是否具有在请求的情况下为数据原发者或接收者提供数据原发证据的功能；应用系统的操作与管理记录，至少应记录操作时间、操作人员及操作类型、操作内容等信息。交易系统应能够记录用户交易行为数据，至少包括业务流水号、账户名、IP 地址、交易指令等信息。（本项适用于：信息系统等级保护三级系统）
b) 是否具有在请求的情况下为数据原发者或接收者提供数据接收证据的功能。应用系统的操作与管理记录，至少应记录操作时间、操作人员及操作类型、操作内容等信息。交易系统应能够记录用户交易行为数据，至少包括业务流水号、账户名、IP 地址、交易指令等信息。（本项适用于：信息系统等级保护三级系统）

A.3.4.2.8 软件容错

本项要求包括：

a) 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。
b) 在故障发生时，应用系统是否能够继续提供一部分功能，确保能够实施必要的措施。（本项适用于：信息系统等级保护二级系统）
c) 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。（本项适用于：信息系统等级保护三级系统）

A.3.4.2.9 资源控制

本项要求包括：

a) 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，另一方是否能够自动结束会话。用户登录应用系统后在规定的时间内未执行任何操作，应自动退出系统。
b) 是否能够对系统的最大并发会话连接数进行限制。
c) 是否能够对单个账户的多重并发会话进行限制。
d) 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。（本项适用于：信息系统等级保护三级系统）
e) 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。(本项适用于：信息系统等级保护三级系统）
f) 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。（本项适用于：信息系统等级保护三级系统）
g) 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。（本项适用于：信息系统等级保护三级系统）
h) 网上信息系统服务端是否监控并能够抵御连续猜测，避免攻击者通过群体大规模对合法证券账户进行非法用户登陆的请求，导致大量用户账户被异常锁定，正常用户无法登录。

A.3.4.3 数据安全及备份恢复

A.3.4.3.1 数据完整性

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存储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。（本项适用于：信息系统等级保护三级系统）

A.3.4.3.2 数据保密性

本项要求包括：

a) 是否采用加密或其他保护措施实现鉴别信息的存储保密性。（本项适用于：信息系统等级保护二级系统）
b) 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。（本项适用于：信息系统等级保护三级系统）
c) 网上基金销售机构是否保证网上基金数据传输的保密性、完整性、真实性和可稽核性，对网上基金交易的客户信息、交易信息及其他敏感信息进行可靠的加密，且不存在任何中间环节对数据进行加解密处理。

A.3.4.3.3 备份和恢复

本项要求包括：

a) 履行基金份额登记职责的，是否妥善保存登记数据，保证登记数据的真实、准确、完整，不得隐匿、伪造、篡改或者毁损，并将基金份额持有人名称、身份信息及基金份额明细等数据备份至国务院证券监督管理机构认定的机构。其保存期限自基金账户销户之日起不得少于 20 年。
b) 系统运行数据中涉及基金投资人信息和交易记录的备份是否在不可修改的介质上保存 15 年。

A.3.5 运维管理

A.3.5.1 系统建设管理

A.3.5.1.1 系统定级

本项要求包括：

a) 是否明确信息系统的边界和安全保护等级。
b) 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。
c) 是否确保信息系统的定级结果经过相关部门的批准。
d) 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。（本项适用于：信息系统等级保护三级系统）
e) 定级结果是否经过相关部门批准，由住所地证监局出具定级审核意见。

A.3.5.1.2 方案设计

本项要求包括：
a) 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。
b) 是否以书面形式描述对系统的安全保护要求、策略和措施等内容，形成系统的安全方案。（本项适用于：信息系统等级保护二级系统）
c) 是否对安全方案进行细化，形成能指导安全系统建设、安全产品采购和使用的详细设计方案。（本项适用于：信息系统等级保护二级系统）
d) 是否组织相关部门和有关安全技术专家对安全设计方案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。（本项适用于：信息系统等级保护二级系统）
e) 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。（本项适用于：信息系统等级保护三级系统）
f) 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。（本项适用于：信息系统等级保护三级系统）
g) 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。（本项适用于：信息系统等级保护三级系统）
h) 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。（本项适用于：信息系统等级保护三级系统）
i) 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。
j) 在系统开发和运行中是否采用已颁布的行业标准和数据接口。

A.3.5.1.3 产品采购和使用

本项要求包括：
a) 是否确保安全产品采购和使用符合国家的有关规定。
b) 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。
c) 是否指定或授权专门的部门负责产品的采购。
d) 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。（本项适用于：信息系统等级保护三级系统）

A.3.5.1.4 自行软件开发

本项要求包括：
a) 开发环境是否与实际运行环境物理分离。（本项适用于：信息系统等级保护二级系统）
b) 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。

c) 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。
d) 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。应保证同一组件或子系统的开发人员和测试人员分离。（本项适用于：信息系统等级保护三级系统）
e) 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。（本项适用于：信息系统等级保护三级系统）
f) 是否对程序资源库的修改、更新、发布进行授权和批准。（本项适用于：信息系统等级保护三级系统）

A.3.5.1.5 外包软件开发

本项要求包括：
a) 是否根据开发要求测试软件质量。
b) 是否确保提供软件设计的相关文档和使用指南。
c) 是否在软件安装之前检测软件包中可能存在的恶意代码。
d) 要求开发单位提供软件源代码，并审查软件中可能存在的后门。

A.3.5.1.6 工程实施

本项要求包括：
a) 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。
b) 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。
c) 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。（本项适用于：信息系统等级保护三级系统）

A.3.5.1.7 系统交付

本项要求包括：
a) 是否向用户提供系统建设文档和运行维护所需文档。
b) 是否书面规定系统交付的控制方法和人员行为准则。（本项适用于：信息系统等级保护三级系统）
c) 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。（本项适用于：信息系统等级保护三级系统）
d) 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。
e) 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。
f) 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。
g) 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。

A.3.5.1.8 测试验收

本项要求包括：
a) 是否对系统进行安全性测试验收。（本项适用于：信息系统等级保护二级系统）
b) 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。
c) 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。

d) 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。（本项适用于：信息系统等级保护三级系统）
e) 是否书面规定系统测试验收的控制方法和人员行为准则。（本项适用于：信息系统等级保护三级系统）
f) 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。（本项适用于：信息系统等级保护三级系统）
g) 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。
h) 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。
i) 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。模拟环境应与生产环境进行有效隔离，不得对生产环境进行干扰。
j) 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。
k) 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。
l) 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。
m) 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。
n) 是否提前发布生产环境测试的系统测试公告。
o) 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。
p) 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。
q) 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。
r) 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。
s) 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。
t) 测试后是否恢复生产环境并验证恢复的有效性。
u) 是否禁止交易时段使用生产环境进行测试。
v) 基金销售业务信息系统升级时是否与基金管理人、基金注册登记机构等进行联网测试。

A.3.5.1.9 系统备案

本项要求包括：

a) 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。（本项适用于：信息系统等级保护三级系统）
b) 经营机构是否将系统等级及相关材料报住所地证监局备案。
c) 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.3.5.1.10 等级测评

本项要求包括：

a) 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。（本项适用于：信息系统等级保护三级系统）
b) 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。（本项适用于：信息系统等级保护三级系统）

c) 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。（本项适用于：信息系统等级保护三级系统）
d) 是否指定或授权专门的部门或人员负责等级测评的管理。（本项适用于：信息系统等级保护三级系统）
e) 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.3.5.2 系统运维管理

A.3.5.2.1 值班管理

本项要求包括：

a) 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。
b) 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。
c) 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。
d) 是否制定交接班流程，并严格执行，留存记录。
e) 是否设置运维值班电话，并保持畅通。

A.3.5.2.2 文档管理

本项要求包括：

a) 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。
b) 是否明确文档管理的责任人。
c) 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。
d) 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。
e) 是否对超范围、超权限使用文档时，保存相关审批、使用记录。
f) 是否妥善保存网上基金销售信息系统关键软件的日志文件，并定期检查、审核记录。

A.3.5.2.3 资产管理

本项要求包括：

a) 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。
b) 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。
c) 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。（本项适用于：信息系统等级保护三级系统）
d) 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。（本项适用于：信息系统等级保护三级系统）

A.3.5.2.4 数据与介质管理

本项要求包括：

a) 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。
b) 是否对介质归档和查询等过程进行记录，并根据存档介质的目录清单定期盘点。（本项适用于：信息系统等级保护二级系统）
c) 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。
d) 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。
e) 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。
f) 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，应按国家相关规定另行处理。
g) 是否根据数据备份的需要对某些介质实行异地存储，存储地的环境要求和管理方法应与本地相同。（本项适用于：信息系统等级保护三级系统）
h) 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。（本项适用于：信息系统等级保护三级系统）
i) 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。
j) 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。
k) 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。
l) 在线数据管理，是否做到如下要求：
    1) 交易业务系统数据应至少每交易日备份一次；
    2) 交易业务系统历史数据至少保留一年；
    3) 未经授权不得访问、复制；
    4) 对数据的修改应通过审批，双岗操作并记录操作日志。
m) 离线数据管理，是否做到如下要求：
    1) 离线数据不得更改；
    2) 应至少每季度对核心交易业务系统的备份数据进行一次有效性验证，如发现问题应采取措施修复备份数据，并查明原因；
    3) 离线数据的调阅、复制、传输、查询，应按照拟定的流程办理审批手续，并进行登记；
    4) 备份数据带离存储环境时应采取必要的安全措施。
n) 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。
o) 离线备份介质是否在本地机房、同城、异地安全可靠存放。
p) 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。
q) 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。

A.3.5.2.5 设备和软件管理

本项要求包括：

a) 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。

b) 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。
c) 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。
d) 信息处理设备是否经过审批才能带离机房或办公地点。
e) 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。（本项适用于：信息系统等级保护三级系统）
f) 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。
g) 是否明确设备和软件管理责任人。
h) 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。
i) 是否编制信息系统设备清单，主要包括设备名称、设备编号、入库时间、设备主要参数、设备序列号、设备状态、设备保修期、设备位置、设备用途和设备使用责任人等内容，并保留设备启用、转移、维修、报废等过程的记录。
j) 是否使用正版软件并保存软件授权证书和许可协议，应编制软件清单，主要包括软件名称、软件编号、入库时间、软件版本，授权和许可情况、软件序列号、软件状态、软件维护期、软件安装设备、用途和使用责任人等内容，并保留软件启用、转移、升级、报废等过程的记录。
k) 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。
l) 是否对外送设备的维修进行严格管理，防止数据泄露。
m) 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.3.5.2.6 变更管理

本项要求包括：

a) 是否确认系统中要发生的变更，并制定相应的变更方案；重要系统变更前应制定详细的变更方案、失败恢复方案、专项应急预案。
b) 系统发生重要变更前，是否向主管领导申请，审批后方可实施变更，并在实施后向相关人员通告。（本项适用于：信息系统等级保护二级系统）
c) 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。（本项适用于：信息系统等级保护三级系统）
d) 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。（本项适用于：信息系统等级保护三级系统）
e) 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。（本项适用于：信息系统等级保护三级系统）
f) 是否建立系统变更流程，对信息系统的变更活动进行规范。
g) 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。
h) 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。
i) 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。
j) 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。

k) 是否按照测试方案，组织变更前后的测试，测试后应提交测试记录或报告。
l) 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。
m) 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。

A.3.5.2.7 配置管理

本项要求包括：

a) 是否制定配置管理流程，明确配置管理负责人。
b) 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。
c) 配置库中配置项的属性是否至少包括以下信息。
   1) 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；
   2) 配置项编号应唯一；
   3) 配置项的添加、修改、替换、删除应有变更记录；
   4) 应保存配置项历史记录，确保与事件管理、问题管理、变更管理等流程记录的关联性。
d) 是否定期对配置库进行备份。
e) 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。
f) 是否建立针对网上基金销售信息系统的配置管理制度，完整、真实地记录和反映系统所涉及的软硬件配置及相互影响关系，并保持与实际生产环境同步更新。

A.3.5.2.8 日常操作

本项要求包括：

a) 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。
b) 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。
c) 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。
d) 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。
e) 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。
f) 是否对核心交易业务系统设置独立的操作和监控环境，与开发、测试等其他操作环境严格分离。
g) 注册邮箱账号是否经过审批。

A.3.5.2.9 口令管理

本项要求包括：

a) 用户和口令管理是否符合如下要求：
   1) 不得设置弱口令，若系统条件允许，口令应采用数字、字母、符号混排且无规律的方式，管理员口令长度原则上不低于 12 位；核心交易业务系统应提示并阻止用户使用弱口令登录；
   2) 应每季度对管理员口令进行修改，更新的管理员口令至少 5 次内不能重复；
   3) 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；
   4) 应重点加强对匿名/默认用户的管理，防止被非法使用；

5) 应及时注销不再使用的账户；
6) 应明确责任人，负责统一保管、安全存放管理员口令，不得泄漏。

b) 网上基金销售信息系统客户端是否具有基金客户交易口令复杂度控制和提醒机制，提醒客户定期修改口令；系统自动生成的初始口令，必须有最小生存期限制或强制客户修改，禁止系统自动生成相同口令或弱口令；基金客户口令的修改和取回操作要有日志记录。

