中国证券监督管理委员会关于印发《进入风险处置程序证券公司信息系统交接技术指引》的通知 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/322/2021_2022__E4_B8_AD_E5_9B_BD_E8_AF_81_E5_c80_322702.htm 中国证券监督管理委员会关于印发《进入风险处置程序证券公司信息系统交接技术指引》的通知各证券公司： 为配合证券公司风险处置工作、防范证券公司信息系统风险，在充分征求行业意见的基础上，我会制定了《进入风险处置程序证券公司信息系统交接技术指引》，现印发给你们，请遵照执行。中国证券监督管理委员会二六年四月二十一日进入风险处置程序证券公司信息系统托管交接工作技术指引目 录 第一章 总则 第二章 管理原则 第三章 组织架构 第一节 组织设置 第二节 职责划分 第四章 托管工作 第一节 准备期 第二节 交接期 第三节 稳定期 第五章 应急预案及应急处理 附件一：管理细则汇总 （一）机房安全管理细则 （二）用户管理细则 （三）权限管理细则 （四）数据安全管理细则 （五）报告办法 （六）病毒防范管理细则 （七）技术文档管理细则 （八）信息技术人员管理细则 （九）软硬件设备管理细则 （十）网络管理细则 （十一）系统安全管理细则 （十二）系统运行维护管理细则 （十三）新系统建设管理细则 附件二：交接工作流程表汇总 准备期 交接期（管理交接） 交接期（技术交接） 附件三：准备期系统摸底表汇总 表1： 信息技术组织架构及人员情况表 表2： 总部信息系统情况表 表3： 企业主干网情况表 表4： 交易系统整体状况表 附件四：交接期交接表汇总 表5： 人员基本情况登记表 表6： 人员基本情况汇总表 表7： 交接日信息系统情况

登记表 表8： 交接日系统备份登记表 表9： 交接前系统超级用户密码登记表 表10： 交接日密码设置修改登记表 表11： 交接日系统用户权限登记表 表12： 交接日员工操作权限登记表 表13： 交接日权限设置修改登记表 表14： 交接日数据备份登记表 表15： 交接日历史数据备份登记表 表16： 交接日系统硬件台账 表17： 交接日系统软件台账 表18： 交接日技术资料登记表 表19： 交接日信息技术合同台账 表20： 交接日相关单位联系方式汇总表 表21： 交接日通讯线路资料表 表22： 交接日系统防病毒检查表 表23： 交接日系统检测登记表 表24： 交接日信息技术工作交接汇总表 附件五：稳定期运维表汇总 表25： 机房人员出入登记表 表26： 机房设备出入登记表 表27： 密码设置修改登记表 表28： 权限设置修改登记表 表29： 每日数据备份登记表 表30： 系统运行维护记录表 表31： 网络改造申请表 表32： 系统硬件台账 表33： 系统软件台账 表34： 技术资料登记表 表35： 信息技术合同台账 表36： 软硬件设备采购申请表 表37： 系统数据维护记录表 表38： 系统防病毒检查表 表39： 系统故障风险登记表 表40： 纠正预防措施实施验证记录表 表41： 信息技术日报表第一章 总则 第一条 为保护证券投资者合法权益，维护国家经济安全和证券市场秩序，妥善处置证券公司风险，根据证券法、公司法、破产法等相关法律，以及证券公司风险处置条例，制定本指引。 第二条 本指引适用于在中华人民共和国境内设立的证券公司，因出现重大风险，或者违法违规经营等情形，由中国证监会指定其他机构对该证券公司进行托管的情况。 第三条 本指引以防范风险为核心，以维护被托管机构信息系统的正常交易、结算系统安全和社会稳定为前提。 第四条 托

