期货公司信息技术管理指引（2019年10月修订）

第一章 总则

第一条

为了进一步促进期货公司信息系统建设，提高运维保障水平，根据国家网络安全法律法规和《期货交易管理条例》、《期货公司监督管理办法》，特制定《期货公司信息技术管理指引》（以下简称“本指引”）。

第二条

本指引实行分类管理，以适应期货公司不同的信息技术基础和技术要求。本指引共分四类，从一类到四类，要求依次提高，且高类别的要求包含低类别的要求，低类别的可选要求在高类别中自动成为必须要求。所有要求，如果在前面一类要求中没有出现，则被标识为“[新增]”，否则被标识为“[延续]”。

第三条

期货公司信息技术管理工作是一项全面、科学、严谨的系统工程，本指引是期货公司开展信息技术管理工作的要点和底线性要求，并不涵盖所有的技术细节。期货公司除认真落实本指引的各项具体要求外，仍应加强其他技术细节的管理工作。

第四条

本指引中使用的名词解释如下：
（一）核心系统指期货公司集中进行交易、结算、风控和银期转账等业务运作所使用的系统；
（二）生产环境，是指正式运行交易系统的计算机环境，包括生产机房、网络、主机、存储、数据库及应用等为业务运行提供服务的所有软硬件环境；
（三）交易系统的所有部件指交易服务器、交换机、报盘机、路由器、网关、防火墙等；
（四）有效隔离指物理分隔、防火墙、网闸、VLAN及等效措施；
（五）现场交易是指期货公司客户使用期货公司现场网络和相关技术设备进行期货交易的行为；
（六）本指引中的机房指部署生产环境的所有机房。

第二章 一类要求

第一条

技术管理
（一）组织结构
（1）[必须][新增] 应设有技术部门，有专职技术人员，并有明确的职责分工和岗位说明。

（2）[必须][新增] 总部技术部门人员总数占公司总部人数的比例不少于8%。

（3）[必须][新增] 总部技术部门人员不少于5人，对于开展连续交易的期货公司应达到8人。机房托管且由托管方维护机房基础设施的，可核减2人。

（4） [必须][新增] 公司应设立内部审计岗位，定期对IT流程执行情况进行审计。

（5）[必须][新增] 应建立负责本公司信息技术规划和网络安全管理的跨部门机构，其职责包括系统规划、安全管理、IT治理等。

（6）[必须][新增] 应建立信息技术合规与风险管理机制，对信息技术应用全过程的合规风险进行评估、识别、监控和干预，合规风控管理部门应参与上述工作机制，并独立出具意见。

（7）[必须][新增] 应至少每年对公司信息技术应用合规风险情况进行一次全面评估，并妥善保存评估记录，保存期限不低于5年。

（8）[必须][新增] 应与所有总部技术部门人员签署保密协议，并对技术人员的离岗严格管理。

（9）[必须][新增] 应设立2名技术联络员，负责组织、协调和处理与网络安全管理部门、交易所及相关单位的各项技术事宜。

（10）[必须][新增] 总部技术部门应有至少1名安全管理人员。

（11）[必须][新增] 提供现场交易的分支机构应配备至少1名技术人员。

（12）[必须][新增] 总部技术部门应有至少1名网络管理人员。

（二） 培训

（1）[必须][新增] 对所有上岗技术人员应进行岗位培训。

（2）[必须][新增] 总部技术部门的所有人员每两年参加期货业协会组织的技术培训应达到15学时。

（3）[必须][新增] 应有明确的培训教材，用于培训上岗操作人员。

（4）[必须][新增] 应有对总部技术部门人员的年度培训计划，并根据计划实施。

（5）[必须][新增] 应定期对技术部门各个岗位的人员进行安全教育和培训，培训内容应包含机房消防及相关应急内容等。

（三） 人员素质

（1）[必须][新增] 总部技术部门人员50%以上应有信息技术相关专业大学本科或以上教育背景。

（2）[必须][新增] 总部技术部门人员至少2人应具备1年及以上的系统运行维护经验。

（四）信息技术服务提供商管理

（1）[必须][新增] 应与信息技术服务提供商签订服务保障协议。

（2）[必须][新增] 应与核心系统的服务提供商签署保密协议。

（3）[必须][新增] 应有信息技术服务提供商的准确联系方式。

（4）[必须][新增] 选择信息技术服务提供商时应评估其资质、经营行为、业绩、服务体系、服务品质和违法违规等要素。

（5）[必须][新增] 应至少每年对信息技术服务提供商的服务质量进行一次评估。

（五）IT投入
（1）[必须][新增] 最近三个会计年度IT投入平均数额应不少于最近三个会计年度平均净利润的6%或不少于最近三个会计年度平均营业收入的3%，取二者数额较大者。

第二条

机房建设
（一）基本
（1）[必须][新增] 机房应为独立封闭区域，并配备门禁。

（2）[必须][新增] 机房承重应达到300公斤每平方米。

（3）[必须][新增] 机房应具备火警检测、灭火和应急照明设施。

（4）[必须][新增] 机房应当具备自动灭火设施。

（5）[必须][新增] 机房出入口和内部应安装7×24小时录像监控设施，录像至少保存90天。

（6）[必须][新增] 机房应有防雷接地、防鼠以及防静电的设施。

（7）[必须][新增] 机房内应安装漏水检测设施，并能够自动报警。

（8）[必须][新增] 机房内应采用卤代烷或可替代的其他气体灭火装置。

（9）[必须][新增] 核心系统所在机房应配备机房环境动力监测系统，明确监测指标，实现声音和短信等自动报警。

（二）供电
（1）[必须][新增] 机房应配备在线UPS设施，UPS应当存放在独立封闭区域。

（2）[必须][新增] UPS供电时间应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。如无上述应急供电方式，UPS的电池应能够支撑4个小时。

（三）空调
（1）[必须][新增] 应配有与机房热容量匹配的精密空调。

（2）[必须][新增] 对机房温湿度应有监控措施和记录。

（四）布线
（1）[必须][新增] 强弱电布线应分开。

（2）[必须][新增] 所有弱电布线应有清晰的线标。

（3）[必须][新增] 强电电缆应有屏蔽或隔离措施。

（4）[必须][新增] 所有布线应置于管道或桥架中。

（五）维护
（1）[必须][新增] 所有UPS和空调设施都应有专业维护人员，或与专业机构签订维护合同。

（2）[必须][新增] 应定期对所有UPS和空调设施进行恰当维护，有维护记录。

第三条

交易系统
（一）功能
（1）[必须][新增] 交易系统应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。

（2）[必须][新增] 交易系统应具备对客户进行实时风险控制的功能。

（3）[必须][新增] 交易系统应产生、记录并存储必要的日志信息供审计使用。日志信息保存期限至少为2年。

（4）[必须][新增] 核心系统应具备向期货市场监控中心上报规定数据的功能。

（5）[必须][新增] 不应具有篡改、伪造交易系统数据或其他可能导致数据失真的功能。

（6）[必须][新增] 交易系统应有授权管理功能。

（7）[必须][新增] 核心系统应有运行监控措施。

（8）[必须][新增] 交易系统应具备流量控制管理功能。

（9）[必须][新增] 应要求核心系统供应商提供交易、银期及相关管理接口。

（10）[必须][新增] 核心系统应具备能够支持逐一录入、文件导入、接口调用方式多渠道开户的功能。

（11）[必须][新增] 核心系统应具备链接期货市场监控中心投资者查询取密钥系统的功能。

（12）[必须][新增] 对于开展互联网开户的期货公司，互联网开户系统应具有落实开户实名制及投资者适当性制度的功能。

（13）[必须][新增] 交易系统应具有并启用客户交易接入认证功能。

（14）[必须][新增] 核心系统应具有并启用客户密码安全管理功能，包括但不限于初始密码修改、弱口令及登录失败次数限制等功能。

（二）性能和容量
（1）[必须][新增] 交易系统的性能和容量应达到所有其作为会员的交易所的要求。

（2）[必须][新增] 应对交易系统的主要业务指标进行实时监控。

（3）[必须][新增] 应对交易系统的主要业务监控指标进行记录。

（4）[必须][新增] 应对所有接入交易所的交易通信链路进行监控。

（5）[必须][新增] 接入交易所的交易通信链路应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。

（6）[必须][新增] 应对所有网上交易的通信链路进行监控。

（三）系统冗余
（1）[必须][新增] 核心系统及其部件应有备份，备份能力应达到RTO<=5分钟、RPO<=30秒。

（2）[必须][新增] 与交易所连接的网络设备应无单点故障。

（3）[必须][新增] 生产环境内的网络设备应有热备份，备份能力应达到RTO<=5分钟。

（4）[必须][新增] 应使用多个电信运营商的链路作为网上交易的通信链路。

（四）行情冗余
（1）[必须][新增] 应提供至少2套行情服务互为备份。

（五）银期系统冗余
（1）[必须][新增] 应与至少2家银行实现全国性银期转帐。

第四条

安全
（一）网络隔离
（1）[必须][新增] 生产网与互联网应实现有效隔离。

（2）[必须][新增] 网站与网上交易系统应实现有效隔离。

（3）[必须][新增] 生产网与办公网应实现有效隔离。

（4）[必须][新增] 总部的生产网与分支机构的网络应实现有效隔离。

（5）[必须][新增] 生产网与交易所、银行等外部网络及客户使用的网络应实现有效隔离。

（6）[必须][新增] 生产网与开发、测试网络应实现有效隔离。

（二）防病毒、补丁和安全加固
（1）[必须][新增] 应建立有效机制，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。