A.3.5.2.10 数据库管理

本项要求包括：

a) 是否保持数据库的可用性，及时维护、更新软件。
b) 是否负责数据库的参数配置、调优，编制文档并保持更新。
c) 是否定期对数据库容量进行检查和评估，形成评估报告。
d) 是否负责管理数据库、表、索引、存储过程，数据库的升级、优化、扩容、迁移。
e) 是否定期检查数据库的用户、口令及权限设置的正确性。

A.3.5.2.11 终端信息

本项要求包括：

a) 向客户提供的交易终端软件，是否采取适当的技术，确保软件能够采集到客户交易终端电话号码、互联网通讯协议地址（IP 地址）、媒介访问控制地址（MAC 地址）以及其他能识别客户交易终端的特征代码。
b) 向客户提供的交易终端软件，是否采取适当的技术，确保软件能够采集到客户交易终端信息。由第三方提供交易终端软件的，应当建立软件认证许可制度，要求第三方采取适当的技术，确保软件能够采集到客户交易终端信息。客户交易终端软件应当具备先提醒升级、再自动升级为最新版本的功能。
c) 网上交易、语音交易、自助交易等外围信息系统是否逐笔记录交易委托、密码修改、账户登录等操作的客户交易终端信息。
d) 是否为证券交易所或登记结算机构采集客户交易终端信息提供相应的数据接口，并在相关技术规范发布之日起 12 个月内，完成信息系统的改造升级，改造后的信息系统应符合国家信息安全标准。
e) 是否按照本规定的要求建设、改造和维护相关信息系统，以妥善管理客户交易终端信息，并提供符合技术规范的查询接口。应当采取必要的技术手段，满足交易时段客户信息查询的需要。
f) 是否按照技术规范对客户的主要开户资料进行电子化，并妥善保存在信息系统中。应当按照技术规范在 18 个月内对新增账户实施开户资料电子化，存量的正常交易类账户应在 36 个月内完成开户资料电子化。
g) 是否妥善保存客户交易终端信息和开户资料电子化信息，保存期限不得少于 20 年。应妥善保存交易时段客户交易区的监控录像资料，保存期限不得少于 6 个月。
h) 是否采取可靠的措施，采集、记录、存储、报送与客户身份识别有关的信息，不得以任何理由拒绝承担相应职责。公司及其工作人员应当对客户交易终端信息予以保密，不得泄露。
i) 是否严格限制对客户交易终端信息的人工操作权限，明确查询权限和操作流程，建立日志文档并指定专人妥善保管。禁止任何人对客户交易终端信息进行隐匿、伪造、篡改或毁损。
j) 发生影响采集、记录、存储、报送客户交易终端信息安全的重大事件时，是否及时向公司住所地和事件发生地证监局报告，不得隐瞒。

A.3.5.2.12 督促检查

本项要求包括：

a) 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。
b) 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。
c) 是否每季组织开展内部检查，形成检查报告。
d) 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。
e) 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。
f) 是否对检查和审计的结果采取纠正性和预防性的措施。
g) 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.3.5.2.13 监控分析

本项要求包括：

a) 是否应采取监控措施，配备监控和报警工具，对影响信息系统正常运行的关键对象，包括机房环境、网络、通信线路、主机、存储、数据库、核心交易业务相关的应用系统、安全设备等进行监控，形成记录并妥善保存。报警方式可包括声光、电话、短信、邮件等。
b) 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。（本项适用于：信息系统等级保护三级系统）
c) 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。（本项适用于：信息系统等级保护三级系统）
d) 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，应开启自动监控系统和自动报警系统。
e) 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。
f) 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。
g) 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。
h) 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。
i) 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。
j) 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。
k) 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。
l) 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。
m) 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。
n) 门户网站监控指标是否包括网页内容、日均访问量等。
o) 是否针对不同系统设置合理的监测频度。

p) 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。
q) 是否保存监控产生的日志，保存时间不少于一年。
r) 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。应至少每季度全面评估监控日志和操作记录，分析异常情况，形成评估报告。
s) 网上基金销售信息系统服务端是否能够提供系统运行状况信息(如活动状态、并发在线客户数目、并发会话数目、线程数目、队列长度等)、错误信息、安全警告等。
t) 是否建立完善的监控体系，对系统升级、网络访问、数据库存取、用户密码修改等重要操作要进行记录并妥善保存日志文件。

A.3.5.2.14 网络安全管理

本项要求包括：

a) 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。
b) 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。
c) 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；应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。
d) 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；
   1) 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；
   2) 实施漏洞扫描或漏洞修补前，应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；
   3) 漏洞扫描或漏洞修补后应进行验证测试，以保证网络系统的正常运行。
e) 是否保证所有与外部系统的连接均得到授权和批准。
f) 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；应在配置变更前、变更后分别对网络设备的配置文件进行备份。（本项适用于：信息系统等级保护三级系统）
g) 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。（本项适用于：信息系统等级保护三级系统）
h) 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。（本项适用于：信息系统等级保护三级系统）
i) 是否合理设置安全域，绘制网络拓扑图，并保持更新。
j) 是否配置、调优网络系统的参数。
k) 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。
l) 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；应正确设置安全设备的接口参数和过滤规则。
m) 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。
n) 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，特殊紧急情况下应采取限制登录 IP、数字证书或动态口令认证、全程监控等措施，在操作完成后应及时关闭，并对维护过程进行监控并留存记录。
o) 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。
p) 是否禁止通过无线网络对交易业务网进行网络管理。

q) 计算机网络跳线是否整齐干净，跳线标识清晰。
r) 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。
s) 是否保持网络设备的可用性，及时维修、更换故障设备。
t) 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.3.5.2.15 系统安全管理

本项要求包括：

a) 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。
b) 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。
c) 是否安装系统的最新补丁程序，在安装系统补丁前，应首先充分评估并在测试环境中测试通过，并对重要文件进行备份后，方可实施系统补丁程序的安装；持续跟踪厂商提供的系统升级更新情况，应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。
d) 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。
e) 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。
f) 是否至少每月对运行日志和审计数据进行分析。
g) 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，权限设定应当遵循最小授权原则。（本项适用于：信息系统等级保护三级系统）
h) 系统管理是否包括：
   1) 应保持系统的可用性，及时维修、更换故障设备和更新软件；
   2) 应负责应用系统、操作系统的参数配置、调优，编制文档并保持更新；
   3) 应定期对系统容量进行检查和评估，形成评估报告；
   4) 应负责管理系统和应用程序服务进程，并关闭与业务无关的服务；
   5) 应定期检查应用系统、操作系统的用户、口令及权限设置的正确性。
i) 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。
j) 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。
k) 是否采取有效措施对门户网站上提供下载的网上证券客户端软件程序进行保护，客户端软件程序编译封装、形成下载文件后，应安排专人对其进行严格的病毒扫描和木马检查，并通过专用安全手段传输至网站文件下载服务器。

A.3.5.2.16 恶意代码防范

本项要求包括：

a) 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。
b) 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。
c) 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。
d) 是否定期检查信息系统内各种产品的恶意代码库的升级情况并进行记录，对主机防病毒产品、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及时分析处理，并形成书面的报表和总结汇报。（本项适用于：信息系统等级保护三级系统）

e) 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。
f) 网上交易软件是否采取安全的密码输入方式，增强防御恶意程序窃取密码的功能。
g) 是否建立定期的网上信息系统安全风险评估机制和整改的工作制度，及时发现 SQL 注入漏洞、弱口令账户、绕过验证、目录遍历、文件上传、跨站脚本、Session 欺骗、拒绝式服务攻击和缓冲区溢出等系统存在的安全隐患和漏洞，并进行改进和完善。风险评估应通过内部评估与外部评估相结合的方式进行。
h) 基金销售机构是否定期进行网上基金销售系统的漏洞扫描和渗透测试工作，及时发现系统中存在的各种安全问题并及时修补。

A.3.5.2.17 密码管理

本项要求包括：
a) 是否使用符合国家密码管理规定的密码技术和产品。（本项适用于：信息系统等级保护二级系统）
b) 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。（本项适用于：信息系统等级保护三级系统）
c) 网上基金销售信息系统客户端是否禁止在客户本地计算机储存客户账户、口令等重要信息。存储其他信息应当提示客户，本地数据存储只是参考数据，应当以基金销售机构记录数据为最终准确数据。

A.3.5.2.18 备份与恢复管理

本项要求包括：
a) 是否识别需要定期备份的重要业务信息、系统数据及软件系统等。
b) 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。
c) 是否根据数据的重要性及其对系统运行的影响，制定数据的备份策略和恢复策略，备份策略指明备份数据的放置场所、文件命名规则、介质替换频率和数据离站运输方法。
d) 是否建立控制数据备份和恢复过程的程序，对备份过程进行记录，所有文件和记录应妥善保存。（本项适用于：信息系统等级保护三级系统）
e) 是否定期执行恢复程序，检查和测试备份介质的有效性，确保可以在恢复程序规定的时间内完成备份的恢复。（本项适用于：信息系统等级保护三级系统）
f) 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；每季度至少对数据备份进行一次有效性验证。
g) 开放式基金注册登记系统、投资交易系统、网上交易系统、直销系统、基金估值核算系统等核心系统备份能力是否不低于《证券期货经营机构信息系统备份能力标准》第三级要求。
h) 是否制定信息系统备份能力建设工作计划。
i) 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。

A.3.5.2.19 业务连续性

在公司灾备系统和业务连续性计划中是否包括网上基金销售系统。

A.3.5.2.20 事件与问题管理

本项要求包括：
a) 是否对安全检查情况进行评估，形成评估报告。

b) 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。
c) 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。
d) 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。
e) 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。
f) 是否每月回顾、分析事件处理记录，完成事件分析报告。
g) 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。
h) 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。
i) 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。
j) 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。
k) 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。

A.3.5.2.21 网站安全

本项要求包括：

a) 是否建立对门户网站内容的审核制度、完整的发布流程和监控机制。
b) 是否对网页内容进行监控，对有害信息进行过滤，防止网站出现不良信息。
c) 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。
d) 是否采取有效措施监控门户网站防止被篡改。当网站上的页面内容、提供给投资者下载的客户端软件及其他文件被异常修改时，能及时发现并恢复。
e) 门户网站是否按照国家主管部门的有关规定办理 ICP 备案，在网站首页公布 ICP 备案号，并提供备案信息的链接。
f) 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。

A.3.5.2.22 软件正版化

本项要求包括：

a) 是否明确部门或责任人，负责本单位软件正版化工作。
b) 是否落实软件采购经费，做好软件正版化工作。
c) 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。
d) 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。
e) 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。
f) 是否每年对软件正版化情况开展自查。
g) 操作系统软件是否有授权（服务器）。
h) 操作系统是否有授权（办公计算机）。
i) 数据库软件是否有授权。
j) 杀毒软件是否有授权。
k) 办公文字处理软件是否有授权。
l) 办公专业处理软件是否有授权。
m) 应用服务器软件是否有授权。
n) 专用业务软件是否有授权。

o) 是否制定了软件正版化计划。

A.3.5.3 应急处置

A.3.5.3.1 应急准备

本项要求包括：

a) 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。
b) 是否对系统相关的人员进行应急预案培训，应急预案的培训应至少每年举办一次。
c) 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。（本项适用于：信息系统等级保护三级系统）
d) 是否定期对应急预案进行演练，根据不同的应急恢复内容，确定演练的周期；应至少每年对应急预案进行演练。（本项适用于：信息系统等级保护三级系统）
e) 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。（本项适用于：信息系统等级保护三级系统）
f) 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。
g) 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。
h) 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。
i) 是否制定了网络与信息安全事件应急预案，内容至少包括：
   1) 应急预案编制的目的和依据；
   2) 应急预案的适用范围；
   3) 应急处置的组织体系及职责；
   4) 预防措施、保障措施与应急准备；
   5) 预警监测、处置和信息报送；
   6) 网络与信息安全事件的分级分类；
   7) 网络与信息安全事件的报告流程；
   8) 网络与信息安全事件处置的一般原则；
   9) 网络与信息安全事件处置的具体方案；
   10) 网络与信息安全事件内部调查处理以及分析总结的要求。
j) 应急预案是否符合如下要求：
   1) 网络与信息安全事件处置的具体方案应包括各种可能发生的技术故障的应急处置流程、报告流程等；
   2) 应针对各种技术故障拟定统一的解释口径和通知公告模板；
   3) 应每年至少进行一次评估，并及时修订；
   4) 应根据应急演练的情况进行评估和更新；
   5) 应向住所地证监局报备；
   6) 在应急预案发生重大变化时，应及时重新报备。
k) 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。
l) 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。

m) 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。
n) 是否建立有效的应急通讯联络系统，确保信息畅通。
o) 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。
p) 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。
q) 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。
r) 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。
s) 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。
t) 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。
u) 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。
v) 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。
w) 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。
x) 是否每半年至少组织一次网络与信息安全应急演练。
y) 是否记录演练情况，演练记录至少保存两年。
z) 是否对演练中发现的问题进行改进。
aa) 是否每年向住所地证监局报告年度应急演练情况。
bb) 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。
cc) 网上信息系统应急预案是否针对电力、通信等基础设施故障、计算机硬件或网络设备故障、操作系统或应用系统故障、操作系统或应用系统漏洞、病毒入侵、恶意攻击、误操作、不可抗力等可能的故障原因制定对应的应急恢复操作流程或步骤。
dd) 基金销售机构是否建立网上基金销售信息系统应急处置组织体系，并有针对性地制定应急预案，应急预案应纳入基金销售机构的整体应急预案体系内，并按照有关规定进行演练。
ee) 是否根据网上基金销售信息系统故障的影响和损失情况对应急组织体系和应急预案进行分级管理，并遵循统一领导、快速响应、协调配合、最小损失的原则。