（2）[必须][新增] 应对使用Windows平台的计算机部署防病毒软件，定期进行全面检查，并及时进行病毒库的更新。

（3）[必须][新增] 应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。

（4）[必须][新增] 应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。

（5）[必须][新增] 应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。

（6）[必须][新增] 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，应先进行病毒检查。

（7）[必须][新增] 所有生产环境服务器应尽量避免使用telnet、ftp等有安全隐患的服务，与服务器通信应采用加密方式，例如SSH。

（三）网站安全
（1）[必须][新增] 应有专人监控网站内容，发现问题后及时处理。

（2）[必须][新增] 应至少每年对网站进行一次安全检查，并对隐患进行及时处理。

（3）[必须][新增] 应准备足够措施，能在发现网站被篡改后5分钟内停止发布被篡改的内容。

（4）[必须][新增] 应安装木马防护软件并定期更新。

（5）[必须][新增] 网站的内容发布应有审核制度和完整的内容发布流程。

（6）[必须][新增] 应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。

（7）[必须][新增] 应建立网站备份系统，备份能力应达到RTO<=60分钟。具备交易功能的网站，RPO<=5分钟。

（8）[必须][新增] 应对网站数据每天进行一次离线备份，并确保离线数据存放介质安全存放。

（9）[必须][新增] 网站系统WEB服务、数据库服务应分别部署在不同服务器上。

（四）网上交易安全
（1）[必须][新增] 应提供可靠的身份认证机制，网上交易客户端支持多种方式与服务端完成身份认证。

（2）[必须][新增] 服务器上的用户认证信息应加密存放。

（3）[必须][新增] 应在与客户签订的服务合同（网上期货服务合同、期货经纪合同及补充协议、风险揭示书）中载明，客户使用网上期货业务可能面临的风险、期货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）。

（4）[必须][新增] 应提供预留验证信息服务，在客户进行登录时向客户进行显示，帮助客户有效识别仿冒的网上期货信息系统，防范利用仿冒的网上期货信息系统进行诈骗活动。

（5）[必须][新增] 应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。

（6）[必须][新增] 应遵守国家关于公民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。未经客户允许和期货公司审批，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。

（7）[必须][新增] 营业场所的客户交易区应安装录像监控设施，监控录像应覆盖所有交易时段，监控录像资料保存至少6个月。

（五）账户与权限
（1）[必须][新增] 应有生产环境内系统账户与权限的关系表。

（2）[必须][新增] 账户和权限变更应有审批和完整的记录。

（3）[必须][新增] 岗位变动应及时调整对应系统的账户和权限。

（4）[必须][新增] 应避免使用超级管理员账户完成日常业务操作。

（六）口令管理
（1）[必须][新增] 所有书面方式保存的口令应有安全的物理保护措施。

（2）[必须][新增] 口令应有复杂度要求。

（3）[必须][新增] 口令应定期更换。

（4）[必须][新增] 数据库用户口令不得明文存放在计算机中。

（七）安全审计
（1）[必须][新增] 交易系统的主要业务操作应产生审计记录，审计记录保存期限至少为2年。

（2）[必须][新增] 应采取有效措施防止删除、修改或覆盖审计记录。

第五条

日常运行
（一）岗位
（1）[必须][新增] 应建立日常值班制度，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。

（2）[必须][新增] 初始化、结算、数据备份等关键操作过程和结果应有复核。

（3）[必须][新增] 交易运行期间应有现场保障人员，设置运维值班电话，以及时维护和应急处理。

（4）[必须][新增] 应实现双人日常值班。

（5）[必须][新增] 应建立文档管理制度，对运维过程中涉及的各类文档进行分类管理。

（二）日常操作与巡检
（1）[必须][新增] 在开盘前、休市、收市等关键时间点应对生产环境运行状态进行巡检。

（2）[必须][新增] 日常操作和巡检应保留记录，并有操作和复核人员的签名。

（3）[必须][新增] 应有生产环境日常操作和定期维护的操作手册，手册中应有详细的操作步骤。

（4）[必须][新增] 交易期间应对核心系统和网络系统状态及网络安全事件进行实时监控、记录，并能及时、有效地报警，相关系统日志至少保留6个月。

（5）[必须][新增] 应保留应用系统的操作日志记录，保存期限至少为2年。

（6）[必须][新增] 应记录生产环境发生的故障和异常。

（7）[必须][新增] 应建立完善和更新重要手册的机制。

（8）[必须][新增] 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。

（9）[必须][新增] 采用自动化运维工具进行日常操作的，应具有有效的机制确保自动化运维工具安全、稳定运行，应具有专门的管理人员，并将自动化运维工具的部署及调整纳入变更管理。

（三）机房进出
（1）[必须][新增] 应建立机房管理制度，对机房环境、供电、空调、消防、安防等基础设施进行运行维护，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。

（2）[必须][新增] 非技术部门人员进入机房应经过审批，并有技术部门人员陪同，所携带设备应专门登记。

（3）[必须][新增] 交易期间如无应急或者巡检需要，不应进入机房。

第六条

备份
（一）数据备份
（1）[必须][新增] 应根据数据的重要性及其对交易系统运行的影响，制定数据备份策略和恢复策略。

（2）[必须][新增] 应建立数据管理、介质维护、销毁和使用管理制度。
（3）[必须][新增] 应对介质进行明确标识。

（4）[必须][新增] 应确保介质存放在安全环境中，实现对备份数据的控制和保护。

（5）[必须][新增] 每日应对结算后数据进行备份，网站数据应按照备份计划进行备份。

（6）[必须][新增] 每周应将结算后数据备份介质进行同城和异地存放。

（7）[必须][新增] 应定期对主要备份业务数据进行恢复验证，根据介质使用期限及时转储数据。

（8）[必须][新增] 应指定专人负责保管业务数据备份介质。

（二）灾难备份
（1）[必须][新增] 应有灾难备份中心，可以接管所有核心业务的运行。

（2）[必须][新增] 灾难备份中心应有满足关键业务功能恢复运作要求的场地和设施。

（3）[必须][新增] 应采取必要手段保证灾难备份中心数据与核心系统保持一致。

（4）[必须][新增] 灾难备份中心应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。

（5）[必须][新增] 灾难备份中心应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。

（6）[必须][新增] 灾难备份中心应在交易和结算时间内有相关技术支持和保障人员。

（7）[必须][新增] 灾难备份中心应有相应的运行维护流程。

（8）[必须][新增] 应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。

（9）[必须][新增] 灾难备份中心的备份能力应达到RTO<=12小时； RPO<=5分钟。

（10）[必须][新增] 设计灾难备份中心运行时，处理能力应不低于主系统处理能力的50%。

第七条

系统维护
（一）变更管理
（1）[必须][新增] 应将所有涉及核心系统的软硬件变更纳入变更管理范围。

（2）[必须][新增] 每次变更前应进行评估和必要的测试。

（3）[必须][新增] 所有变更操作应有操作记录。

（4）[必须][新增] 所有变更应进行事后检查。

（5）[必须][新增] 对于风险较大的变更，在条件允许的情况下，应制定应急和回退方案。

（6）[必须][新增] 对于风险较大的变更，应在变更后对系统的运行情况进行跟踪。

（7）[必须][新增] 应及时对变更涉及的系统配置和操作手册进行修改。

（8）[必须][新增] 应建立信息系统软硬件测试管理制度和流程，规范各类系统软硬件上线前的测试。

（9）[必须][新增] 应在独立于生产环境的测试环境中进行技术和业务测试，因业务需要使用生产环境进行测试的，应纳入变更管理流程。

（10）[必须][新增] 应对测试所使用的客户信息进行数据脱敏，因业务需要使用未脱敏数据进行测试的，应采取数据使用授权、操作审计等安全控制措施防止客户信息泄露。

（二）配置管理
（1）[必须][新增] 应具有生产环境设计和部署文档，并根据变更及时更新。

（2）[必须][新增] 应对重要的配置信息进行有效备份。

（3）[必须][新增] 应建立配置管理制度和配置文档库。

（三）容量管理
（1）[必须][新增] 每年应对核心系统的性能和容量情况进行评估。

（2）[必须][新增] 应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。

（四）应急演练
（1）[必须][新增] 应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及安全风险应有书面的应急预案和排障流程。

（2）[必须][新增] 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。

（3）[必须][新增] 应根据机构、人员、技术等变化，及时调整应急预案。

（4）[必须][新增] 演练前应制定详细的应急演练计划，并根据计划进行演练。

（5）[必须][新增] 应准备必要工具和设备设施，以便应急预案的顺利执行。

（五）技术事故管理
（1）[必须][新增] 应建立技术事故报告制度和流程。

（2）[必须][新增] 应保存技术事故的记录。

（3）[必须][新增] 应根据技术事故情况，及时提出改进计划，落实改进措施。

第八条

分支机构技术要求
（一）基本要求
（1）[必须][新增] 提供现场交易的分支机构设备区域应是一个单独的区域，用于放置开展业务所需的网络、通信和主机设备。

（2）[必须][新增] 提供现场交易的分支机构应确保在交易时间内有技术人员负责技术系统保障。

（3）[必须][新增] 提供现场交易的分支机构应有与当前运行情况相符的业务系统结构文档。

（4）[必须][新增] 提供现场交易的分支机构应配备防火墙或相当的安全防护设备。

（5）[必须][新增] 提供现场交易的分支机构应对交易系统所使用的计算机部署防病毒软件，定期进行全面检查，并及时进行病毒库及操作系统补丁的更新。

（6）[必须][新增] 应建立有效机制，保障总部了解各个分支机构的运行情况。

（7）[必须][新增] 提供现场交易的分支机构应有总部和信息技术服务提供商的准确联系方式。

（二）交易保障
（1）[必须][新增] 提供现场交易的分支机构应有至少两条交易通信链路。

（2）[必须][新增] 提供现场交易的分支机构关键设备应有冗余。

（3）[必须][新增] 提供现场交易的分支机构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。

第三章 二类要求

第一条

技术管理
（一）组织结构
（1）[必须][延续] 应设有技术部门，有专职技术人员，并有明确的职责分工和岗位说明。

（2）[必须][延续] 总部技术部门人员总数占公司总部人数的比例不少于8%。

（3）[必须][新增] 总部技术部门人员不少于8人，对于开展连续交易的期货公司应达到11人。机房托管且由托管方维护机房基础设施的，可核减2人。

（4）[必须][延续] 公司应设立内部审计岗位，定期对IT流程执行情况进行审计。

（5）[必须][延续] 应建立负责本公司信息技术规划和网络安全管理的跨部门机构，其职责包括系统规划、安全管理、IT治理等。

（6）[必须][延续] 应建立信息技术合规与风险管理机制，对信息技术应用全过程的合规风险进行评估、识别、监控和干预，合规风控管理部门应参与上述工作机制，并独立出具意见。

（7）[必须][延续] 应至少每年对公司信息技术应用合规风险情况进行一次全面评估，并妥善保存评估记录，保存期限不低于5年。

（8）[必须][延续] 应与所有总部技术部门人员签署保密协议，并对技术人员的离岗严格管理。

（9）[必须][延续] 应设立2名技术联络员，负责组织、协调和处理与网络安全管理部门、交易所及相关单位的各项技术事宜。

（10）[必须][延续] 总部技术部门应有至少1名安全管理人员。

（11）[必须][延续] 提供现场交易的分支机构应配备至少1名技术人员。

（12）[必须][延续] 总部技术部门应有至少1名网络管理人员。

（二）培训
（1）[必须][延续] 对所有上岗技术人员应进行岗位培训。

（2）[必须][延续] 总部技术部门的所有人员每两年参加期货业协会组织的技术培训应达到15学时。

（3）[必须][延续] 应有明确的培训教材，用于培训上岗操作人员。

（4）[必须][延续] 应有对总部技术部门人员的年度培训计划，并根据计划实施。

（5）[必须][延续] 应定期对技术部门各个岗位的人员进行安全教育和培训，培训内容应包含机房消防及相关应急内容等。

（三）人员素质
（1）[必须][延续] 总部技术部门人员50%以上应有信息技术相关专业大学本科或以上教育背景。

（2）[必须][新增] 总部技术部门人员至少4人应具备1年及以上的系统运行维护经验。

（四）信息技术服务提供商管理
（1）[必须][延续] 应与信息技术服务提供商签订服务保障协议。

（2）[必须][延续] 应与核心系统的服务提供商签署保密协议。

（3）[必须][延续] 应有信息技术服务提供商的准确联系方式。

（4）[必须][延续] 选择信息技术服务提供商时应评估其资质、经营行为、业绩、服务体系、服务品质和违法违规等要素。

（5）[必须][延续] 应至少每年对信息技术服务提供商的服务质量进行一次评估。

（五）IT投入
（1）[必须][延续] 最近三个会计年度IT投入平均数额应不少于最近三个会计年度平均净利润的6%或不少于最近三个会计年度平均营业收入的3%，取二者数额较大者。

第二条

机房建设
（一）基本
（1）[必须][延续] 机房应为独立封闭区域，并配备门禁。

（2）[必须][延续] 机房承重应达到300公斤每平方米。

（3）[必须][延续] 机房应具备火警检测、灭火和应急照明设施。

（4）[必须][延续] 机房应当具备自动灭火设施。

（5）[必须][延续] 机房出入口和内部应安装7×24小时录像监控设施，录像至少保存90天。

（6）[必须][延续] 机房应有防雷接地、防鼠以及防静电的设施。

（7）[必须][延续] 机房内应安装漏水检测设施，并能够自动报警。

（8）[必须][延续] 机房内应采用卤代烷或可替代的其他气体灭火装置。

（9）[必须][延续] 核心系统所在机房应配备机房环境动力监测系统，明确监测指标，实现声音和短信等自动报警。

（二）供电
（1）[必须][延续] 机房应配备在线UPS设施。UPS应当存放在独立封闭区域。

（2）[必须][新增] 应具有双路市电供电，双路供电应能实现自动切换，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。

（三）空调
（1）[必须][新增] 应配有与机房热容量匹配的精密空调，并有冗余的空调设备。

（2）[必须][延续] 对机房温湿度应有监控措施和记录。

（四）布线
（1）[必须][延续] 强弱电布线应分开。

（2）[必须][延续] 所有弱电布线应有清晰的线标。

（3）[必须][延续] 强电电缆应有屏蔽或隔离措施。

（4）[必须][延续] 所有布线应置于管道或桥架中。

（五）维护
（1）[必须][延续] 所有UPS和空调设施都应有专业维护人员，或与专业机构签订维护合同。

（2）[必须][延续] 应定期对所有UPS和空调设施进行恰当维护，有维护记录。

第三条

交易系统
（一）功能
（1）[必须][延续] 交易系统应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。

（2）[必须][延续] 交易系统应具备对客户进行实时风险控制的功能。

（3）[必须][延续] 交易系统应产生、记录并存储必要的日志信息供审计使用。日志信息保存期限至少为2年。

（4）[必须][延续] 核心系统应具备向期货市场监控中心上报规定数据的功能。

（5）[必须][延续] 不应具有篡改、伪造交易系统数据或其他可能导致数据失真的功能。

（6）[必须][延续] 交易系统应有授权管理功能。

（7）[必须][延续] 核心系统应有运行监控措施。

（8）[必须][延续] 交易系统应具备流量控制管理功能。

（9）[必须][延续] 应要求核心系统供应商提供交易、银期及相关管理接口。

（10）[必须][延续] 核心系统应具备能够支持逐一录入、文件导入、接口调用方式多渠道开户的功能。

（11）[必须][延续] 核心系统应具备链接期货市场监控中心投资者查询取密钥系统的功能。

（12）[必须][延续] 对于开展互联网开户的期货公司，互联网开户系统应具有落实开户实名制及投资者适当性制度的功能。

（13）[必须][延续] 交易系统应具有并启用客户交易接入认证功能。

（14）[必须][延续] 核心系统应具有并启用客户密码安全管理功能，包括但不限于初始密码修改、弱口令及登录失败次数限制等功能。

（二）性能和容量
（1）[必须][延续] 交易系统的性能和容量应达到所有其作为会员的交易所的要求。

（2）[必须][延续] 应对交易系统的主要业务指标进行实时监控。

（3）[必须][延续] 应对交易系统的主要业务监控指标进行记录。

（4）[必须][延续] 应对所有接入交易所的交易通信链路进行监控。

（5）[必须][延续] 接入交易所的交易通信链路应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。

（6）[可选][新增] 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应不超过80%。

（7）[必须][延续] 应对所有网上交易的通信链路进行监控。

（8）[可选][新增] 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应不超过80%。

（三）系统冗余
（1）[必须][延续] 核心系统及其部件应有备份，备份能力应达到RTO<=5分钟、RPO<=30秒。

（2）[必须][延续] 与交易所连接的网络设备应无单点故障。

（2）[必须][延续] 生产环境内的网络设备应有热备份，备份能力应达到RTO<=5分钟。

（4）[必须][延续] 应使用多个电信运营商的链路作为网上交易的通信链路。

（四）行情冗余
（1）[必须][延续] 应提供至少2套行情服务互为备份。

（五）银期系统冗余
（1）[必须][延续] 应与至少2家银行实现全国性银期转帐。

第四条

安全
（一）网络隔离
（1）[必须][延续] 生产网与互联网应实现有效隔离。

（2）[必须][延续] 网站与网上交易系统应实现有效隔离。

（3）[必须][延续] 生产网与办公网应实现有效隔离。

（4）[必须][延续] 总部的生产网与分支机构的网络应实现有效隔离。

（5）[必须][延续] 生产网与交易所、银行等外部网络及客户使用的网络应实现有效隔离。

（6）[必须][延续] 生产网与开发、测试网络应实现有效隔离。

（二）防病毒、补丁和安全加固
（1）[必须][延续] 应建立有效机制，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。

（2）[必须][延续] 应对使用Windows平台的计算机部署防病毒软件，定期进行全面检查，并及时进行病毒库的更新。

（3）[必须][延续] 应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。

（4）[必须][延续] 应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。

（5）[必须][延续] 应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。

（6）[必须][延续] 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，应先进行病毒检查。

（7）[必须][延续] 所有生产环境服务器应尽量避免使用telnet、ftp等有安全隐患的服务，与

服务器通信应采用加密方式，例如SSH。

（三）网站安全
（1）[必须][延续] 应有专人监控网站内容，发现问题后及时处理。

（2）[必须][延续] 应至少每年对网站进行一次安全检查，并对隐患进行及时处理。

（3）[必须][延续] 应准备足够措施，能在发现网站被篡改后5分钟内停止发布被篡改的内容。

（4）[必须][延续] 应安装木马防护软件并定期更新。

（5）[必须][延续] 网站的内容发布应有审核制度和完整的内容发布流程。

（6）[必须][延续] 应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。

（7）[必须][延续] 应建立网站备份系统，备份能力应达到RTO<=60分钟。具备交易功能的网站，RPO<=5分钟。

（8）[必须][延续] 应对网站数据每天进行一次离线备份，并确保离线数据存放介质安全存放。

（9）[必须][延续] 网站系统WEB服务、数据库服务应分别部署在不同服务器上。

（四）网上交易安全
（1）[必须][延续] 应提供可靠的身份认证机制，网上交易客户端支持多种方式与服务端完成身份认证。

（2）[必须][延续] 服务器上的用户认证信息应加密存放。

（3）[必须][延续] 应在与客户签订的服务合同（网上期货服务合同、期货经纪合同及补充协议、风险揭示书）中载明，客户使用网上期货业务可能面临的风险、期货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）。