A.3.5.3.2 应急处置

本项要求包括：

a) 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。
b) 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。
c) 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。

d) 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。
e) 是否记录并保存所有报告的安全弱点和可疑事件，分析事件原因，监督事态发展，采取措施避免安全事件发生。（本项适用于：信息系统等级保护二级系统）
f) 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。（本项适用于：信息系统等级保护三级系统）
g) 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。（本项适用于：信息系统等级保护三级系统）
h) 是否做好应急处置的相关记录，保留有关证据。
i) 是否对造成系统中断和造成信息泄密的安全事件应采用不同的处理程序和报告程序。（本项适用于：信息系统等级保护三级系统）
j) 是否对证券期货行业内通报的重大安全隐患，应立即进行专项安全检查。
k) 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。
l) 是否在应急处置中注意保证工作人员的人身安全。
m) 是否在应急处置结束前，保证专人 24 小时值班。
n) 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。
o) 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。
p) 因系统变更而导致的网上基金销售服务暂停，是否提前向投资者公告。

A.3.5.3.3 调查处理

本项要求包括：

a) 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。事件总结报告内容应当包括：
   1) 事件基本情况，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；
   2) 应急处置情况，包括事件报告的情况、采取的措施及效果；
   3) 事件调查情况，包括事件原因、事件级别、责任认定和结论；
   4) 事件处理情况，包括事件暴露出的问题及采取的整改措施，责任追究情况。
b) 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。
c) 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。
d) 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。
e) 是否向住所地中国证监会派出机构进行预警报告、应急报告和事件总结报告，分支机构应当向所在地中国证监会派出机构进行预警报告、应急报告和事件总结报告。事件总结报告同时抄送中国证券投资基金业协会。

f) 发生信息安全事件影响到证券期货交易业务时，是否同时向相关证券期货交易所进行应急报告和事件总结报告；影响到证券登记结算业务时，应当同时向中国证券登记结算公司进行应急报告和事件总结报告；影响到其他机构的，应当及时向有关机构进行应急通报。
g) 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.4 期货公司系统运行安全审计项汇总

A.4.1 组织管理

A.4.1.1 安全管理制度

A.4.1.1.1 管理制度

本项要求包括：
a) 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。
b) 是否建立安全管理制度，覆盖安全策略的制定、实施、检查、评估、改进等全过程。
c) 是否形成由安全策略、管理制度、操作规程等构成的全面的信息安全管理制度体系。（本项适用于：信息系统等级保护三级系统）
d) 是否对安全管理人员或操作人员执行的日常管理操作建立操作规程。
e) 是否制定覆盖运维工作各个环节的、体系化的运维管理制度和操作流程。运维管理制度包括但不限于：机房管理、网络与系统管理、数据和介质管理、交付管理、测试管理、配置管理、安全管理、值班管理、监控管理、文档管理、设备和软件管理、供应商管理、关联单位关系管理、检查审计等制度。运维操作流程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。
f) 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。

A.4.1.1.2 制定和发布

本项要求包括：
a) 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。
b) 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。
c) 安全管理制度是否具有统一的格式，并进行版本控制。（本项适用于：信息系统等级保护三级系统）
d) 是否建立信息发布管理审核制度；安全管理制度是否通过正式、有效的方式发布。
e) 安全管理制度是否注明发布范围，并对收发文进行登记。（本项适用于：信息系统等级保护三级系统）

A.4.1.1.3 评审和修订

本项要求包括：
a) 信息安全领导小组是否负责定期组织相关部门和相关人员对安全管理制度体系的合理性和适用性进行审定；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。（本项适用于：信息系统等级保护三级系统）

b) 是否定期或不定期对安全管理制度进行检查和审定，对存在不足或需要改进的安全管理制度进行修订。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。

c) 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.4.1.2 安全管理机构

A.4.1.2.1 机构设置

本项要求包括：

a) 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。

b) 是否设立 IT 治理委员会或类似机构，负责公司 IT 治理工作。

c) IT 治理委员是否包括公司 IT 治理直接责任人、IT 总监、IT 部门负责人、相关业务负责人、财务负责人、内部控制负责人以及部分技术骨干等人员，其中 IT 人员的比例是否在 30%以上。

d) IT 治理委员会是否履行以下职责：

1) 拟订公司 IT 治理目标和 IT 治理工作计划；
2) 审议公司 IT 发展规划；
3) 审议公司年度 IT 工作计划和 IT 预算；
4) 审议公司重大 IT 项目立项、投入和优先级；
5) 审议公司 IT 管理制度和重要流程；
6) 制订与 IT 治理相关的培训和教育工作计划；
7) 检查所拟订和审议事项的落实和执行情况；
8) 组织评估公司 IT 重大事项并提出处置意见；
9) 向公司管理层报告 IT 治理状况。

A.4.1.2.2 岗位设置

本项要求包括：

a) 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。

b) 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。

c) 是否设有技术部门并有专职技术人员，并有明确的职责分工和岗位说明。

d) 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。（本项适用于：信息系统等级保护三级系统）

e) 是否合理设置运维岗位，规定岗位职责及技能要求，并符合如下要求：

1) 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；
2) 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。

f) 公司是否设立内部审计岗位，定期对 IT 流程执行情况进行审计。（本项适用于：四类期货公司）

g) 网络、主机、数据库、应用系统的运行维护等关键技术岗位是否有备岗人员。（本项适用于：二类、三类、四类期货公司）

h) 是否指定专人负责保管业务数据备份介质。

i) 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。

j) 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.4.1.2.3 人员配备

本项要求包括：

a) 是否配备系统管理员、网络管理员、安全管理员等；每个岗位应有备岗。
b) 安全管理员是否禁止兼任网络管理员、系统管理员、数据库管理员。（本项适用于：信息系统等级保护二级系统）
c) 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。
d) 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。
e) 关键事务岗位是否配备多人共同管理。（本项适用于：信息系统等级保护三级系统）
f) 公司是否配备足够的信息技术人员，公司的IT工作人员总数是否不少于公司员工总人数的8%。
g) 总部技术部门人员是否不少于5人，对于开展连续交易的期货公司应达到7人。（本项适用于：一类期货公司）
h) 总部技术部门人员是否不少于8人，对于开展连续交易的期货公司应达到11人。（本项适用于：二类期货公司）
i) 总部技术部门人员是否不少于11人，对于开展连续交易的期货公司应达到16人。（本项适用于：三类期货公司）
j) 总部技术部门人员是否不少于15人，对于开展连续交易的期货公司应达到20人。（本项适用于：四类期货公司）
k) 是否设立2名技术联络员，负责组织、协调和处理与信息安全管理部门、交易所及相关单位的各项技术事宜。
l) 总部技术部门是否有至少1名安全管理人员。
m) 每个营业部是否配备至少1名技术人员。
n) 总部技术部门是否有至少1名网络管理人员。（本项适用于：二类期货公司）
o) 总部技术部门是否有至少2名网络管理人员。（本项适用于：三类、四类期货公司）
p) 总部技术部门人员50%以上是否有信息技术相关专业大学本科或以上教育背景。
q) 总部技术部门人员4人以上是否具备1年及以上的系统运行维护经验。（本项适用于：二类期货公司）
r) 总部技术部门人员6人以上是否具备2年及以上的系统运行维护经验。（本项适用于：三类期货公司）
s) 总部技术部门人员8人以上是否具备2年及以上的系统运行维护经验。（本项适用于：四类期货公司）
t) 是否有应急技术支援队伍。

A.4.1.2.4 授权和审批

本项要求包括：

a) 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。
b) 是否针对关键活动建立审批流程，并由批准人签字确认。（本项适用于：信息系统等级保护二级系统）
c) 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。（本项适用于：信息系统等级保护三级系统）

d) 是否定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息；每年至少审查一次审批事项。（本项适用于：信息系统等级保护三级系统）
e) 是否记录审批过程并保存审批文档。（本项适用于：信息系统等级保护三级系统）
f) 权限分配是否有审批和完整的记录，权限设置后应复核。
g) 是否按照最小安全访问原则分配用户权限。
h) 是否建立权限分配表，对用户的访问权限进行合理分配，对文件系统访问权限进行合理设置，编制文档并保持更新。
i) 是否在用户账户变化时，同时变更或撤销其权限。
j) 是否定期检查权限设置的有效性。
k) 是否避免使用超级管理员账户完成日常业务操作。

A.4.1.2.5 供应商管理

本项要求包括：

a) 是否确保安全服务商的选择符合国家、行业的有关规定。
b) 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。
c) 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。
d) 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。
e) 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。
f) 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，明确供应商应接受证券期货行业监管部门的信息安全延伸检查。
g) 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。
h) 是否加强运维外包服务管理，主要包括：
   1) 与外包公司及外包人员签订保密协议；
   2) 明确外包公司应当承担的责任及追究方式；
   3) 明确界定外包人员的工作职责、活动范围、操作权限；
   4) 对外包人员工作情况进行监督和检查，并保留相应记录；
   5) 对驻场外包人员的入场和离场进行管理；
   6) 定期评估外包的服务质量；制定外包服务意外终止的应急措施。
i) 是否有信息技术服务提供商的准确联系方式。
j) 营业部是否有总部和信息技术服务提供商的准确联系方式。
k) 选择信息技术服务提供商时是否评估其资质、经营行为、业绩、服务体系和服务品质等要素。
l) 是否要求交易系统供应商提供交易、银期及相关查询接口。
m) 是否请有资质的专业安全机构定期对网上交易系统提供安全评估或扫描服务，并对安全漏洞进行整改。（本项适用于：三类、四类期货公司）

A.4.1.2.6 关联单位关系管理

本项要求包括：

a) 是否加强各类管理人员之间、组织内部机构之间以及信息安全职能部门内部的合作与沟通。（本项适用于：信息系统等级保护二级系统）

b) 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。
c) 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。（本项适用于：信息系统等级保护三级系统）
d) 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。（本项适用于：信息系统等级保护三级系统）
e) 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。（本项适用于：信息系统等级保护三级系统）
f) 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。

A.4.1.2.7 客户关系管理

本项要求包括：

是否在与客户签订的服务合同、经纪合同及补充协议、风险揭示书等中载明，客户使用网上交易可能面临的风险、公司采取的风险控制措施、客户应采取的风险控制措施以及相关风险对应的责任承担（如防止用于网上交易的计算机或手机终端感染木马、病毒，以免被恶意程序窃取口令；加强帐号、口令的保护，不使用简单口令、定期修改口令、输入口令时防止他人偷看、不对他人泄露口令等）。

A.4.1.2.8 审核和检查

本项要求包括：

a) 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。安全检查应至少每季度一次。
b) 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；全面安全检查应至少每年一次。（本项适用于：信息系统等级保护三级系统）
c) 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。（本项适用于：信息系统等级保护三级系统）
d) 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。（本项适用于：信息系统等级保护三级系统）

A.4.1.3 经费和人员管理

A.4.1.3.1 经费投入

本项要求包括：

a) 最近三个财政年度IT投入平均数额是否不少于最近三个财政年度平均净利润的6%或不少于最近三个财政年度平均营业收入的3%，取二者数额较大者。
b) 是否制定信息系统运行维护年度预算计划，每年进行核算。预算和核算应接受监督和审计。
c) 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。

d) 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。

A.4.1.3.2 人员录用

本项要求包括：

a) 是否指定或授权专门的部门或人员负责人员录用。
b) 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。
c) 是否与开发、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。
d) 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。（本项适用于：信息系统等级保护三级系统）

A.4.1.3.3 人员离岗

本项要求包括：

a) 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。
b) 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。
c) 是否办理严格的调离手续。（本项适用于：信息系统等级保护二级系统）
d) 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。（本项适用于：信息系统等级保护三级系统）

A.4.1.3.4 人员考核

本项要求包括：

a) 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应至少每年一次。
b) 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。（本项适用于：信息系统等级保护三级系统）
c) 是否对考核结果进行记录并保存。（本项适用于：信息系统等级保护三级系统）

A.4.1.3.5 教育和培训

本项要求包括：

a) 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。
b) 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。
c) 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。
d) 是否对所有上岗技术人员进行岗位培训。
e) 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。（本项适用于：信息系统等级保护三级系统）
f) 总部技术部门的所有人员是否每两年参加期货业协会组织的技术培训达到 18 学时，其中至少有 3 学时的信息技术法律法规及标准培训。
g) 是否有明确的培训教材，用于培训上岗操作人员。