（4）[必须][延续] 应提供预留验证信息服务，在客户进行登录时向客户进行显示，帮助客户有效识别仿冒的网上期货信息系统，防范利用仿冒的网上期货信息系统进行诈骗活动。

（5）[必须][延续] 应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。

（6）[必须][延续] 应遵守国家关于公民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。未经客户允许和期货公司审批，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。

（7）[必须][延续] 营业场所的客户交易区应安装录像监控设施，监控录像应覆盖所有交易时段

，监控录像资料保存至少6个月。

（五）账户与权限
（1）[必须][延续] 应有生产环境内系统账户与权限的关系表。

（2）[必须][延续] 账户和权限变更应有审批和完整的记录。

（3）[必须][延续] 岗位变动应及时调整对应系统的账户和权限。

（4）[必须][延续] 应避免使用超级管理员账户完成日常业务操作。

（六）口令管理
（1）[必须][延续] 所有书面方式保存的口令应有安全的物理保护措施。

（2）[必须][延续] 口令应有复杂度要求。

（3）[必须][延续] 口令应定期更换。

（4）[必须][延续] 数据库用户口令不得明文存放在计算机中。

（七）安全审计
（1）[必须][延续] 交易系统的主要业务操作应产生审计记录，审计记录保存期限至少为2年。

（2）[必须][延续] 应采取有效措施防止删除、修改或覆盖审计记录。

第五条

日常运行
（一）岗位
（1）[必须][延续] 应建立日常值班制度，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。

（2）[必须][延续] 初始化、结算、数据备份等关键操作过程和结果应有复核。

（3）[必须][延续] 交易运行期间应有现场保障人员，设置运维值班电话，以及时维护和应急处理。

（4）[必须][新增] 网络、主机、数据库、应用系统的运行维护等关键技术岗位应有备岗人员。

（5）[必须][延续] 应实现双人日常值班。

（6）[必须][延续] 应建立文档管理制度，对运维过程中涉及的各类文档进行分类管理。

（二）日常操作与巡检
（1）[必须][延续] 在开盘前、休市、收市等关键时间点应对生产环境运行状态进行巡检。

（2）[必须][延续] 日常操作和巡检应保留记录，并有操作和复核人员的签名。

（3）[必须][延续] 应有生产环境日常操作和定期维护的操作手册，手册中应有详细的操作步骤。

（4）[必须][延续] 交易期间应对核心系统和网络系统状态及网络安全事件进行实时监控、记录，并能及时、有效地报警，相关系统日志至少保留6个月。

（5）[必须][延续] 应保留应用系统的操作日志记录，保存期限至少为2年。

（6）[必须][延续] 应记录生产环境发生的故障和异常。

（7）[必须][延续] 应建立完善和更新重要手册的机制。

（8）[必须][延续] 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。

（9）[必须][延续] 采用自动化运维工具进行日常操作的，应具有有效的机制确保自动化运维工具安全、稳定运行，应具有专门的管理人员，并将自动化运维工具的部署及调整纳入变更管理。

（三）机房进出
（1）[必须][延续] 应建立机房管理制度，对机房环境、供电、空调、消防、安防等基础设施进行运行维护，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。

（2）[必须][延续] 非技术部门人员进入机房应经过审批，并有技术部门人员陪同，所携带设备应专门登记。

（3）[必须][延续] 交易期间如无应急或者巡检需要，不应进入机房。

第六条

备份
（一）数据备份
（1）[必须][延续] 应根据数据的重要性及其对交易系统运行的影响，制定数据备份策略和恢复策略。

（2）[必须][延续] 应建立数据管理、介质维护、销毁和使用管理制度。

（3）[必须][延续] 应对介质进行明确标识。

（4）[必须][延续] 应确保介质存放在安全环境中，实现对备份数据的控制和保护。

（5）[必须][延续] 每日应对结算后数据进行备份，网站数据应按照备份计划进行备份。

（6）[必须][延续] 每周应将结算后数据备份介质进行同城和异地存放。

（7）[必须][延续] 应定期对主要备份业务数据进行恢复验证，根据介质使用期限及时转储数据。

（8）[必须][延续] 应指定专人负责保管业务数据备份介质。

（二）灾难备份
（1）[必须][延续] 应有灾难备份中心，可以接管所有核心业务的运行。

（2）[必须][延续] 灾难备份中心应有满足关键业务功能恢复运作要求的场地和设施。

（3）[必须][延续] 应采取必要手段保证灾难备份中心数据与核心系统保持一致。

（4）[必须][延续] 灾难备份中心应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。

（5）[必须][延续] 灾难备份中心应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。

（6）[必须][延续] 灾难备份中心应在交易和结算时间内有相关技术支持和保障人员。

（7）[必须][延续] 灾难备份中心应有相应的运行维护流程。

（8）[必须][延续] 应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。

（9）[必须][延续] 灾难备份中心的备份能力应达到RTO<=12小时、 RPO<=5分钟。

（10）[必须][延续] 设计灾难备份中心运行时，处理能力应不低于主系统处理能力的50%。

第七条

系统维护
（一）变更管理
（1）[必须][延续] 应将所有涉及核心系统的软硬件变更纳入变更管理范围。

（2）[必须][延续] 每次变更前应进行评估和必要的测试。

（3）[必须][延续] 所有变更操作应有操作记录。

（4）[必须][延续] 所有变更应进行事后检查。

（5）[必须][延续] 对于风险较大的变更，在条件允许的情况下，应制定应急和回退方案。

（6）[必须][延续] 对于风险较大的变更，应在变更后对系统的运行情况进行跟踪。

（7）[必须][延续] 应及时对变更涉及的系统配置和操作手册进行修改。

（8）[可选][新增] 对于风险较大的核心系统变更，在条件允许的情况下，应在上线前进行演练。

（9）[必须][延续] 应建立信息系统软硬件测试管理制度和流程，规范各类系统软硬件上线前的测试。

（10）[可选][新增] 应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。

（11）[必须][延续] 应在独立于生产环境的测试环境中进行技术和业务测试，因业务需要使用生产环境进行测试的，应纳入变更管理流程。

（12）[必须][延续] 应对测试所使用的客户信息进行数据脱敏，因业务需要使用未脱敏数据进行测试的，应采取数据使用授权、操作审计等安全控制措施防止客户信息泄露。

（二）配置管理
（1）[必须][延续] 应具有生产环境设计和部署文档，并根据变更及时更新。

（2）[必须][延续] 应对重要的配置信息进行有效备份。

（3）[必须][新增] 应有配置信息的恢复流程。

（4）[必须][延续] 应建立配置管理制度和配置文档库。

（三）容量管理
（1）[必须][延续] 每年应对核心系统的性能和容量情况进行评估。

（2）[必须][延续] 应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。

（四）应急演练
（1）[必须][延续] 应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及安全风险应有书面的应急预案和排障流程。

（2）[必须][延续] 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。

（3）[必须][延续] 应根据机构、人员、技术等变化，及时调整应急预案。

（4）[必须][延续] 演练前应制定详细的应急演练计划，并根据计划进行演练。

（5）[必须][延续] 应准备必要工具和设备设施，以便应急预案的顺利执行。

（五）技术事故管理
（1）[必须][延续] 应建立技术事故报告制度和流程。

（2）[必须][延续] 应保存技术事故的记录。

（3）[必须][延续] 应根据技术事故情况，及时提出改进计划，落实改进措施。

第八条

分支机构技术要求
（一）基本要求
（1）[必须][延续] 提供现场交易的分支机构设备区域应是一个单独的区域，用于放置开展业务所需的网络、通信和主机设备。

（2）[必须][延续] 提供现场交易的分支机构应确保在交易时间内有技术人员负责技术系统保障。

（3）[必须][延续] 提供现场交易的分支机构应有与当前运行情况相符的业务系统结构文档。

（4）[必须][延续] 提供现场交易的分支机构应配备防火墙或相当的安全防护设备。

（5）[必须][延续] 提供现场交易的分支机构应对交易系统所使用的计算机部署防病毒软件，定期进行全面检查，并及时进行病毒库及操作系统补丁的更新。

（6）[必须][延续] 应建立有效机制，保障总部了解各个分支机构的运行情况。

（7）[必须][延续] 提供现场交易的分支机构应有总部和信息技术服务提供商的准确联系方式。

（二）交易保障
（1）[必须][延续] 提供现场交易的分支机构应有至少两条交易通信链路。

（2）[必须][延续] 提供现场交易的分支机构关键设备应有冗余。

（3）[必须][延续] 提供现场交易的分支机构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。

第四章 三类要求

第一条

技术管理
（一）组织结构
（1）[必须][延续] 应设有技术部门，有专职技术人员，并有明确的职责分工和岗位说明。

（2）[必须][延续] 总部技术部门人员总数占公司总部人数的比例不少于8%。

（3）[必须][新增] 总部技术部门人员不少于11人，对于开展连续交易的期货公司应达到16人。机房托管且由托管方维护机房基础设施的，可核减3人。

（4）[必须][延续] 公司应设立内部审计岗位，定期对IT流程执行情况进行审计。

（5）[必须][延续] 应建立负责本公司信息技术规划和网络安全管理的跨部门机构，其职责包括系统规划、安全管理、IT治理等。

（6）[必须][延续] 应建立信息技术合规与风险管理机制，对信息技术应用全过程的合规风险进行评估、识别、监控和干预，合规风控管理部门应参与上述工作机制，并独立出具意见。