A.4.1.3.6 外部人员访问管理

本项要求包括：

a) 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。

b) 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。（本项适用于：信息系统等级保护三级系统）

A.4.2 机房管理

A.4.2.1 基础保障

A.4.2.1.1 物理位置的选择

本项要求包括：

a) 机房和办公场地是否选择具有防震、防风和防雨等能力的建筑：
   1) 应具有机房或机房所在建筑物符合当地抗震要求的相关证明；
   2) 机房外墙壁应没有对外的窗户。否则，应采用双层固定窗，并作密封、防水处理。

b) 机房场地是否避免设在建筑物的高层或地下室，以及用水设备的下层或隔壁：（本项适用于：信息系统等级保护三级系统）
   1) 机房场地不宜设在建筑物顶层，如果不可避免，应采取有效的防水措施。机房场地设在建筑物地下室的，应采取有效的防水措施；
   2) 机房场地设在建筑物高层的，应对设备采取有效固定措施；
   3) 如果机房周围有用水设备，应当有防渗水和疏导措施。

c) 机房承重是否达到300公斤每平方米。（本项适用于：二类期货公司）

d) 机房承重是否达到500公斤每平方米。（本项适用于：三类、四类期货公司）

e) 营业部设备区域是否是一个单独的区域，用于放置营业部开展业务所需的网络、通信和主机设备。

f) 机房是否为独立封闭区域，并配备门禁。

A.4.2.1.2 防雷击

本项要求包括：

a) 机房或机房所在大楼，是否设计并安装防雷击措施，防雷措施应至少包括避雷针或避雷器等。

b) 机房是否设置交流电源地线。

c) 是否设置防雷保安器，防止感应雷。（本项适用于：信息系统等级保护三级系统）

A.4.2.1.3 防火

本项要求包括：

a) 机房是否设置灭火设备和火灾自动报警系统。机房的火灾自动报警系统应向当地公安消防部门备案。（本项适用于：信息系统等级保护二级系统）

b) 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应向当地公安消防部门备案。（本项适用于：信息系统等级保护三级系统）

c) 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。（本项适用于：信息系统等级保护三级系统）

d) 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。（本项适用于：信息系统等级保护三级系统）
e) 机房内是否采用卤代烷或可替代的其他新型气体灭火装置。（本项适用于：三类、四类期货公司）

A.4.2.1.4 防水和防潮

本项要求包括：
a) 水管安装，是否穿过机房屋顶和活动地板下；
   1) 与机房设备无关的水管不得穿过机房屋顶和活动地板下；
   2) 机房屋顶和活动地板下铺有水管的，应采取有效防护措施。
b) 是否采取措施防止雨水通过机房窗户、屋顶和墙壁渗透。
c) 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。
d) 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。（本项适用于：信息系统等级保护三级系统）
e) 机房内是否安装漏水检测设施，并能够自动报警。（本项适用于：三类、四类期货公司）

A.4.2.1.5 防静电

本项要求包括：
a) 关键设备应采用必要的接地防静电措施。（本项适用于：信息系统等级保护二级系统）
b) 主要设备是否采用必要的接地防静电措施。（本项适用于：信息系统等级保护三级系统）
c) 机房是否采用防静电地板。（本项适用于：信息系统等级保护三级系统）

A.4.2.1.6 空调

本项要求包括：
a) 机房是否设置温、湿度自动调节设施，使机房温、湿度的变化在设备运行所允许的范围之内：
   1) 开机时机房温度应控制在 22℃-24℃；
   2) 开机时机房相对湿度应控制在 40%-55%。
b) 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。
c) 是否配有与机房热容量匹配的空调。（本项适用于：一类期货公司）
d) 是否提供与机房热容量匹配的精密空调，并有冗余设备。（本项适用于：二类期货公司）
e) 是否配有与机房热容量匹配的精密空调，并有冗余的精密空调设备。（本项适用于：三类、四类期货公司）
f) 空调是否双路供电。（本项适用于：三类、四类期货公司）
g) 机房是否配备新风设施。（本项适用于：三类、四类期货公司）
h) 是否具有为空调供电的发电机。（本项适用于：三类、四类期货公司，其中三类期货公司可选）

A.4.2.1.7 电力供应

本项要求包括：
a) 是否在机房供电线路上配置稳压器和过电压防护设备。
b) 是否提供短期的备用电力供应，至少满足主要设备在断电情况下的正常运行要求。
   1) 机房应配备 UPS，UPS 实际供电能力能够满足主要设备在断电情况下正常运行 2 个小时以上；
   2) 机房应自备或租用发电机，能够保障持续供电。

c) 是否采用双路市电，双路市电应能实现自动切换。（本项适用于：信息系统等级保护三级系统）
d) 机房是否配备在线 UPS 设施。UPS 应当存放在独立封闭区域。
e) UPS 供电时间是否超过从断电到发电机启动或者应急供电协议规定到场响应时间的 2 倍。如无发电设备，UPS 的电池应能够支撑 4 个小时。（本项适用于：一类期货公司）
f) 是否具有双路市电供电，双路供电能实现自动切换，或在单路供电情况下，备用供电措施能提供超过 4 小时的供电时间。（本项适用于：二类期货公司）
g) 是否提供双路市电，双路供电应能实现自动切换，双 UPS 供电，并能够采用发电机应急供电。（本项适用于：三类、四类期货公司）
h) 发电机是否能够提供不少于 6 小时的连续供电，在满负载运行的情况下，UPS 供电时间应超过从断电到发电机开始供电的间隔时间。（本项适用于：三类期货公司）
i) 发电机是否能够提供不少于 12 小时的连续供电，在满负载运行的情况下，UPS 供电时间应超过从断电到发电机开始供电的间隔时间。（本项适用于：四类期货公司）

A.4.2.1.8 电磁防护

本项要求包括：

a) 电源线和通信线缆是否隔离铺设，避免互相干扰。电源线和通信线缆应铺设在不同的桥架或管道，避免互相干扰。
b) 是否采用接地方式防止外界电磁干扰和设备寄生耦合干扰：（本项适用于：信息系统等级保护三级系统）
   1) 机房或机房所在的大楼必须有接地措施，并且接地电阻必须小于 1 欧姆；
   2) 机房验收报告应提供合格的检测结果。
c) 是否对关键设备和磁介质实施电磁屏蔽。（本项适用于：信息系统等级保护三级系统）
d) 所有弱电布线是否有清晰的线标。
e) 强弱电布线应分开。（本项适用于：二类、三类、四类期货公司）
f) 强电电缆是否有屏蔽或隔离措施。（本项适用于：三类、四类期货公司）

A.4.2.2 机房运维

A.4.2.2.1 物理访问控制

本项要求包括：

a) 机房出入口是否安排专人值守，控制、鉴别和记录进入的人员；
   1) 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；
   2) 没有门禁系统的机房，应当安排专人控制、鉴别和记录人员的进出；
   3) 有门禁系统的机房，应当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。
b) 需进入机房的来访人员是否经过申请和审批流程，并限制和监控其活动范围；
   1) 来访人员进入机房，应有审批流程，记录带进带出的设备、进出时间、工作内容，并有专人陪同其在限定的范围内工作；
   2) 机房出入口应有视频监控，监控记录至少保存 3 个月。
c) 是否对机房划分区域进行管理，区域和区域之间设置物理隔离装置，在重要区域前设置交付或安装等过渡区域：（本项适用于：信息系统等级保护三级系统）
   1) 机房应当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；
   2) 机房应当设置专门的过渡区域，用于设备的交付或安装；

3) 重要区域包括：主机房、辅助区、支持区等功能区域。

d) 机房出入口和内部是否安装 7×24 小时录像监控设施，录像至少保存 90 天。

A.4.2.2.2 防盗窃和防破坏

本项要求包括：

a) 是否将主要设备放置在机房内。

b) 是否将设备或主要部件进行固定，并设置明显的不易除去的标记；

1) 主要设备应当安装、固定在机柜内或机架上；

2) 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。

c) 是否将通信线缆铺设在隐蔽处，可铺设在地下或管道中；通信线缆可铺设在管道或线槽、线架中。

d) 是否对介质分类标识，存储在介质库或档案室中。

e) 主机房应安装必要的防盗报警设施。（本项适用于：信息系统等级保护二级系统）

f) 是否利用光、电等技术设置机房防盗报警系统。（本项适用于：信息系统等级保护三级系统）

g) 是否对机房设置监控报警系统：（本项适用于：信息系统等级保护三级系统）

1) 应至少对机房的出入口、操作台等区域进行摄像监控；

2) 监控录像记录至少保存 3 个月。

h) 是否实现声音或短信等自动报警或 7×24 小时值守。

A.4.2.2.3 机房管理

本项要求包括：

a) 是否指定专门的部门或人员定期对机房供配电、空调、温湿度控制等设施进行维护管理；

1) 应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；

2) 应每年对防盗报警、防雷、消防等装置进行检测维护并保存相关维护记录。

b) 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。

c) 是否加强对办公环境的保密性管理，包括工作人员调离办公室应立即交还该办公室钥匙和不在办公区接待来访人员等。（本项适用于：信息系统等级保护二级系统）

d) 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。

e) 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。（本项适用于：信息系统等级保护三级系统）

f) 是否指定机房管理负责人。

g) 是否确保机房环境整洁和安全，包括：

1) 应定期检查防水、防雷、防火、防潮、防尘、防鼠、防静电、防电磁辐射等措施的有效性；

2) 应保持机房环境卫生，采取防尘措施，定期进行除尘处理；

3) 交易时间内不得进行机房施工、保洁操作。

h) 是否对设备和人员出入进行严格管理，包括：

1) 应指定人员负责控制、鉴别和记录设备和人员的进出情况，记录进出人员、进出时间、工作内容，并留存记录至少 90 天；

2) 机房出入口的监控录像至少保存 90 天；

3) 外来人员进入机房应经过申请和审批流程，并限制和监控其活动范围，并有专人陪同；

4) 外来设备未经批准不得接入生产环境。

i) 对机房温湿度是否有监控措施和记录。

j) 是否具有机房环境监控系统，至少能够监控供配电、空调、温湿度等重要指标。（本项适用于：三类、四类期货公司）

k) 所有 UPS 和空调设施是否有专业维护人员，或与专业机构签订维护合同。（本项适用于：二类、三类、四类期货公司）

l) 是否定期对所有 UPS 和空调设施进行恰当维护，有维护记录。（本项适用于：二类、三类、四类期货公司）

m) 是否建立机房管理制度，对机房环境、供电、空调、消防、安防等基础设施进行运行维护，对设备和人员出入机房和值班操作间进行登记，并保留相关记录。

n) 非技术保障人员进入机房是否获得授权，并有技术保障人员陪同，所携带设备应专门登记。

o) 交易期间如无应急或者巡检需要，不应进入机房。

A.4.2.2.4 用电安全

本项要求包括：

a) 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。

b) 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。

c) 是否在危险性高的位置张贴相应的用电安全操作方法、警示及指引。

d) 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。

e) 未经审批是否禁止接入其他用电设备。

A.4.2.2.5 机房消防

本项要求包括：

a) 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。

b) 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。

c) 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。

d) 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。

e) 是否定期进行消防设施的使用培训和演习。

A.4.3 网络管理

A.4.3.1 网络安全

A.4.3.1.1 结构安全

本项要求包括：

a) 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%。

b) 是否保证接入网络和核心网络的带宽满足业务高峰期需要。（本项适用于：信息系统等级保护二级系统）
c) 是否保证网络各个部分的带宽满足业务高峰期需要。（本项适用于：信息系统等级保护三级系统）
d) 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。（本项适用于：信息系统等级保护三级系统）
e) 是否绘制与当前运行情况相符的网络拓扑结构图；应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。
f) 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。
g) 是否提供关键网络设备、通信线路和数据处理系统的硬件冗余，保证系统的可用性。（本项适用于：信息系统等级保护二级系统）
h) 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，重要网段与其他网段之间采取可靠的技术隔离手段。（本项适用于：信息系统等级保护三级系统）
i) 是否按照对业务服务的重要次序来指定带宽分配优先级别，保证在网络发生拥堵的时候优先保护重要主机。应对所有业务确定重要性、优先级，制定业务相关带宽分配原则及相应的带宽控制策略，根据安全需求，采取网络 QoS 或专用带宽管理设备等措施。（本项适用于：信息系统等级保护三级系统）
j) 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。（本项适用于：信息系统等级保护三级系统）
k) 接入交易所的交易通信链路是否达到所有其作为会员的交易所的要求，并采用不同运营商的通讯线路作为备份线路。
l) 接入交易所的交易通信链路带宽使用率每交易日峰值按月统计的平均值是否不超过 80%。（本项适用于：二类、三类、四类期货公司，其中二类期货公司可选）
m) 网上交易的通信链路带宽使用率每交易日峰值按月统计的平均值是否不超过 80%。（本项适用于：二类、三类、四类期货公司，其中二类期货公司可选）
n) 是否使用多个电信运营商的链路作为网上交易的通信链路。（本项适用于：二类、三类、四类期货公司）
o) 是否使用至少 2 家行情商提供的行情服务，其中至少有 1 家使用至少 2 套服务器。（本项适用于：一类期货公司）
p) 是否向客户同时提供至少 2 套行情服务，且均使用至少 2 套服务器。（本项适用于：二类、三类、四类期货公司）
q) 是否通过至少两个电信运营商提供行情服务。（本项适用于：二类期货公司）
r) 是否有至少 2 套行情服务，且均通过至少两个电信运营商提供服务。（本项适用于：三类、四类期货公司）
s) 提供现场交易的营业部是否有至少两条交易通信链路。

A.4.3.1.2 访问控制

本项要求包括：

a) 网络边界是否部署访问控制设备并启用访问控制功能。
b) 是否针对数据流提供明确的允许/拒绝访问的访问控制策略，控制力度达到网段级。网络边界访问控制设备应设定过滤规则集。规则集应涵盖对所有出入边界的数据包的处理方式，对于没有明确定义的数据包，应缺省拒绝。（本项适用于：信息系统等级保护二级系统）

c) 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。（本项适用于：信息系统等级保护三级系统）
d) 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。
e) 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。
f) 是否对进出网络的信息内容进行过滤，实现对应用层 HTTP、FTP、TELNET、SMTP、POP3 等协议命令级的控制；对通过互联网传输的信息内容进行过滤，实现对应用层 HTTP、FTP、TELNET、SMTP、POP3 等通用性协议命令级控制。（本项适用于：信息系统等级保护三级系统）
g) 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。（本项适用于：信息系统等级保护三级系统）
h) 是否限制网络最大流量数及网络连接数。（本项适用于：信息系统等级保护三级系统）
i) 重要网段是否采取技术手段防止地址欺骗。（本项适用于：信息系统等级保护三级系统）
j) 是否制定网络访问控制策略，应合理设置网络隔离设施上的访问控制列表，关闭与业务无关的端口；编制文档并保持更新；访问控制策略的变更应履行审批手续。

A.4.3.1.3 安全审计

本项要求包括：

a) 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) 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。
c) 是否能够根据记录数据进行分析，并生成审计报表。（本项适用于：信息系统等级保护三级系统）
d) 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。（本项适用于：信息系统等级保护三级系统）
e) 是否定期检查网络设备的用户、口令及权限设置的正确性。
f) 是否留存网络访问日志。

A.4.3.1.4 边界完整性检查

本项要求包括：

a) 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，准确定出位置，并对其进行有效阻断。（本项适用于：信息系统等级保护二级系统）
b) 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。（本项适用于：信息系统等级保护三级系统）
c) 是否能够对内部网络用户私自联到外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。（本项适用于：信息系统等级保护三级系统）
d) 是否定期检查安全隔离情况，确保各安全域之间有效隔离。
e) 生产网与互联网是否实现有效隔离。
f) 网站与网上交易系统是否实现有效隔离。
g) 生产网与办公网是否实现有效隔离。
h) 总部的生产网与营业部的网络是否实现有效隔离。
i) 生产网与交易所、银行等外联单位网络是否实现有效隔离。

j) 支持核心业务的网络、主机设备是否通过独立网络进行管理，实现监控数据流和生产数据流的分离。

A.4.3.1.5 入侵防范

本项要求包括：

a) 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。
b) 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应提供报警。（本项适用于：信息系统等级保护三级系统）
c) 是否配备防火墙或相当的安全防护设备。
d) 核心交易系统是否至少有一条网上交易线路部署了防拒绝服务攻击措施，包括部署防拒绝服务攻击设备或与基础运营商签署流量清洗协议等。（本项适用于：三类、四类期货公司）

A.4.3.1.6 恶意代码防范

本项要求包括：

a) 是否在网络边界处对恶意代码进行检测和清除：（本项适用于：信息系统等级保护三级系统）
   1) 在不严重影响网络性能和业务的情况下，应在网络边界部署恶意代码检测系统；
   2) 如果部署了主机恶意代码检测系统，可选择安装部署网络边界恶意代码检测系统。
b) 是否维护恶意代码库的升级和检测系统的更新。（本项适用于：信息系统等级保护三级系统）

A.4.3.1.7 网络设备防护

本项要求包括：

a) 是否对登录网络设备的用户进行身份鉴别；应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。
b) 是否对网络设备的管理员登录地址进行限制。
c) 网络设备用户的标识是否唯一。
d) 身份鉴别信息是否具有不易被冒用的特点，口令是否有复杂度要求并定期更换；
   1) 口令应符合以下条件：数字、字母、符号混排，无规律的方式；
   2) 管理员用户口令的长度至少为 12 位；
   3) 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；
   4) 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。
e) 是否具有登录失败处理功能，是否采取结束会话、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。
f) 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。
g) 主要网络设备是否对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别：（本项适用于：信息系统等级保护三级系统）
   1) 通过本地控制台管理主要网络设备时，应采用一种或一种以上身份鉴别技术；
   2) 以远程方式登录主要网络设备，应采用两种或两种以上组合的鉴别技术进行身份鉴别。
h) 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。（本项适用于：信息系统等级保护三级系统）

A.4.4 主机和系统管理

A.4.4.1 主机安全

A.4.4.1.1 身份鉴别

本项要求包括：

a) 是否对登录操作系统和数据库系统的用户进行身份标识和鉴别。

b) 操作系统和数据库系统管理用户身份标识是否具有不易被冒用的特点，口令应有复杂度要求并定期更换；

1) 口令应符合以下条件：数字、字母、符号混排，无规律的方式；

2) 口令的长度至少为 12 位；

3) 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；

4) 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。

c) 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。

d) 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。

e) 是否为操作系统和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：

1) 应为操作系统的不同用户分配不同的用户名；

2) 应为数据库系统的不同用户分配不同的用户名。

f) 是否采用两种或两种以上组合的鉴别技术对管理用户进行身份鉴别：（本项适用于：信息系统等级保护三级系统）

1) 通过本地控制台管理主机设备时，应采用一种或一种以上身份鉴别技术；

2) 以远程方式登录主机设备，应采用两种或两种以上组合的鉴别技术进行身份鉴别。

A.4.4.1.2 访问控制

本项要求包括：

a) 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。

b) 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。

c) 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。

1) 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；

2) 系统无法重命名的特殊默认账户，可不重命名。

d) 是否及时删除多余的、过期的账户，避免共享账户的存在。

e) 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。（本项适用于：信息系统等级保护三级系统）

A.4.4.1.3 安全审计

本项要求包括：

a) 审计范围是否覆盖到服务器上的每个操作系统用户和数据库用户；应在保证系统运行安全和效率的前提，启用系统审计或采用第三方安全审计产品实现审计要求。（本项适用于：信息系统等级保护二级系统）

b) 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。

c) 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。

d) 是否保护审计记录，避免受到未预期的删除、修改或覆盖等。审计记录应至少保存6个月。
e) 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和数据库用户；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。（本项适用于：信息系统等级保护三级系统）
f) 是否能够根据记录数据进行分析，并生成审计报表。（本项适用于：信息系统等级保护三级系统）
g) 是否保护审计进程，避免受到未预期的中断。（本项适用于：信息系统等级保护三级系统）

A.4.4.1.4 入侵防范

本项要求包括：

a) 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，应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。
b) 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。（本项适用于：信息系统等级保护三级系统）
c) 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，应停止有关服务，并提供报警。（本项适用于：信息系统等级保护三级系统）
d) 总部及营业部是否建立有效机制，保障及时对核心系统依赖的各种系统软件所需要的补丁进行了解、评估、必要的测试和升级。

A.4.4.1.5 恶意代码防范

本项要求包括：

a) 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；
   1) 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；
   2) 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。
b) 是否支持防恶意代码软件的统一管理。
c) 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。（本项适用于：信息系统等级保护三级系统）
d) 是否建立有效机制，保障及时对核心系统依赖的各种系统软件所需要的补丁进行了解、评估、必要的测试和升级。
e) 是否对通过互联网向外提供服务的设备和系统进行定期安全扫描，关闭不需要的端口。
f) 是否对生产环境所有服务器定期进行安全扫描和合理加固，关闭不需要的端口。（本项适用于：二类、三类、四类期货公司）
g) 是否在计算机或存储设备接入生产环境之前对其进行安全检查。（本项适用于：二类、三类、四类期货公司）
h) 在读取移动存储设备上的数据以及从网络上接收文件或邮件之前，是否先进行病毒检查。（本项适用于：二类、三类、四类期货公司）

A.4.4.1.6 资源控制

本项要求包括：

a) 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。
b) 是否根据安全策略设置登录终端的操作超时锁定。

c) 是否限制单个用户对系统资源的最大或最小使用限度。
d) 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。（本项适用于：信息系统等级保护三级系统）
e) 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。（本项适用于：信息系统等级保护三级系统）

A.4.4.2 应用安全

A.4.4.2.1 结构安全

本项要求包括：
a) 交易系统的性能和容量是否达到所有其作为会员的交易所的要求。
b) 是否与至少2家银行实现银期转账，其中至少一家提供全国性银期转账服务。（本项适用于：一类期货公司）
c) 是否与至少2家银行实现全国性银期转帐。（本项适用于：二类、三类、四类期货公司）
d) 所有银期转账系统是否具备抗单点故障的能力。（本项适用于：四类期货公司）

A.4.4.2.2 身份鉴别

本项要求包括：
a) 是否提供专用的登录控制模块对登录用户进行身份标识和鉴别。
b) 是否提供用户身份标识唯一和鉴别信息复杂度检查功能，保证应用系统中不存在重复用户身份标识，身份鉴别信息不易被冒用。
c) 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。
d) 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。
e) 是否对同一用户采用两种或两种以上组合的鉴别技术实现用户身份鉴别：（本项适用于：信息系统等级保护三级系统）
   1) 管理用户通过受控本地控制台管理应用系统时，应采用一种或一种以上身份鉴别技术；
   2) 管理用户以远程方式登录应用系统，应采用两种或两种以上组合的鉴别技术进行身份鉴别；
   3) 面向互联网服务的系统应当提供两种或两种以上组合的鉴别技术供用户选择。
f) 网上交易客户端是否提供可靠的身份认证机制，支持多种方式与服务端完成身份认证。
g) 网上信息系统服务端是否能向客户提供可证明服务端自身身份的信息，如提供预留验证信息服务，在网上交易客户登录时回显，帮助客户有效识别仿冒的网上交易信息系统，防范利用仿冒的网上交易信息系统进行诈骗活动。
h) 网上信息系统是否提供可靠的身份验证机制，除采用账号名、口令、验证码的身份认证方式外，是否向客户提供一种以上强度更高的身份认证方式供客户选择使用，如客户端电脑或手机特征码绑定、软硬件证书、动态口令等认证方式，确认客户的身份和登录的合法性，防止不法分子利用木马等黑客程序窃取客户账号和口令。（本项适用于：三类、四类期货公司，其中三类期货公司可选）

A.4.4.2.3 访问控制

本项要求包括：

a) 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、数据库表等客体的访问，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。
b) 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。
c) 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。
d) 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。
e) 核心系统是否有授权管理功能。

A.4.4.2.4 安全审计

本项要求包括：

a) 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。
b) 是否采取有效措施防止删除、修改或覆盖审计记录。（本项适用于：信息系统等级保护二级系统）
c) 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。审计记录应至少保存 6 个月。
d) 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。（本项适用于：信息系统等级保护三级系统）
e) 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。（本项适用于：信息系统等级保护三级系统）
f) 交易系统是否具备对客户进行实时风险控制的功能。
g) 交易系统是否产生、记录并存储必要的日志信息供审计使用。
h) 核心系统是否具备向期货保证金监控中心上报规定数据的功能。
i) 核心系统的主要业务操作应产生审计记录。
j) 所有的主要运维操作是否采取恰当的认证措施，并产生审计记录。（本项适用于：三类、四类期货公司，其中三类期货公司可选）

A.4.4.2.5 通信完整性

本项要求包括：

a) 通过互联网、卫星网进行通信时，是否采用校验码技术保证通信过程中数据的完整性。（本项适用于：信息系统等级保护二级系统）
b) 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。（本项适用于：信息系统等级保护三级系统）
c) 是否能够检测到鉴别信息和重要业务数据在传输过程中完整性受到破坏。（本项适用于：信息系统等级保护二级系统）
d) 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。（本项适用于：信息系统等级保护三级系统）

A.4.4.2.6 通信保密性

本项要求包括：

a) 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。

b) 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。
c) 所有生产环境服务器是否尽量避免使用 telnet、ftp 等有安全隐患的服务，与服务器通信是否采用加密方式，例如 SSH。（本项适用于：二类、三类、四类期货公司，其中二类期货公司可选）

A.4.4.2.7 抗抵赖

本项要求包括：
a) 是否具有在请求的情况下为数据原发者或接收者提供数据原发证据的功能;应用系统的操作与管理记录，至少应记录操作时间、操作人员及操作类型、操作内容等信息。交易系统应能够记录用户交易行为数据，至少包括业务流水号、账户名、IP 地址、交易指令等信息。（本项适用于：信息系统等级保护三级系统）
b) 是否具有在请求的情况下为数据原发者或接收者提供数据接收证据的功能。应用系统的操作与管理记录，至少应记录操作时间、操作人员及操作类型、操作内容等信息。交易系统应能够记录用户交易行为数据，至少包括业务流水号、账户名、IP 地址、交易指令等信息。（本项适用于：信息系统等级保护三级系统）

A.4.4.2.8 软件容错

本项要求包括：
a) 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。
b) 在故障发生时，应用系统是否能够继续提供一部分功能，确保能够实施必要的措施。（本项适用于：信息系统等级保护二级系统）
c) 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。（本项适用于：信息系统等级保护三级系统）

A.4.4.2.9 资源控制

本项要求包括：
a) 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，另一方是否能够自动结束会话。用户登录应用系统后在规定的时间内未执行任何操作，应自动退出系统。
b) 是否能够对系统的最大并发会话连接数进行限制。
c) 是否能够对单个账户的多重并发会话进行限制。
d) 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。（本项适用于：信息系统等级保护三级系统）
e) 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。(本项适用于：信息系统等级保护三级系统）
f) 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。（本项适用于：信息系统等级保护三级系统）
g) 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。（本项适用于：信息系统等级保护三级系统）
h) 交易系统是否实现数据与应用分离，防止客户终端绕过应用程序界面直接访问核心数据。
i) 交易系统是否具备流量控制管理功能。（本项适用于：三类、四类期货公司）