（7）[必须][延续] 应至少每年对公司信息技术应用合规风险情况进行一次全面评估，并妥善保存评估记录，保存期限不低于5年。

（8）[必须][延续] 应与所有总部技术部门人员签署保密协议，并对技术人员的离岗严格管理。

（9）[必须][延续] 应设立2名技术联络员，负责组织、协调和处理与网络安全管理部门、交易所及相关单位的各项技术事宜。

（10）[必须][延续] 总部技术部门应有至少1名安全管理人员。

（11）[必须][延续] 提供现场交易的分支机构应配备至少1名技术人员。

（12）[必须][新增] 总部技术部门应有至少2名网络管理人员。

（二）培训
（1）[必须][延续] 对所有上岗技术人员应进行岗位培训。

（2）[必须][延续] 总部技术部门的所有人员每两年参加期货业协会组织的技术培训应达到15学时。

（3）[必须][延续] 应有明确的培训教材，用于培训上岗操作人员。

（4）[必须][延续] 应有对总部技术部门人员的年度培训计划，并根据计划实施。

（5）[必须][延续] 应定期对技术部门各个岗位的人员进行安全教育和培训，培训内容应包含机房消防及相关应急内容等。

（三）人员素质
（1）[必须][延续] 总部技术部门人员50%以上应有信息技术相关专业大学本科或以上教育背景。

（2）[必须][新增] 总部技术部门人员至少6人应具备2年及以上的系统运行维护经验。

（四）信息技术服务提供商管理
（1）[必须][延续] 应与信息技术服务提供商签订服务保障协议。

（2）[必须][延续] 应与核心系统的服务提供商签署保密协议。

（3）[必须][延续] 应有信息技术服务提供商的准确联系方式。

（4）[必须][延续] 选择信息技术服务提供商时应评估其资质、经营行为、业绩、服务体系、服务品质和违法违规等要素。

（5）[必须][延续] 应至少每年对信息技术服务提供商的服务质量进行一次评估。

（五）IT投入
（1）[必须][延续] 最近三个会计年度IT投入平均数额应不少于最近三个会计年度平均净利润的6%或不少于最近三个会计年度平均营业收入的3%，取二者数额较大者。

第二条

机房建设
（一）基本
（1）[必须][延续] 机房应为独立封闭区域，并配备门禁。

（2）[必须][新增] 机房承重应达到500公斤每平方米。

（3）[必须][延续] 机房应具备火警检测、灭火和应急照明设施。

（4）[必须][延续] 机房应当具备自动灭火设施。

（5）[必须][延续] 机房出入口和内部应安装7×24小时录像监控设施，录像至少保存90天。

（6）[必须][延续] 机房应有防雷接地、防鼠以及防静电的设施。

（7）[必须][延续] 机房内应安装漏水检测设施，并能够自动报警。

（8）[必须][延续] 机房内应采用卤代烷或可替代的其他气体灭火装置。

（9）[必须][延续] 核心系统所在机房应配备机房环境动力监测系统，明确监测指标，实现声音和短信等自动报警。

（二）供电
（1）[必须][延续] 机房应配备在线UPS设施。UPS应当存放在独立封闭区域。

（2）[必须][新增] 应提供双路市电，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。

（3）[必须][新增] 应具有电力设施实时切换演练制度和记录。

（4）[必须][新增] 发电机应能够提供不少于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。

（5）[必须][新增] 应定期对发电机进行开机测试。

（三）空调
（1）[必须][新增] 应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。

（2）[必须][延续] 对机房温湿度应有监控措施和记录。

（3）[必须][新增] 空调应采用双路供电。

（4）[必须][新增] 机房应配备新风设施。

（5）[可选][新增] 应配备为空调供电的发电机。

（四）布线
（1）[必须][延续] 强弱电布线应分开。

（2）[必须][延续] 所有弱电布线应有清晰的线标。

（3）[必须][延续] 强电电缆应有屏蔽或隔离措施。

（4）[必须][延续] 所有布线应置于管道或桥架中。

（五）维护
（1）[必须][延续] 所有UPS和空调设施都应有专业维护人员，或与专业机构签订维护合同。

（2）[必须][延续] 应定期对所有UPS和空调设施进行恰当维护，有维护记录。

第三条

交易系统
（一）功能
（1）[必须][延续] 交易系统应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。

（2）[必须][延续] 交易系统应具备对客户进行实时风险控制的功能。

（3）[必须][延续] 交易系统应产生、记录并存储必要的日志信息供审计使用。日志信息保存期限至少为2年。

（4）[必须][延续] 核心系统应具备向期货市场监控中心上报规定数据的功能。

（5）[必须][延续] 不应具有篡改、伪造交易系统数据或其他可能导致数据失真的功能。

（6）[必须][延续] 交易系统应有授权管理功能。

（7）[必须][延续] 核心系统应有运行监控措施。

（8）[必须][延续] 交易系统应具备流量控制管理功能。

（9）[必须][延续] 应要求核心系统供应商提供交易、银期及相关管理接口。

（10）[必须][延续] 核心系统应具备能够支持逐一录入、文件导入、接口调用方式多渠道开户的功能。

（11）[必须][延续] 核心系统应具备链接期货市场监控中心投资者查询取密钥系统的功能。

（12）[必须][延续] 对于开展互联网开户的期货公司，互联网开户系统应具有落实开户实名制及投资者适当性制度的功能。

（13）[必须][延续] 交易系统应具有并启用客户交易接入认证功能。

（14）[必须][延续] 核心系统应具有并启用客户密码安全管理功能，包括但不限于初始密码修改、弱口令及登录失败次数限制等功能。

（二）性能和容量
（1）[必须][延续] 交易系统的性能和容量应达到所有其作为会员的交易所的要求。

（2）[必须][延续] 应对交易系统的主要业务指标进行实时监控。

（3）[必须][延续] 应对交易系统的主要业务监控指标进行记录。

（4）[必须][延续] 应对所有接入交易所的交易通信链路进行监控。

（4）[必须][延续] 接入交易所的交易通信链路应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。

（5）[必须][延续] 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应不超过80%。

（6）[必须][延续] 应对所有网上交易的通信链路进行监控。

（7）[必须][延续] 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应不超过80%。

（三）系统冗余
（1）[必须][延续] 核心系统及其部件应有热备份，备份能力应达到RTO<=5分钟、RPO<=30秒钟。

（2）[必须][延续] 与交易所连接的网络设备应无单点故障。

（3）[必须][延续] 生产环境内的网络设备应有热备份，备份能力应达到RTO<=5分钟。

（4）[必须][延续] 应使用多个电信运营商的链路作为网上交易的通信链路。

（四）行情冗余
（1）[必须][延续] 应提供至少2套行情服务互为备份。

（五）银期系统冗余
（1）[必须][延续] 应与至少2家银行实现全国性银期转帐。

第四条

安全
（一）网络隔离
（1）[必须][延续] 生产网与互联网应实现有效隔离。

（2）[必须][延续] 网站与网上交易系统应实现有效隔离。

（3）[必须][延续] 生产网与办公网应实现有效隔离。

（4）[必须][延续] 总部的生产网与分支机构的网络应实现有效隔离。

（5）[必须][延续] 生产网与交易所、银行等外部网络及客户使用的网络应实现有效隔离。

（6）[必须][延续] 生产网与开发、测试网络应实现有效隔离。

（二）防病毒、补丁和安全加固
（1）[必须][延续] 应建立有效机制，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。

（2）[必须][延续] 应对使用Windows平台的计算机部署防病毒软件，定期进行全面检查，并及时进行病毒库的更新。

（3）[必须][延续] 应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。

（4）[必须][延续] 应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。

（5）[必须][延续] 应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。

（6）[必须][延续] 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，应先进行病毒检查。

（7）[可选][新增] 对通过互联网传送的交易及结算数据应有加密手段，以保护数据的安全。

（8）[必须][延续] 所有生产环境服务器应尽量避免使用telnet、ftp等有安全隐患的服务，与服务器通信应采用加密方式，例如SSH。

（三）网站安全
（1）[必须][延续] 应有专人监控网站内容，发现问题后及时处理。

（2）[必须][延续] 应至少每年对网站进行一次安全检查，并对隐患进行及时处理。

（3）[必须][延续] 应准备足够措施，能在发现网站被篡改后5分钟内停止发布被篡改的内容。

（4）[必须][延续] 应安装木马防护软件并定期更新。

（5）[必须][延续] 网站的内容发布应有审核制度和完整的内容发布流程。

（6）[必须][新增] 应对网站主页内容实现自动监控，能在5分钟内检测到篡改。

（7）[必须][延续] 应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。

（8）[必须][延续] 应建立网站备份系统，备份能力应达到RTO<=60分钟。具备交易功能的网站，RPO<=5分钟。

（9）[必须][延续] 应对网站数据每天进行一次离线备份，并确保离线数据存放介质安全存放。

（10）[必须][延续] 网站系统WEB服务、数据库服务应分别部署在不同服务器上。

（四）网上交易安全
（1）[必须][延续] 应提供可靠的身份认证机制，网上交易客户端支持多种方式与服务端完成身份认证。

（2）[必须][延续] 服务器上的用户认证信息应加密存放。

（3）[必须][延续] 应在与客户签订的服务合同（网上期货服务合同、期货经纪合同及补充协议、风险揭示书）中载明，客户使用网上期货业务可能面临的风险、期货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）。

（4）[必须][延续] 应提供预留验证信息服务，在客户进行登录时向客户进行显示，帮助客户有效识别仿冒的网上期货信息系统，防范利用仿冒的网上期货信息系统进行诈骗活动。

（5）[可选][新增] 至少提供一种强度较高的用户身份认证机制。

（6）[必须][延续] 应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。

（7）[必须][新增] 核心系统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。

（8）[必须][延续] 应遵守国家关于公民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。未经客户允许和期货公司审批，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。