A.4.4.3 数据安全及备份恢复

A.4.4.3.1 数据完整性

本项要求包括：

a) 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存储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。（本项适用于：信息系统等级保护三级系统）

b) 是否禁止具有篡改、伪造核心系统数据或其他可能导致数据失真的功能。

A.4.4.3.2 数据保密性

本项要求包括：

a) 是否采用加密或其他保护措施实现鉴别信息的存储保密性。（本项适用于：信息系统等级保护二级系统）

b) 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。（本项适用于：信息系统等级保护三级系统）

c) 对存有重要生产数据计算机的光盘刻录、USB 接口等功能是否采取有效的控制手段，防止非授权的数据复制。（本项适用于：四类期货公司）

d) 是否遵守国家关于个人信息保护的相关规定，确保网上交易数据和客户信息的安全性和完整性。未经客户允许或期货公司授权，不得以任何方式向除中国证监会及其派出机构、执法机关、审计机关以外的第三方提供交易数据和客户信息。

A.4.4.3.3 备份和恢复

本项要求包括：

a) 应利用通信网络将关键业务数据实时传送至异地数据备份场所。（本项适用于：三类、四类期货公司，其中三类期货公司可选）

b) 当日备份的交易和结算数据是否立即进行恢复验证。（本项适用于：三类、四类期货公司）

c) 是否建立交易、结算、财务数据的备份制度。有关开户、变更、销户的客户资料档案应当自期货经纪合同终止之日起至少保存 20 年；交易指令记录、交易结算记录、错单记录、客户投诉档案以及其他业务记录应当至少保存 20 年。应当确保电子数据的真实、可靠，采取有效措施防止电子数据被篡改、损毁，保存的电子数据资料应当能随时转化为纸质形式。

A.4.5 运维管理

A.4.5.1 系统建设管理

A.4.5.1.1 系统定级

本项要求包括：

a) 是否明确信息系统的边界和安全保护等级。

b) 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。

c) 是否确保信息系统的定级结果经过相关部门的批准。

d) 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。（本项适用于：信息系统等级保护三级系统）

e) 定级结果是否经过相关部门批准，由住所地证监局出具定级审核意见。

A.4.5.1.2 方案设计

本项要求包括：

a) 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。
b) 是否以书面形式描述对系统的安全保护要求、策略和措施等内容，形成系统的安全方案。（本项适用于：信息系统等级保护二级系统）
c) 是否对安全方案进行细化，形成能指导安全系统建设、安全产品采购和使用的详细设计方案。（本项适用于：信息系统等级保护二级系统）
d) 是否组织相关部门和有关安全技术专家对安全设计方案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。（本项适用于：信息系统等级保护二级系统）
e) 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。（本项适用于：信息系统等级保护三级系统）
f) 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。（本项适用于：信息系统等级保护三级系统）
g) 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。（本项适用于：信息系统等级保护三级系统）
h) 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。（本项适用于：信息系统等级保护三级系统）
i) 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.4.5.1.3 产品采购和使用

本项要求包括：

a) 是否确保安全产品采购和使用符合国家的有关规定。
b) 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。
c) 是否指定或授权专门的部门负责产品的采购。
d) 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。（本项适用于：信息系统等级保护三级系统）

A.4.5.1.4 自行软件开发

本项要求包括：

a) 开发环境是否与实际运行环境物理分离。（本项适用于：信息系统等级保护二级系统）
b) 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。
c) 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。
d) 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。应保证同一组件或子系统的开发人员和测试人员分离。（本项适用于：信息系统等级保护三级系统）
e) 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。（本项适用于：信息系统等级保护三级系统）
f) 是否对程序资源库的修改、更新、发布进行授权和批准。（本项适用于：信息系统等级保护三级系统）

A.4.5.1.5 外包软件开发

本项要求包括：

a) 是否根据开发要求测试软件质量。
b) 是否确保提供软件设计的相关文档和使用指南。
c) 是否在软件安装之前检测软件包中可能存在的恶意代码。
d) 要求开发单位提供软件源代码，并审查软件中可能存在的后门。

A.4.5.1.6 工程实施

本项要求包括：

a) 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。
b) 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。
c) 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。（本项适用于：信息系统等级保护三级系统）

A.4.5.1.7 系统交付

本项要求包括：

a) 是否向用户提供系统建设文档和运行维护所需文档。
b) 是否书面规定系统交付的控制方法和人员行为准则。（本项适用于：信息系统等级保护三级系统）
c) 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。（本项适用于：信息系统等级保护三级系统）
d) 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。
e) 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。
f) 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。
g) 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。

A.4.5.1.8 测试验收

本项要求包括：

a) 是否对系统进行安全性测试验收。（本项适用于：信息系统等级保护二级系统）
b) 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。
c) 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。
d) 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。（本项适用于：信息系统等级保护三级系统）
e) 是否书面规定系统测试验收的控制方法和人员行为准则。（本项适用于：信息系统等级保护三级系统）
f) 是否建立核心系统软硬件上线前测试的流程和制度，规范系统上线前进行的测试。（本项适用于：二类、三类、四类期货公司，其中二类期货公司可选）
g) 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。（本项适用于：信息系统等级保护三级系统）
h) 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。

i) 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。
j) 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。模拟环境应与生产环境进行有效隔离，不得对生产环境进行干扰。
k) 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。
l) 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。
m) 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。
n) 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。
o) 是否提前发布生产环境测试的系统测试公告。
p) 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。
q) 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。
r) 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。
s) 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。
t) 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。
u) 测试后是否恢复生产环境并验证恢复的有效性。
v) 是否禁止交易时段使用生产环境进行测试。
w) 是否有专人负责系统测试计划、组织、实施和记录，并对参与测试的各方进行统筹协调。（本项适用于：二类、三类、四类期货公司，其中二类期货公司可选）

A.4.5.1.9 系统备案

本项要求包括：
a) 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。（本项适用于：信息系统等级保护三级系统）
b) 经营机构是否将系统等级及相关材料报住所地证监局备案。
c) 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.4.5.1.10 等级测评

本项要求包括：
a) 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。（本项适用于：信息系统等级保护三级系统）
b) 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。（本项适用于：信息系统等级保护三级系统）
c) 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。（本项适用于：信息系统等级保护三级系统）
d) 是否指定或授权专门的部门或人员负责等级测评的管理。（本项适用于：信息系统等级保护三级系统）

e) 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.4.5.2 系统运维管理

A.4.5.2.1 值班管理

本项要求包括：

a) 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。
b) 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。
c) 是否建立日常值班制度，设立专门运行保障岗位，指定运维值班负责人，运维值班负责人应有备岗，制定明确的每日值班表，保障交易期间有人值守。
d) 是否制定交接班流程，并严格执行，留存记录。
e) 是否设置运维值班电话，并保持畅通。
f) 交易运行期间是否有现场保障人员，设置运维值班电话，以及时维护和应急处理。
g) 是否实现双人日常值班。（本项适用于：二类、三类、四类期货公司）
h) 是否实现对机房和网站的 24 小时连续监控。（本项适用于：四类期货公司）

A.4.5.2.2 文档管理

本项要求包括：

a) 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。
b) 是否明确文档管理的责任人。
c) 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。
d) 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。
e) 是否对超范围、超权限使用文档时，保存相关审批、使用记录。
f) 是否有与当前运行情况相符的业务系统结构文档。

A.4.5.2.3 资产管理

本项要求包括：

a) 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。
b) 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。
c) 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。（本项适用于：信息系统等级保护三级系统）
d) 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。（本项适用于：信息系统等级保护三级系统）

A.4.5.2.4 数据与介质管理

本项要求包括：

a) 是否建立数据管理、介质维护、销毁和使用管理制度。
b) 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。
c) 是否对介质归档和查询等过程进行记录，并根据存档介质的目录清单定期盘点。（本项适用于：信息系统等级保护二级系统）
d) 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。
e) 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。
f) 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。
g) 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，应按国家相关规定另行处理。
h) 是否根据数据备份的需要对某些介质实行异地存储，存储地的环境要求和管理方法应与本地相同。（本项适用于：信息系统等级保护三级系统）
i) 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。（本项适用于：信息系统等级保护三级系统）
j) 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。
k) 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。
l) 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。
m) 在线数据管理，是否做到如下要求：
    1) 交易业务系统数据应至少每交易日备份一次；
    2) 交易业务系统历史数据至少保留一年；
    3) 未经授权不得访问、复制；
    4) 对数据的修改应通过审批，双岗操作并记录操作日志。
n) 离线数据管理，是否做到如下要求：
    1) 离线数据不得更改；
    2) 应至少每季度对核心交易业务系统的备份数据进行一次有效性验证，如发现问题应采取措施修复备份数据，并查明原因；
    3) 离线数据的调阅、复制、传输、查询，应按照拟定的流程办理审批手续，并进行登记；
    4) 备份数据带离存储环境时应采取必要的安全措施。
o) 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。
p) 离线备份介质是否在本地机房、同城、异地安全可靠存放。
q) 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。
r) 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。

A.4.5.2.5 设备和软件管理

本项要求包括：

a) 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。

b) 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。
c) 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。
d) 信息处理设备是否经过审批才能带离机房或办公地点。
e) 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。（本项适用于：信息系统等级保护三级系统）
f) 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。
g) 是否明确设备和软件管理责任人。
h) 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。
i) 是否编制信息系统设备清单，主要包括设备名称、设备编号、入库时间、设备主要参数、设备序列号、设备状态、设备保修期、设备位置、设备用途和设备使用责任人等内容，并保留设备启用、转移、维修、报废等过程的记录。
j) 是否使用正版软件并保存软件授权证书和许可协议，应编制软件清单，主要包括软件名称、软件编号、入库时间、软件版本，授权和许可情况、软件序列号、软件状态、软件维护期、软件安装设备、用途和使用责任人等内容，并保留软件启用、转移、升级、报废等过程的记录。
k) 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。
l) 是否对外送设备的维修进行严格管理，防止数据泄露。
m) 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。
n) 每年是否对核心系统的性能和容量情况进行评估。
o) 是否根据核心系统的性能容量评估报告，结合业务发展情况及时提出改进计划。
p) 是否及时执行改进计划，并对执行结果进行跟踪和评估。（本项适用于：三类、四类期货公司）

A.4.5.2.6 变更管理

本项要求包括：

a) 是否确认系统中要发生的变更，并制定相应的变更方案；重要系统变更前应制定详细的变更方案、失败恢复方案、专项应急预案。
b) 系统发生重要变更前，是否向主管领导申请，审批后方可实施变更，并在实施后向相关人员通告。（本项适用于：信息系统等级保护二级系统）
c) 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。（本项适用于：信息系统等级保护三级系统）
d) 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。（本项适用于：信息系统等级保护三级系统）
e) 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。（本项适用于：信息系统等级保护三级系统）
f) 是否建立系统变更流程，对信息系统的变更活动进行规范。
g) 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。
h) 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。

i) 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。
j) 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。
k) 是否按照测试方案，组织变更前后的测试，测试后应提交测试记录或报告。
l) 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。
m) 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。
n) 是否将所有涉及核心系统的软硬件变更纳入变更管理范围。
o) 所有变更操作是否有操作记录。
p) 对于风险较大的变更，在条件允许的情况下，是否制定应急和回退方案。
q) 核心交易业务系统等风险较大的变更，是否在变更后对系统的运行情况进行跟踪。
r) 进行与核心系统相关的开发工作时，是否避免在生产环境上进行日常测试。
s) 如果需要使用生产环境进行测试，是否纳入变更管理。（本项适用于：三类、四类期货公司）
t) 是否及时对变更涉及的系统配置和操作手册进行修改。（本项适用于：三类、四类期货公司）
u) 对于风险较大的核心系统变更，在条件允许的情况下，是否在上线前进行演练。（本项适用于：二类、三类、四类期货公司，其中二类期货公司可选）
v) 是否定期进行风险评估，及时发现风险隐患，并予以处理。（本项适用于：三类、四类期货公司）

A.4.5.2.7 配置管理

本项要求包括：

a) 是否制定配置管理流程，明确配置管理负责人。
b) 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。
c) 配置库中配置项的属性是否至少包括以下信息。
    1) 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；
    2) 配置项编号应唯一；
    3) 配置项的添加、修改、替换、删除应有变更记录；
    4) 应保存配置项历史记录，确保与事件管理、问题管理、变更管理等流程记录的关联性。
d) 是否定期对配置库进行备份。
e) 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。
f) 是否具有生产环境设计和部署文档，并根据变更及时更新。
g) 是否对重要的配置信息进行有效备份。
h) 是否有恢复配置信息的流程。（本项适用于：二类、三类、四类期货公司）
i) 是否对配置信息的恢复进行演练。（本项适用于：三类、四类期货公司，其中三类期货公司可选）
j) 是否建立配置管理制度和配置文档库。（本项适用于：三类、四类期货公司）
k) 是否有专人负责生产环境配置管理。（本项适用于：三类、四类期货公司）
l) 是否定期对核心系统进行配置比对，以及时发现配置的变化。（本项适用于：四类期货公司）

A.4.5.2.8 日常操作

本项要求包括：

a) 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。
b) 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。
c) 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。
d) 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。
e) 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。
f) 是否对核心交易业务系统设置独立的操作和监控环境，与开发、测试等其他操作环境严格分离。
g) 核心系统是否有运行监控功能。（本项适用于：二类、三类、四类期货公司）
h) 核心系统是否具备通过监控中心统一开户系统进行开户的功能。
i) 核心系统是否具备链接监控中心投资者查询服务系统的功能。
j) 初始化、结算、数据备份等关键操作过程和结果是否有复核。
k) 注册邮箱账号是否经过审批。
l) 是否对交易系统的主要业务指标进行实时监控。
m) 是否对所有接入交易所的交易通信链路进行监控。
n) 是否对交易系统的主要业务监控指标进行记录。（本项适用于：二类、三类、四类期货公司，其中二类期货公司可选）
o) 是否对所有网上交易的通信链路进行监控。
p) 在关键时间点是否对生产环境运行状态进行巡检。
q) 日常操作和巡检是否保留记录，并有操作和复核人员的签名。
r) 是否记录生产环境发生的故障和异常。
s) 是否建立完善和更新重要手册的机制。
t) 是否有详细的操作手册（包括日常操作和定期维护操作），手册中应有详细的操作步骤。（本项适用于：二类、三类、四类期货公司）
u) 交易期间是否对核心系统和网络系统进行实时监控，并能及时、有效地报警。
v) 是否保留关键操作的记录和签名。（本项适用于：二类、三类、四类期货公司）
w) 是否保留应用系统的操作日志记录。（本项适用于：二类、三类、四类期货公司）
x) 对核心系统和网络系统的实时监控是否包括系统的可用性和系统性能。（本项适用于：三类、四类期货公司）
y) 是否采取管理和技术手段对业务部门进行的关键参数修改予以复核。（本项适用于：四类期货公司）

A.4.5.2.9 口令管理

本项要求包括：

a) 用户和口令管理是否符合如下要求：
   1) 不得设置弱口令，若系统条件允许，口令应采用数字、字母、符号混排且无规律的方式，管理员口令长度原则上不低于 12 位；核心交易业务系统应提示并阻止用户使用弱口令登录；
   2) 应每季度对管理员口令进行修改，更新的管理员口令至少 5 次内不能重复；
   3) 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；
   4) 应重点加强对匿名/默认用户的管理，防止被非法使用；

5) 应及时注销不再使用的账户；
6) 应明确责任人，负责统一保管、安全存放管理员口令，不得泄漏。

b) 所有书面方式保存的口令是否有安全的物理保护措施。
c) 数据库用户口令不得明文存放在计算机中。（本项适用于：四类期货公司）

A.4.5.2.10 数据库管理

本项要求包括：

a) 是否保持数据库的可用性，及时维护、更新软件。
b) 是否负责数据库的参数配置、调优，编制文档并保持更新。
c) 是否定期对数据库容量进行检查和评估，形成评估报告。
d) 是否负责管理数据库、表、索引、存储过程，数据库的升级、优化、扩容、迁移。
e) 是否定期检查数据库的用户、口令及权限设置的正确性。

A.4.5.2.11 终端信息

本项要求包括：

a) 向客户提供的交易终端软件，是否采取适当的技术，确保软件能够采集到客户交易终端电话号码、互联网通讯协议地址（IP 地址）、媒介访问控制地址（MAC 地址）以及其他能识别客户交易终端的特征代码。
b) 向客户提供的交易终端软件，是否采取适当的技术，确保软件能够采集到客户交易终端信息。由第三方提供交易终端软件的，应当建立软件认证许可制度，要求第三方采取适当的技术，确保软件能够采集到客户交易终端信息。客户交易终端软件应当具备先提醒升级、再自动升级为最新版本的功能。
c) 网上交易、语音交易、自助交易等外围信息系统是否逐笔记录交易委托、银期转账、密码修改、账户登录等操作的客户交易终端信息。核心业务系统还应当同时逐笔存储交易委托、银期转账等操作的客户交易终端信息。
d) 是否为期货交易所采集客户交易终端信息提供相应的数据接口，并在相关技术规范发布之日起 12 个月内，完成信息系统的改造升级，改造后的信息系统应符合国家信息安全标准。
e) 是否按照本规定的要求建设、改造和维护相关信息系统，以妥善管理客户交易终端信息，并提供符合技术规范的查询接口。应当采取必要的技术手段，满足交易时段客户信息查询的需要。
f) 是否按照技术规范对客户的主要开户资料进行电子化，并妥善保存在信息系统中。应当按照技术规范在 18 个月内对新增账户实施开户资料电子化，存量的正常交易类账户应在 36 个月内完成开户资料电子化。
g) 是否妥善保存客户交易终端信息和开户资料电子化信息，保存期限不得少于 20 年。应妥善保存交易时段客户交易区的监控录像资料，保存期限不得少于 6 个月。
h) 是否采取可靠的措施，采集、记录、存储、报送与客户身份识别有关的信息，不得以任何理由拒绝承担相应职责。公司及其工作人员应当对客户交易终端信息予以保密，不得泄露。
i) 是否严格限制对客户交易终端信息的人工操作权限，明确查询权限和操作流程，建立日志文档并指定专人妥善保管。禁止任何人对客户交易终端信息进行隐匿、伪造、篡改或毁损。
j) 发生影响采集、记录、存储、报送客户交易终端信息安全的重大事件时，是否及时向公司住所地和事件发生地证监局报告，不得隐瞒。

A.4.5.2.12 督促检查

本项要求包括：

a) 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。
b) 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。
c) 是否每季组织开展内部检查，形成检查报告。
d) 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。
e) 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。
f) 是否对检查和审计的结果采取纠正性和预防性的措施。
g) 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.4.5.2.13 监控分析

本项要求包括：

a) 是否应采取监控措施，配备监控和报警工具，对影响信息系统正常运行的关键对象，包括机房环境、网络、通信线路、主机、存储、数据库、核心交易业务相关的应用系统、安全设备等进行监控，形成记录并妥善保存。报警方式可包括声光、电话、短信、邮件等。
b) 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。（本项适用于：信息系统等级保护三级系统）
c) 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。（本项适用于：信息系统等级保护三级系统）
d) 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，应开启自动监控系统和自动报警系统。
e) 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。
f) 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。
g) 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。
h) 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。
i) 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。
j) 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。
k) 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。
l) 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。
m) 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。
n) 门户网站监控指标是否包括网页内容、日均访问量等。
o) 是否针对不同系统设置合理的监测频度。

p) 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。
q) 是否保存监控产生的日志，保存时间不少于一年。
r) 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。应至少每季度全面评估监控日志和操作记录，分析异常情况，形成评估报告。
s) 是否建立有效机制，保障总部了解各个营业部的运行情况。
t) 营业部是否对设备容量、交易通信链路进行监控，及时进行必要的升级。（本项适用于：三类、四类期货公司）

A.4.5.2.14 网络安全管理

本项要求包括：

a) 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。
b) 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。
c) 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；应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。
d) 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；
   1) 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；
   2) 实施漏洞扫描或漏洞修补前，应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；
   3) 漏洞扫描或漏洞修补后应进行验证测试，以保证网络系统的正常运行。
e) 是否保证所有与外部系统的连接均得到授权和批准。
f) 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；应在配置变更前、变更后分别对网络设备的配置文件进行备份。（本项适用于：信息系统等级保护三级系统）
g) 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。（本项适用于：信息系统等级保护三级系统）
h) 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。（本项适用于：信息系统等级保护三级系统）
i) 是否合理设置安全域，绘制网络拓扑图，并保持更新。
j) 是否配置、调优网络系统的参数。
k) 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。
l) 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；应正确设置安全设备的接口参数和过滤规则。
m) 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。
n) 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，特殊紧急情况下应采取限制登录 IP、数字证书或动态口令认证、全程监控等措施，在操作完成后应及时关闭，并对维护过程进行监控并留存记录。
o) 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。
p) 是否禁止通过无线网络对交易业务网进行网络管理。
q) 计算机网络跳线是否整齐干净，跳线标识清晰。

r) 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。
s) 是否保持网络设备的可用性，及时维修、更换故障设备。
t) 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.4.5.2.15 系统安全管理

本项要求包括：

a) 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。
b) 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。
c) 是否安装系统的最新补丁程序，在安装系统补丁前，应首先充分评估并在测试环境中测试通过，并对重要文件进行备份后，方可实施系统补丁程序的安装；持续跟踪厂商提供的系统升级更新情况，应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。
d) 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。
e) 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。
f) 是否至少每月对运行日志和审计数据进行分析。
g) 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，权限设定应当遵循最小授权原则。（本项适用于：信息系统等级保护三级系统）
h) 系统管理是否包括：
   1) 应保持系统的可用性，及时维修、更换故障设备和更新软件；
   2) 应负责应用系统、操作系统的参数配置、调优，编制文档并保持更新；
   3) 应定期对系统容量进行检查和评估，形成评估报告；
   4) 应负责管理系统和应用程序服务进程，并关闭与业务无关的服务；
   5) 应定期检查应用系统、操作系统的用户、口令及权限设置的正确性。
i) 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。
j) 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.4.5.2.16 恶意代码防范

本项要求包括：

a) 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。
b) 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。
c) 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。
d) 是否定期检查信息系统内各种产品的恶意代码库的升级情况并进行记录，对主机防病毒产品、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及时分析处理，并形成书面的报表和总结汇报。（本项适用于：信息系统等级保护三级系统）
e) 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。
f) 网上交易软件是否采取安全的密码输入方式，增强防御恶意程序窃取密码的功能。

A.4.5.2.17 密码管理

本项要求包括：

a) 是否使用符合国家密码管理规定的密码技术和产品。（本项适用于：信息系统等级保护二级系统）

b) 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。（本项适用于：信息系统等级保护三级系统）

A.4.5.2.18 备份与恢复管理

本项要求包括：

a) 是否识别需要定期备份的重要业务信息、系统数据及软件系统等。

b) 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。

c) 是否根据数据的重要性及其对系统运行的影响，制定数据的备份策略和恢复策略，备份策略指明备份数据的放置场所、文件命名规则、介质替换频率和数据离站运输方法。

d) 是否建立控制数据备份和恢复过程的程序，对备份过程进行记录，所有文件和记录应妥善保存。（本项适用于：信息系统等级保护三级系统）

e) 是否定期执行恢复程序，检查和测试备份介质的有效性，确保可以在恢复程序规定的时间内完成备份的恢复。（本项适用于：信息系统等级保护三级系统）

f) 交易系统及其部件应有备份。（本项适用于：一类、二类期货公司）

g) 交易系统及其部件是否有热备份。（本项适用于：三类、四类期货公司）

h) 交易系统与交易所连接的网络设备是否无单点故障。（本项适用于：二类、三类、四类期货公司）

i) 生产环境内的网络设备是否有备份。（本项适用于：一类、二类期货公司）

j) 生产环境内的网络设备是否有热备份。（本项适用于：三类、四类期货公司）

k) 是否有灾难备份中心，可以接管所有核心业务的运行。（本项适用于：三类期货公司可选）

l) 是否有与生产中心直线距离至少达到 100 公里且位于不同城市的灾难备份中心，可以接管所有核心业务的运行。（本项适用于：四类期货公司）

m) 灾难备份中心是否有满足关键业务功能恢复运作要求的场地和设施。（本项适用于：三类、四类期货公司，其中三类期货公司可选）

n) 是否采用远程数据复制技术，并利用通信网络将关键数据实时复制到灾难备份中心。（本项适用于：三类、四类期货公司，其中三类期货公司可选）

o) 灾难备份中心是否配备灾难恢复所需的全部运行环境，并处于就绪状态或运行状态。（本项适用于：三类、四类期货公司，其中三类期货公司可选）

p) 灾难备份中心是否配备灾难恢复所需的通信链路和网络设备，并处于就绪状态。（本项适用于：三类、四类期货公司，其中三类期货公司可选）

q) 灾难备份中心是否在交易和结算时间内有相关技术支持和保障人员。（本项适用于：三类、四类期货公司，其中三类期货公司可选）

r) 灾难备份中心是否有相应的运行维护流程。（本项适用于：三类、四类期货公司，其中三类期货公司可选）

s) 是否有详细的灾难恢复预案及操作流程，并根据流程每年进行演练。（本项适用于：三类、四类期货公司，其中三类期货公司可选）

t) 设计灾难备份中心运行时，处理能力是否不低于主系统处理能力的 50%。（本项适用于：三类、四类期货公司，其中三类期货公司可选）

u) 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；每季度至少对数据备份进行一次有效性验证。
v) 重要信息系统的故障应对能力是否达到《证券期货经营机构信息系统备份能力标准》第三级要求。（本项适用于：一类、二类期货公司）
w) 重要信息系统的故障应对能力是否达到《证券期货经营机构信息系统备份能力标准》第四级要求。（本项适用于：三类期货公司）
x) 重要信息系统的故障应对能力是否达到《证券期货经营机构信息系统备份能力标准》第六级的要求。（本项适用于：四类期货公司）
y) 2014 年底前，二类期货公司重要信息系统的故障应对能力是否达到《证券期货经营机构信息系统备份能力标准》第四级要求。（本项适用于：二类期货公司）
z) 2014 年底前，三类期货公司重要信息系统的灾难应对能力是否达到《证券期货经营机构信息系统备份能力标准》第五级要求。（本项适用于：三类期货公司）
aa) 2015 年底前，一类期货公司是否进一步提高重要信息系统的故障应对能力，达到《备份标准》第四级的要求。（本项适用于：一类期货公司）
bb) 是否制定信息系统备份能力建设工作计划。
cc) 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。
dd) 提供现场交易的营业部关键设备是否有冗余。