（9）[必须][延续] 营业场所的客户交易区应安装录像监控设施，监控录像应覆盖所有交易时段，监控录像资料保存至少6个月。

（五）账户与权限
（1）[必须][延续] 应有生产环境内系统账户与权限的关系表。

（2）[必须][延续] 账户和权限变更应有审批和完整的记录。

（3）[必须][延续] 岗位变动应及时调整对应系统的账户和权限。

（4）[必须][延续] 应避免使用超级管理员账户完成日常业务操作。

（六）口令管理
（1）[必须][延续] 所有书面方式保存的口令应有安全的物理保护措施。

（2）[必须][延续] 口令应有复杂度要求。

（3）[必须][延续] 口令应定期更换。

（4）[必须][延续] 数据库用户口令不得明文存放在计算机中。

（七）安全审计
（1）[必须][延续] 交易系统的主要业务操作应产生审计记录，审计记录保存期限至少为2年。

（2）[必须][延续] 应采取有效措施防止删除、修改或覆盖审计记录。

（3）[可选][新增] 所有的主要运维操作应采取恰当的认证措施，并产生审计记录，审计记录保存期限至少为2年。

第五条

日常运行
（一）岗位
（1）[必须][延续] 应建立日常值班制度，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。

（2）[必须][延续] 初始化、结算、数据备份等关键操作过程和结果应有复核。

（3）[必须][延续] 交易运行期间应有现场保障人员，设置运维值班电话，以及时维护和应急处理。

（4）[必须][延续] 网络、主机、数据库、应用系统的运行维护等关键技术岗位应有备岗人员。

（5）[必须][延续] 应实现双人日常值班。

（6）[必须][延续] 应建立文档管理制度，对运维过程中涉及的各类文档进行分类管理。

（二）日常操作与巡检
（1）[必须][延续] 在开盘前、休市、收市等关键时间点应对生产环境运行状态进行巡检。

（2）[必须][延续] 日常操作和巡检应保留记录，并有操作和复核人员的签名。

（3）[必须][延续] 应有生产环境日常操作和定期维护的操作手册，手册中应有详细的操作步骤。

（4）[必须][延续] 交易期间应对核心系统和网络系统状态及网络安全事件进行实时监控、记录，并能及时、有效地报警，相关系统日志至少保留6个月。

（5）[必须][延续] 应保留应用系统的操作日志记录，保存期限至少为2年。

（6）[必须][延续] 应记录生产环境发生的故障和异常。

（7）[必须][新增] 对核心系统和网络系统的实时监控应当包括系统的可用性和系统性能。

（8）[必须][延续] 应建立完善和更新重要手册的机制。

（9）[必须][延续] 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。

（10）[必须][延续] 采用自动化运维工具进行日常操作的，应具有有效的机制确保自动化运维工具安全、稳定运行，应具有专门的管理人员，并将自动化运维工具的部署及调整纳入变更管理。

（三）机房进出
（1）[必须][延续] 应建立机房管理制度，对机房环境、供电、空调、消防、安防等基础设施进行运行维护，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。

（2）[必须][延续] 非技术部门人员进入机房应经过审批，并有技术部门人员陪同，所携带设备应专门登记。

（3）[必须][延续] 交易期间如无应急或者巡检需要，不应进入机房。

第六条

备份
（一）数据备份
（1）[必须][延续] 应根据数据的重要性及其对交易系统运行的影响，制定数据备份策略和恢复

策略。

（2）[必须][延续] 应建立数据管理、介质维护、销毁和使用管理制度。

（3）[必须][延续] 应对介质进行明确标识。

（4）[必须][延续] 应确保介质存放在安全环境中，实现对备份数据的控制和保护。

（5）[必须][延续] 每日应对结算后数据进行备份，网站数据应按照备份计划进行备份。

（6）[必须][延续] 每周应将结算后数据备份介质进行同城和异地存放。

（7）[必须][延续] 应定期对主要备份业务数据进行恢复验证，根据介质使用期限及时转储数据。

（8）[可选][新增] 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。

（9）[必须][新增] 当日备份的交易和结算数据应立即进行恢复验证。

（10）[必须][延续] 应指定专人负责保管业务数据备份介质。

（二）灾难备份
（1）[必须][延续] 应有灾难备份中心，可以接管所有核心业务的运行。

（2）[必须][延续] 灾难备份中心应有满足关键业务功能恢复运作要求的场地和设施。

（3）[必须][延续] 应采取必要手段保证灾难备份中心数据与核心系统保持一致。

（4）[必须][延续] 灾难备份中心应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。

（5）[必须][延续] 灾难备份中心应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。

（6）[必须][延续] 灾难备份中心应在交易和结算时间内有相关技术支持和保障人员。

（7）[必须][延续] 灾难备份中心应有相应的运行维护流程。

（8）[必须][延续] 应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。

（9）[必须][延续] 灾难备份中心的备份能力应达到RTO<=12小时、RPO<=5分钟。

（10）[必须][延续] 设计灾难备份中心运行时，处理能力应不低于主系统处理能力的50%。

第七条

系统维护
（一）变更管理
（1）[必须][延续] 应将所有涉及核心系统的软硬件变更纳入变更管理范围。

（2）[必须][延续] 每次变更前应进行评估和必要的测试。

（3）[必须][延续] 所有变更操作应有操作记录。

（4）[必须][延续] 所有变更应进行事后检查。

（5）[必须][延续] 对于风险较大的变更，在条件允许的情况下，应制定应急和回退方案。

（6）[必须][延续] 对于风险较大的变更，应在变更后对系统的运行情况进行跟踪。

（7）[必须][延续] 应及时对变更涉及的系统配置和操作手册进行修改。

（8）[必须][延续] 对于风险较大的核心系统变更，在条件允许的情况下，应在上线前进行演练。

（9）[必须][新增] 应定期进行风险评估，及时发现风险隐患，并予以处理。

（10）[必须][延续] 应建立信息系统软硬件测试管理制度和流程，规范各类系统软硬件上线前的测试。

（11）[必须][延续] 应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。

（12）[必须][延续] 应在独立于生产环境的测试环境中进行技术和业务测试，因业务需要使用生产环境进行测试的，应纳入变更管理流程。

（13）[必须][延续] 应对测试所使用的客户信息进行数据脱敏，因业务需要使用未脱敏数据进行测试的，应采取数据使用授权、操作审计等安全控制措施防止客户信息泄露。

（二）配置管理
（1）[必须][延续] 应具有生产环境设计和部署文档，并根据变更及时更新。

（2）[必须][延续] 应对重要的配置信息进行有效备份。

（3）[必须][延续] 应有配置信息的恢复流程。

（4）[可选][新增] 应对配置信息的恢复进行演练。

（5）[必须][延续] 应建立配置管理制度和配置文档库。

（6）[必须][新增] 应有专人负责生产环境配置管理。

（三）容量管理
（1）[必须][延续] 每年应对核心系统的性能和容量情况进行评估。

（2）[必须][延续] 应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。

（3）[必须][新增] 应及时执行改进计划，并对执行结果进行跟踪和评估。

（四）应急演练
（1）[必须][延续] 应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及安全风险应有书面的应急预案和排障流程。

（2）[必须][延续] 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。

（3）[必须][延续] 应根据机构、人员、技术等变化，及时调整应急预案。

（4）[必须][延续] 演练前应制定详细的应急演练计划，并根据计划进行演练。

（5）[必须][延续] 应准备必要工具和设备设施，以便应急预案的顺利执行。

（五）技术事故管理
（1）[必须][延续] 应建立技术事故报告制度和流程。

（2）[必须][延续] 应保存技术事故的记录。

（3）[必须][延续] 应根据技术事故情况，及时提出改进计划，落实改进措施。

第八条

分支机构技术要求
（一）基本要求
（1）[必须][延续] 提供现场交易的分支机构设备区域应是一个单独的区域，用于放置开展业务所需的网络、通信和主机设备。

（2）[必须][延续] 提供现场交易的分支机构应确保在交易时间内有技术人员负责技术系统保障。

（3）[必须][延续] 提供现场交易的分支机构应有与当前运行情况相符的业务系统结构文档。

（4）[必须][延续] 提供现场交易的分支机构应配备防火墙或相当的安全防护设备。

（5）[必须][延续] 提供现场交易的分支机构应对交易系统所使用的计算机部署防病毒软件，定期进行全面检查，并及时进行病毒库及操作系统补丁的更新。

（6）[必须][延续] 应建立有效机制，保障总部了解各个分支机构的运行情况。

（7）[必须][延续] 提供现场交易的分支机构应有总部和信息技术服务提供商的准确联系方式。

（二）交易保障
（1）[必须][延续] 提供现场交易的分支机构应有至少两条交易通信链路。

（2）[必须][延续] 提供现场交易的分支机构关键设备应有冗余。

（3）[必须][新增] 提供现场交易的分支机构应对设备容量、交易通信链路进行监控，及时进行必要的升级。

（4）[必须][延续] 提供现场交易的分支机构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。

第五章 四类要求

第一条

技术管理
（一）组织结构
（1）[必须][延续] 应设有技术部门，有专职技术人员，并有明确的职责分工和岗位说明。

（2）[必须][延续] 总部技术部门人员总数占公司总部人数的比例不少于8%。

（3）[必须][新增] 总部技术部门人员不少于15人，对于开展连续交易的期货公司应达到20人。机房托管且由托管方维护机房基础设施的，可核减3人。

（4）[必须][延续] 公司应设立内部审计岗位，定期对IT流程执行情况进行审计。

（5）[必须][延续] 应建立负责本公司信息技术规划和网络安全管理的跨部门机构，其职责包括系统规划、安全管理、IT治理等。

（6）[必须][延续] 应建立信息技术合规与风险管理机制，对信息技术应用全过程的合规风险进行评估、识别、监控和干预，合规风控管理部门应参与上述工作机制，并独立出具意见。