A.4.5.2.19 事件与问题管理

本项要求包括：

a) 是否对安全检查情况进行评估，形成评估报告。
b) 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。
c) 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。
d) 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。
e) 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。
f) 是否每月回顾、分析事件处理记录，完成事件分析报告。
g) 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。
h) 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。
i) 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。
j) 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。
k) 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。

A.4.5.2.20 网站安全

本项要求包括：

a) 是否建立对门户网站内容的审核制度、完整的发布流程和监控机制。
b) 是否有专人监控网站内容，发现问题后及时处理。
c) 是否定期对网站进行安全检查，并对隐患进行及时处理。
d) 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。
e) 是否准备足够措施，能在发现网站被篡改后 5 分钟内停止发布被篡改的内容。

f) 是否安装木马防护软件并定期更新。
g) 是否对网站主页内容实现自动监控，能在5分钟内检测到篡改。（本项适用于：三类、四类期货公司）
h) 是否请有资质的专业安全机构定期对网站提供安全评估或扫描服务，并对安全漏洞进行整改。
i) 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。

A.4.5.2.21 软件正版化

本项要求包括：
a) 是否明确部门或责任人，负责本单位软件正版化工作。
b) 是否落实软件采购经费，做好软件正版化工作。
c) 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。
d) 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。
e) 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。
f) 是否每年对软件正版化情况开展自查。
g) 操作系统软件是否有授权（服务器）。
h) 操作系统是否有授权（办公计算机）。
i) 数据库软件是否有授权。
j) 杀毒软件是否有授权。
k) 办公文字处理软件是否有授权。
l) 办公专业处理软件是否有授权。
m) 应用服务器软件是否有授权。
n) 专用业务软件是否有授权。
o) 是否制定了软件正版化计划。

A.4.5.3 应急处置

A.4.5.3.1 应急准备

本项要求包括：
a) 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。
b) 是否对系统相关的人员进行应急预案培训，应急预案的培训应至少每年举办一次。
c) 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。（本项适用于：信息系统等级保护三级系统）
d) 是否定期对应急预案进行演练，根据不同的应急恢复内容，确定演练的周期；应至少每年对应急预案进行演练。（本项适用于：信息系统等级保护三级系统）
e) 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。（本项适用于：信息系统等级保护三级系统）
f) 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。
g) 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。

h) 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。

i) 是否制定了网络与信息安全事件应急预案，内容至少包括：
   1) 应急预案编制的目的和依据；
   2) 应急预案的适用范围；
   3) 应急处置的组织体系及职责；
   4) 预防措施、保障措施与应急准备；
   5) 预警监测、处置和信息报送；
   6) 网络与信息安全事件的分级分类；
   7) 网络与信息安全事件的报告流程；
   8) 网络与信息安全事件处置的一般原则；
   9) 网络与信息安全事件处置的具体方案；
   10) 网络与信息安全事件内部调查处理以及分析总结的要求。

j) 应急预案是否符合如下要求：
   1) 网络与信息安全事件处置的具体方案应包括各种可能发生的技术故障的应急处置流程、报告流程等；
   2) 应针对各种技术故障拟定统一的解释口径和通知公告模板；
   3) 应每年至少进行一次评估，并及时修订；
   4) 应根据应急演练的情况进行评估和更新；
   5) 应向住所地证监局报备；
   6) 在应急预案发生重大变化时，应及时重新报备。

k) 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。

l) 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。

m) 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。

n) 是否建立有效的应急通讯联络系统，确保信息畅通。

o) 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。

p) 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。

q) 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。

r) 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。

s) 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。

t) 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。

u) 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。

v) 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。

w) 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。
x) 是否每半年至少组织一次网络与信息安全应急演练。
y) 是否记录演练情况，演练记录至少保存两年。
z) 是否对演练中发现的问题进行改进。
aa) 是否每年向住所地证监局报告年度应急演练情况。
bb) 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。
cc) 是否具有电力设施实时切换演练制度和记录。（本项适用于：三类、四类期货公司）
dd) 是否建立健全网络与信息安全事件应急组织体系，对核心系统的常见故障应有书面的应急预案和排障流程。
ee) 应参与交易所等行业相关机构组织的测试和应急演练并有记录。
ff) 应根据机构、人员、技术等变化，及时调整应急预案。
gg) 演练前是否制定详细的应急演练计划，并根据计划进行演练。
hh) 应准备必要工具，以便应急预案的顺利执行。
ii) 网上信息系统应急预案是否针对电力、通信等基础设施故障、计算机硬件或网络设备故障、操作系统或应用系统故障、操作系统或应用系统漏洞、病毒入侵、恶意攻击、误操作、不可抗力等可能的故障原因制定对应的应急恢复操作流程或步骤。
jj) 营业部应有有效的日常运行流程和应急处理流程，并进行适当的演练。

A.4.5.3.2 应急处置

本项要求包括：

a) 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。
b) 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。
c) 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。
d) 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。
e) 是否记录并保存所有报告的安全弱点和可疑事件，分析事件原因，监督事态发展，采取措施避免安全事件发生。（本项适用于：信息系统等级保护二级系统）
f) 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。（本项适用于：信息系统等级保护三级系统）
g) 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。（本项适用于：信息系统等级保护三级系统）
h) 是否做好应急处置的相关记录，保留有关证据。
i) 是否对造成系统中断和造成信息泄密的安全事件应采用不同的处理程序和报告程序。（本项适用于：信息系统等级保护三级系统）
j) 是否对证券期货行业内通报的重大安全隐患，应立即进行专项安全检查。
k) 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。
l) 是否在应急处置中注意保证工作人员的人身安全。

m) 是否在应急处置结束前，保证专人 24 小时值班。
n) 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。
o) 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。

A.4.5.3.3 调查处理

本项要求包括：

a) 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。事件总结报告内容应当包括：
   1) 事件基本情况，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；
   2) 应急处置情况，包括事件报告的情况、采取的措施及效果；
   3) 事件调查情况，包括事件原因、事件级别、责任认定和结论；
   4) 事件处理情况，包括事件暴露出的问题及采取的整改措施，责任追究情况。
b) 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。
c) 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。
d) 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。
e) 是否向住所地中国证监会派出机构进行预警报告、应急报告和事件总结报告，分支机构应当向所在地中国证监会派出机构进行预警报告、应急报告和事件总结报告。事件总结报告同时抄送中国期货业协会。
f) 发生信息安全事件影响到期货交易业务时,是否同时向相关期货交易所进行应急报告和事件总结报告；影响到其他机构的，应当及时向有关机构进行应急通报。
g) 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。

附 录 B
（规范性附录）
系统建设合规审计项汇总

B.1 需求论证

B.1.1 需求分析

a) 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。
b) 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。

B.1.2 可行性论证

a) 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。
b) 项目目标是否与现有需求相匹配。
c) 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。
d) 可行性分析是否已充分考虑复用现有资源的可能性。

B.2 预算制定

B.2.1 预算编制

a) 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。
b) 是否有预算评审的机构或机制。
c) 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。

B.2.2 预算调整

a) 预算管理是否明确预算调整原则和条件。
b) 是否有论述预算调整合理性的书面材料。
c) 预算管理是否建立预算调整审批程序和流程。
d) 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。

B.2.3 预算执行

a) 预算管理是否建立预算审批程序和流程。
b) 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。
c) 会议纪要、审批记录等相关资料是否完整且归档。

B.3 项目立项

B.3.1 立项机构

a) 项目管理是否有项目审核小组或委员会。
b) 项目管理审核小组或委员会成员是否 3 人以上（含）。

c) 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。
d) 项目管理审核小组或委员会成员是否实行任期制。
e) 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。
f) 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。

B.3.2 立项审批

a) 项目管理是否有完整有效的项目立项报告。
b) 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。
c) 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。
d) 是否对需求分析、可行性论证、预算编制进行了审查。

B.4 项目采购

B.4.1 采购申请

a) 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。
b) 对同一需求进行分批采购是否提供需求说明。

B.4.2 采购程序

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。

B.4.3 职责分工

是否明确IT项目采购的职责分工。

B.4.4 产品列表

是否有可选产品列表。

B.4.5 计划制定与审批

a) 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。
b) 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。

B.4.6 询价采购

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。

B.4.7 单一品牌或单一来源采购

项目是否对单一品牌或单一来源采购有书面说明材料。

B.4.8 采购验收

a) 是否对产品验收进行签字留痕确认和复核。
b) 采购归档
c) 项目采购相关文档和凭据是否归档。

B.5 项目招标

B.5.1 招标制度

a) 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。
b) 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。
c) 项目审批人员构成是否合理，是否履职尽责。

B.5.2 招标公告

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。

B.5.3 发送招标邀请

a) 投标人的资质是否符合标书要求。
b) 项目是否进行市场询价。

B.5.4 委托代理机构招标

a) 是否有代理机构选择程序。
b) 代理机构是否有相关资质。
c) 选择的代理机构是否经过项目管理委员会审批。

B.5.5 开标、评标、中标现场流程（委托招标除外）

a) 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。
b) 评标委员会人员构成是否合理。
c) 是否采取相关保密措施，缩小知悉范围。

B.5.6 中标公示

是否在规定时间段在指定媒体等公开渠道发布中标公示。

B.6 商务谈判

B.6.1 谈判人员

a) 是否由专门工作小组或委员会负责商务谈判。
b) 项目是否有谈判人员名单及其职责说明。
c) 项目是否有谈判人员签字的相关记录。

B.6.2 谈判内容

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。

B.6.3 谈判过程

a) 项目是否有标书、情况说明等相关书面材料。

b) 如有低于标书要求项，是否有相关书面材料。

B.6.4 结果记录

项目是否有谈判纪要等相关记录，并由全体谈判人员签字。

B.7 供应商管理

B.7.1 供应商列表建立

a) 是否制定供应商列表管理制度。
b) 可选供应商的相关材料是否齐备。
c) 可选供应商数量是否达到一定规模。

B.7.2 供应商列表调整

a) 是否有供应商列表调整策略。
b) 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。
c) 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。

B.8 合同管理

B.8.1 合同制度体系

a) 是否有合同管理制度、流程。
b) 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。
c) 合同合规性
d) 是否按照制度规定，有财务、法律等部门审核通过的记录。

B.8.2 合同签订前

a) 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。
b) 合同制度中是否具有防范被篡改的控制机制。

B.8.3 合同履行

a) 是否有项目合同履约情况定期检查机制。
b) 是否有保密协议签订内容。
c) 是否有安全手段进行敏感信息保护。

B.9 项目验收

B.9.1 成立验收小组

a) 验收小组和招标小组成员是否相同。
b) 验收小组是否签名廉洁承诺书。

B.9.2 验收过程

a) 合同是否有相关具体指标，且与验收表单一致。
b) 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。
c) 是否有合同变更记录和验收记录。

B.9.3 系统上线

a) 系统上线是否经过合理审批流程。
b) 信息系统项目开发技术文档是否保存完整。

B.10 钱款支付

B.10.1 支付条件

项目费用是否有合同支付记录及相关审批手续。

说明：

1.合规审计按照 IT 项目生命周期对 IT 项目进行合规审计，重点关注立项、采购和实施 3 个阶段。
2.立项阶段主要有需求分析、可行性论证、预算制定和项目立项 4 个环节，这 4 个环节具有顺序性。
3.采购阶段主要有项目采购、项目招标、商务谈判、供应商管理等 4 个环节，这 4 个环节具有并行性。
4.实施阶段主要有合同管理、项目验收、钱款支付 3 个环节，这 3 个环节具有并行性。

附 录 C
（规范性附录）
系统应用绩效审计项汇总

C.1 系统建设

C.1.1 项目提出

a) 项目建设目标、建设内容是否明确。
b) 项目的设立是否符合相关的政策、文件要求。

C.1.2 项目验收

a) 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。
b) 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。
c) 建设项目是否如期完成上线。
d) 建设项目如果没有如期上线，是否有合理的理由。
e) 预算的建设资金与实际的建设资金的差距是否合理。
f) 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。
g) 预算的运营资金与实际的运营资金的差距是否合理。
h) 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。

C.1.3 系统性能

a) 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。
b) 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。
c) 系统、设备实际使用时长是否合理。
d) 系统实际处理能力与最大处理能力比值是否合理。
e) 系统是否能快速扩展。
f) 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%。
g) 是否提高了数据共享水平。

C.2 经济效益

C.2.1 有形经济效益

项目完成产生的经济效益是否与立项报告的预期一致。

C.2.2 无形经济效益

a) 项目建成后，组织机构是否得到优化调整。
b) 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。
c) 项目建成后，是否提高了办事效率。
d) 是否达到国内或行业先进水平。

C.3 用户满意度

C.3.1 满意度调查

a) 项目建成后，业务人员对系统功能、性能、可用性等是否认可。
b) 项目建成后，IT 人员对系统功能、性能、可用性等是否认可。
c) 项目建成后，外部机构对系统功能、性能、可用性等是否认可。
d) 是否按用户的要求提供了相关的服务。

C.3.2 投诉情况

a) 是否有关于系统功能的投诉。
b) 是否有关于系统性能的投诉。

C.3.3 问题与事件管理

a) 所有事件报告、服务请求和相关需求是否能得到及时处理。
b) 是否可以有效避免重复问题的发生。