（7）[必须][延续] 应至少每年对公司信息技术应用合规风险情况进行一次全面评估，并妥善保存评估记录，保存期限不低于5年。

（8）[必须][延续] 应与所有总部技术部门人员签署保密协议，并对技术人员的离岗严格管理。

（9）[必须][延续] 应设立2名技术联络员，负责组织、协调和处理与网络安全管理部门、交易所及相关单位的各项技术事宜。

（10）[必须][延续] 总部技术部门应有至少1名安全管理人员。

（11）[必须][延续] 提供现场交易的分支机构应配备至少1名技术人员。

（12）[必须][延续] 总部技术部门应有至少2名网络管理人员。

（二）培训
（1）[必须][延续] 对所有上岗技术人员应进行岗位培训。

（2）[必须][延续] 总部技术部门的所有人员每两年参加期货业协会组织的技术培训应达到15学时。

（3）[必须][延续] 应有明确的培训教材，用于培训上岗操作人员。

（4）[必须][延续] 应有对总部技术部门人员的年度培训计划，并根据计划实施。

（5）[必须][延续] 应定期对技术部门各个岗位的人员进行安全教育和培训，培训内容应包含机房消防及相关应急内容等。

（三）人员素质
（1）[必须][延续] 总部技术部门人员50%以上应有信息技术相关专业大学本科或以上教育背景。

（2）[必须][新增] 总部技术部门人员至少8人应具备2年及以上的系统运行维护经验。

（四）信息技术服务提供商管理
（1）[必须][延续] 应与信息技术服务提供商签订服务保障协议。

（2）[必须][延续] 应与核心系统的服务提供商签署保密协议。

（3）[必须][延续] 应有信息技术服务提供商的准确联系方式。

（4）[必须][延续] 选择信息技术服务提供商时应评估其资质、经营行为、业绩、服务体系、服务品质和违法违规等要素。

（5）[必须][延续] 应至少每年对信息技术服务提供商的服务质量进行一次评估。

（五）IT投入
（1）[必须][延续] 最近三个会计年度IT投入平均数额应不少于最近三个会计年度平均净利润的6%或不少于最近三个会计年度平均营业收入的3%，取二者数额较大者。

第二条

机房建设
（一）基本
（1）[必须][延续] 机房应为独立封闭区域，并配备门禁。

（2）[必须][延续] 机房承重应达到500公斤每平方米。

（3）[必须][延续] 机房应具备火警检测、灭火和应急照明设施。

（4）[必须][延续] 机房应当具备自动灭火设施。

（5）[必须][延续] 机房出入口和内部应安装7×24小时录像监控设施，录像至少保存90天。

（6）[必须][延续] 机房应有防雷接地、防鼠以及防静电的设施。

（7）[必须][延续] 机房内应安装漏水检测设施，并能够自动报警。

（8）[必须][延续] 机房内应采用卤代烷或可替代的其他气体灭火装置。

（9）[必须][延续] 核心系统所在机房应配备机房环境动力监测系统，明确监测指标，实现声音和短信等自动报警。

（二）供电
（1）[必须][延续] 机房应配备在线UPS设施。UPS应当存放在独立封闭区域。

（2）[必须][延续] 应提供双路市电，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。

（3）[必须][延续] 应具有电力设施实时切换演练制度和记录。

（4）[必须][新增] 发电机应能够提供不少于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。

（5）[必须][延续] 应定期对发电机进行开机测试。

（三）空调
（1）[必须][延续] 应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。

（2）[必须][延续] 对机房温湿度应有监控措施和记录。

（3）[必须][延续] 空调应采用双路供电。

（4）[必须][延续] 机房应配备新风设施。

（5）[必须][延续] 应配备为空调供电的发电机。

（四）布线
（1）[必须][延续] 强弱电布线应分开。

（2）[必须][延续] 所有弱电布线应有清晰的线标。

（3）[必须][延续] 强电电缆应有屏蔽或隔离措施。

（4）[必须][延续] 所有布线应置于管道或桥架中。

（五）维护
（1）[必须][延续] 所有UPS和空调设施都应有专业维护人员，或与专业机构签订维护合同。

（2）[必须][延续] 应定期对所有UPS和空调设施进行恰当维护，有维护记录。

第三条

交易系统
（一）功能
（1）[必须][延续] 交易系统应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。

（2）[必须][延续] 交易系统应具备对客户进行实时风险控制的功能。

（3））[必须][延续] 交易系统应产生、记录并存储必要的日志信息供审计使用。日志信息保存期限至少为2年。

（4）[必须][延续] 核心系统应具备向期货市场监控中心上报规定数据的功能。

（5）[必须][延续] 不应具有篡改、伪造交易系统数据或其他可能导致数据失真的功能。

（6）[必须][延续] 交易系统应有授权管理功能。

（7）[必须][延续] 核心系统应有运行监控措施。

（8）[必须][延续] 交易系统应具备流量控制管理功能。

（9）[必须][延续] 应要求核心系统供应商提供交易、银期及相关管理接口。

（10）[必须][延续] 核心系统应具备能够支持逐一录入、文件导入、接口调用方式多渠道开户的功能。

（11）[必须][延续] 核心系统应具备链接期货市场监控中心投资者查询取密钥系统的功能。

（12）[必须][延续] 对于开展互联网开户的期货公司，互联网开户系统应具有落实开户实名制及投资者适当性制度的功能。

（13）[必须][延续] 交易系统应具有并启用客户交易接入认证功能。

（14）[必须][延续] 核心系统应具有并启用客户密码安全管理功能，包括但不限于初始密码修改、弱口令及登录失败次数限制等功能。

（二）性能和容量
（1）[必须][延续] 交易系统的性能和容量应达到所有其作为会员的交易所的要求。

（2）[必须][延续] 应对交易系统的主要业务指标进行实时监控。

（3）[必须][延续] 应对交易系统的主要业务监控指标进行记录。

（4）[必须][延续] 应对所有接入交易所的交易通信链路进行监控。

（5）[必须][延续] 接入交易所的交易通信链路应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。

（6）[必须][延续] 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应不超过80%。

（7）[必须][延续] 应对所有网上交易的通信链路进行监控。

（8）[必须][延续] 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应不超过80%。

（9）[可选][新增] 应正确设置自动化监控工具的预警阀值，并定期进行检查和评估。

（三）系统冗余
（1）[必须][延续] 核心系统及其部件应有热备份，备份能力应达到RTO<=5分钟、RPO<=30秒钟。

（2）[必须][延续] 与交易所连接的网络设备应无单点故障。

（3）[必须][延续] 生产环境内的网络设备应有热备份，备份能力应达到RTO<=5分钟。

（4）[必须][延续] 应使用多个电信运营商的链路作为网上交易的通信链路。

（四）行情冗余
（1）[必须][延续] 应提供至少2套行情服务互为备份。

（五）银期系统冗余
（1）[必须][延续] 应与至少2家银行实现全国性银期转帐。

（2）[必须][新增] 所有银期转账系统应具备抗单点故障的能力。

第四条

安全
（一）网络隔离
（1）[必须][延续] 生产网与互联网应实现有效隔离。

（2）[必须][延续] 网站与网上交易系统应实现有效隔离。

（3）[必须][延续] 生产网与办公网应实现有效隔离。

（4）[必须][延续] 总部的生产网与分支机构的网络应实现有效隔离。

（5）[必须][延续] 生产网与交易所、银行等外部网络及客户使用的网络应实现有效隔离。

（6）[必须][延续] 生产网与开发、测试网络应实现有效隔离。

（7）[必须][新增] 支持核心业务的网络、主机设备应通过独立网络进行管理，实现管理数据流和生产数据流的分离。

（二）防病毒、补丁和安全加固
（1）[必须][延续] 应建立有效机制，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。

（2）[必须][延续] 应对使用Windows平台的计算机部署防病毒软件，定期进行全面检查，并及时进行病毒库的更新。

（3）[必须][延续] 应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。

（4）[必须][延续] 应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。

（5）[必须][延续] 应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。

（6）[必须][延续] 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，应先进行病毒检查。

（7）[必须][延续] 对通过互联网传送的交易及结算数据应有加密手段，以保护数据的安全。

（8）[必须][延续] 所有生产环境服务器应尽量避免使用telnet、ftp等有安全隐患的服务，与服务器通信应采用加密方式，例如SSH。

（9）[必须][新增] 对存有重要生产数据计算机的光盘刻录、USB接口等功能应采取有效的控制手段，防止非授权的数据复制。

（三）网站安全
（1）[必须][延续] 应有专人监控网站内容，发现问题后及时处理。

（2）[必须][延续] 应至少每年对网站进行一次安全检查，并对隐患进行及时处理。

（3）[必须][延续] 应准备足够措施，能在发现网站被篡改后5分钟内停止发布被篡改的内容。

（4）[必须][延续] 应安装木马防护软件并定期更新。

（5）[必须][延续] 网站的内容发布应有审核制度和完整的内容发布流程。

（6）[必须][延续] 应对网站主页内容实现自动监控，能在5分钟内检测到篡改。

（7）[必须][延续] 应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。

（8）[必须][延续] 应建立网站备份系统，备份能力应达到RTO<=60分钟。具备交易功能的网站，RPO<=5分钟。

（9）[必须][延续] 应对网站数据每天进行一次离线备份，并确保离线数据存放介质安全存放。

（10）[必须][延续] 网站系统WEB服务、数据库服务应分别部署在不同服务器上。

（四）网上交易安全
（1）[必须][延续] 应提供可靠的身份认证机制，网上交易客户端支持多种方式与服务端完成身份认证。

（2）[必须][延续] 服务器上的用户认证信息应加密存放。

（3）[必须][延续] 应在与客户签订的服务合同（网上期货服务合同、期货经纪合同及补充协议、风险揭示书）中载明，客户使用网上期货业务可能面临的风险、期货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）。

（4）[必须][延续] 应提供预留验证信息服务，在客户进行登录时向客户进行显示，帮助客户有效识别仿冒的网上期货信息系统，防范利用仿冒的网上期货信息系统进行诈骗活动。

（5）[必须][延续] 至少提供一种强度较高的用户身份认证机制。

（6）[必须][延续] 应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。

（7）[必须][延续] 核心系统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。

（8）[必须][延续] 应遵守国家关于公民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。未经客户允许和期货公司审批，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。

（9）[必须][延续] 营业场所的客户交易区应安装录像监控设施，监控录像应覆盖所有交易时段，监控录像资料保存至少6个月。

（五）账户与权限
（1）[必须][延续] 应有生产环境内系统账户与权限的关系表。

（2）[必须][延续] 账户和权限变更应有审批和完整的记录。

（3）[必须][延续] 岗位变动应及时调整对应系统的账户和权限。

（4）[必须][延续] 应避免使用超级管理员账户完成日常业务操作。

（六）口令管理
（1）[必须][延续] 所有书面方式保存的口令应有安全的物理保护措施。

（2）[必须][延续] 口令应有复杂度要求。

（3）[必须][延续] 口令应定期更换。

（4）[必须][延续] 数据库用户口令不得明文存放在计算机中。

（七）安全审计
（1）[必须][延续] 交易系统的主要业务操作应产生审计记录，审计记录保存期限至少为2年。

（2）[必须][延续] 应采取有效措施防止删除、修改或覆盖审计记录。

（3）[必须][延续] 所有的主要运维操作应采取恰当的认证措施，并产生审计记录，审计记录保存期限至少为2年。

第五条

日常运行
（一）岗位
（1）[必须][延续] 应建立日常值班制度，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。

（2）[必须][延续] 初始化、结算、数据备份等关键操作过程和结果应有复核。

（3）[必须][延续] 交易运行期间应有现场保障人员，设置运维值班电话，以及时维护和应急处理。

（4）[必须][延续] 网络、主机、数据库、应用系统的运行维护等关键技术岗位应有备岗人员。

（5）[必须][延续] 应实现双人日常值班。

（6）[必须][新增] 应实现对机房和网站的24小时连续监控。

（7）[必须][延续] 应建立文档管理制度，对运维过程中涉及的各类文档进行分类管理。

（二）日常操作与巡检
（1）[必须][延续] 在开盘前、休市、收市等关键时间点应对生产环境运行状态进行巡检。

（2）[必须][延续] 日常操作和巡检应保留记录，并有操作和复核人员的签名。

（3）[必须][延续] 应有生产环境日常操作和定期维护的操作手册，手册中应有详细的操作步骤。

（4）[必须][延续] 交易期间应对核心系统和网络系统状态及网络安全事件进行实时监控、记录，并能及时、有效地报警，相关系统日志至少保留6个月。

（5）[必须][延续] 应保留应用系统的操作日志记录，保存期限至少为2年。

（6）[必须][延续] 应记录生产环境发生的故障和异常。

（7）[必须][延续] 对核心系统和网络系统的实时监控应当包括系统的可用性和系统性能。

（8）[必须][延续] 应建立完善和更新重要手册的机制。

（9）[必须][新增] 应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。

（10）[必须][延续] 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。

（11）[必须][延续] 采用自动化运维工具进行日常操作的，应具有有效的机制确保自动化运维工具安全、稳定运行，应具有专门的管理人员，并将自动化运维工具的部署及调整纳入变更管理。

（三）机房进出
（1）[必须][延续] 应建立机房管理制度，对机房环境、供电、空调、消防、安防等基础设施进行运行维护，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。

（2）[必须][延续] 非技术部门人员进入机房应经过审批，并有技术部门人员陪同，所携带设备应专门登记。

（3）[必须][延续] 交易期间如无应急或者巡检需要，不应进入机房。

第六条

备份
（一）数据备份
（1）[必须][延续] 应根据数据的重要性及其对交易系统运行的影响，制定数据备份策略和恢复策略。

（2）[必须][延续] 应建立数据管理、介质维护、销毁和使用管理制度。

（3）[必须][延续] 应对介质进行明确标识。

（4）[必须][延续] 应确保介质存放在安全环境中，实现对备份数据的控制和保护。

（5）[必须][延续] 每日应对结算后数据进行备份，网站数据应按照备份计划进行备份。

（6）[必须][延续] 每周应将结算后数据备份介质进行同城和异地存放。

（7）[必须][延续] 应定期对主要备份业务数据进行恢复验证，根据介质使用期限及时转储数据。

（8）[必须][延续] 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。

（9）[必须][延续] 当日备份的交易和结算数据应立即进行恢复验证。

（10）[必须][延续] 应指定专人负责保管业务数据备份介质。

（二）灾难备份
（1）[必须][新增] 应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。

（2）[必须][延续] 灾难备份中心应有满足关键业务功能恢复运作要求的场地和设施。

（3）[必须][延续] 应采取必要手段保证灾难备份中心数据与核心系统保持一致。

（4）[必须][延续] 灾难备份中心应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。

（5）[必须][延续] 灾难备份中心应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。

（6）[必须][延续] 灾难备份中心应在交易和结算时间内有相关技术支持和保障人员。

（7）[必须][延续] 灾难备份中心应有相应的运行维护流程。

（8）[必须][延续] 应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。

（9）[必须][延续] 灾难备份中心的备份能力应达到RTO<=12小时、RPO<=5分钟。

（10）[必须][延续] 设计灾难备份中心运行时，处理能力应不低于主系统处理能力的50%。

第七条

系统维护
（一）变更管理
（1）[必须][延续] 应将所有涉及核心系统的软硬件变更纳入变更管理范围。

（2）[必须][延续] 每次变更前应进行评估和必要的测试。

（3）[必须][延续] 所有变更操作应有操作记录。

（4）[必须][延续] 所有变更应进行事后检查。

（5）[必须][延续] 对于风险较大的变更，在条件允许的情况下，应制定应急和回退方案。

（6）[必须][延续] 对于风险较大的变更，应在变更后对系统的运行情况进行跟踪。

（7）[必须][延续] 应及时对变更涉及的系统配置和操作手册进行修改。

（8）[必须][延续] 对于风险较大的核心系统变更，在条件允许的情况下，应在上线前进行演练。

（9）[必须][延续] 应定期进行风险评估，及时发现风险隐患，并予以处理。

（10）[必须][延续] 应建立信息系统软硬件测试管理制度和流程，规范各类系统软硬件上线前的测试。

（11） [必须][延续] 应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。

（12）[必须][延续] 应在独立于生产环境的测试环境中进行技术和业务测试，因业务需要使用生产环境进行测试的，应纳入变更管理流程。

（13）[必须][延续] 应对测试所使用的客户信息进行数据脱敏，因业务需要使用未脱敏数据进行测试的，应采取数据使用授权、操作审计等安全控制措施防止客户信息泄露。

（二）配置管理

（1）[必须][延续] 应具有生产环境设计和部署文档，并根据变更及时更新。

（2）[必须][延续] 应对重要的配置信息进行有效备份。

（3）[必须][延续] 应有配置信息的恢复流程。

（4）[必须][延续] 应对配置信息的恢复进行演练。

（5）[必须][延续] 应建立配置管理制度和配置文档库。

（6）[必须][延续] 应有专人负责生产环境配置管理。

（7）[必须][新增] 应定期对核心系统进行配置比对，以及时发现配置的变化。

（三）容量管理

（1）[必须][延续] 每年应对核心系统的性能和容量情况进行评估。

（2）[必须][延续] 应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。

（3）[必须][延续] 应及时执行改进计划，并对执行结果进行跟踪和评估。

（四）应急演练
（1）[必须][延续] 应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及安全风险应有书面的应急预案和排障流程。

（2）[必须][延续] 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。

（3）[必须][延续] 应根据机构、人员、技术等变化，及时调整应急预案。

（4）[必须][延续] 演练前应制定详细的应急演练计划，并根据计划进行演练。

（5）[必须][延续] 应准备必要工具和设备设施，以便应急预案的顺利执行。

（五）技术事故管理
（1）[必须][延续] 应建立技术事故报告制度和流程。

（2）[必须][延续] 应保存技术事故的记录。

（3）[必须][延续] 应根据技术事故情况，及时提出改进计划，落实改进措施。

第八条

分支机构技术要求
（一）基本要求
（1）[必须][延续] 提供现场交易的分支机构设备区域应是一个单独的区域，用于放置开展业务所需的网络、通信和主机设备。

（2）[必须][延续] 提供现场交易的分支机构应确保在交易时间内有技术人员负责技术系统保障。

（3）[必须][延续] 提供现场交易的分支机构应有与当前运行情况相符的业务系统结构文档。

（4）[必须][延续] 提供现场交易的分支机构应配备防火墙或相当的安全防护设备。

（5）[必须][延续] 提供现场交易的分支机构应对交易系统所使用的计算机部署防病毒软件，定期进行全面检查，并及时进行病毒库及操作系统补丁的更新。

（6）[必须][延续] 应建立有效机制，保障总部了解各个分支机构的运行情况。

（7）[必须][延续] 提供现场交易的分支机构应有总部和信息技术服务提供商的准确联系方式。

（二）交易保障

（1）[必须][延续] 提供现场交易的分支机构应有至少两条交易通信链路。

（2）[必须][延续] 提供现场交易的分支机构关键设备应有冗余。

（3）[必须][延续] 提供现场交易的分支机构应对设备容量、交易通信链路进行监控，及时进行必要的升级。

（4）[必须][延续] 提供现场交易的分支机构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。