管机构应参照本指引制定信息技术托管方案，方案应涵盖被托管机构现有的、与托管工作相关的、影响信息系统安全运行的相关内容。 第五条 信息技术托管按照不同时期的工作特点可分为准备期、交接期、稳定期。 第六条 托管机构在对被托管机构信息系统托管过程中，当地证监局、证监会现场工作组、行政清理工作组（清算组）应当加强对被托管机构信息系统维护和建设的监督、指导和协调工作，有关部门和单位应配合和协作。第二章 管理原则 第七条 防范风险原则：托管期间，各方必须顾全大局，严明纪律，按照统一部署，做好信息系统的风险防范工作。 第八条 责任制原则：托管期间，各项技术与技术管理工作责任必须落实到人。托管与被托管双方实行“ 托管方监督，被托管方执行 ”的一般原则。对重要操作的授权和执行，履行双重签字的程序。 第九条 规范化原则：托管期间，对被托管机构信息技术的管理应采取流程化、规范化的管理模式，各方应严格按照本指引或托管方有关规定执行相应流程，对本指引和托管方未做规定的，沿用被托管机构原有的相关制度执行。 第十条 报告制原则：托管期间，各方应按照有关规定，实行严格的报告制度。 第十一条 保密原则：在托管机构未进场前，应当做好保密工作，未经证监会同意不得公开被托管机构的名称及托管时间；托管期间，各方应保守被托管机构自身及客户的商业秘密。第三章 组织架构第一节 组织设置 第十二条 托管机构应在托管工作组下设托管信息技术组（以下简称技术组）。负责统一管理被托管机构的信息技术工作。 第十三条 技术组应在被托管机构总部、区域中心、各分支营业部及其所属服务部设置现场技术岗位，负责现场的运维、协调和监督工作。 第十四

条 被托管机构的信息技术部门（以下简称被托管技术方）应服从托管机构的要求，做好本职以及托管方要求的各项工作。第二节 职责划分 第十五条 技术组主要职责：1．负责制定信息技术的托管方案，对信息技术托管工作进行总体安排、部署；2．负责对信息技术托管中出现的风险事项进行风险评估、提出应急预案并对发生的风险事项及时研究处理；3．负责对托管范围内的信息技术人员的管理和考核；4．监督托管范围内信息系统资产、文档、合同、数据资料等的管理；5．发现托管范围内的技术和业务异常时，及时上报并完成托管工作组安排的任务；6．配合其他托管工作。 第十六条 现场技术岗位主要职责：1．落实技术组要求的各项工作；2．负责监督被托管机构信息系统的日常运行、管理和维护；3．负责检查被托管机构信息系统数据的完整性和备份数据的安全性；4．负责组织被托管机构信息系统的安全防范和应急演练；5．负责检查应急预案的可行性；6．为被托管机构提供必要的技术支持；7．负责被托管机构信息系统异常的上报和处理工作；8．配合其他的托管工作。 第十七条 被托管技术方主要职责：1．落实技术组要求的各项工作；2．按照技术组的要求做好本职工作，保证交易、清算等信息系统的正常运行；3．妥善保管其占有和管理的所有财产、资料和其他物品；4．配合其他的托管工作。第四章 托管工作第一节 准备期 第十八条 准备期是指证监会宣布被托管机构的处置日前，证监局及托管机构为托管工作做相应准备的时期。 第十九条 托管机构在准备期的主要技术管理责任是组建参与托管的技术队伍，完成相关制度和文档的准备，对技术队伍进行业务、技术和有关托管政策培训；采集相关

技术资料，完成托管技术准备。 第二十条 托管机构在准备期应做好以下技术相关工作： 1．成立技术组：托管机构应成立由信息技术骨干组成的技术组，并明确其工作职责及要求。 2．制定信息系统托管方案：技术组应根据本指引制定信息系统托管方案，对托管工作进行总体安排、部署，包括制定信息技术托管工作管理制度、托管工作流程、交接清单等。 3．获取相关资料：当地证监局加强对辖区高风险证券公司的摸底调查工作，要求以月报或季报形式上报《信息技术组织架构及人员情况表》（表1）、《总部信息系统情况表》（表2）、《企业主干网情况表》（表3）、《交易系统整体情况表》（表4）等相关技术资料，以便托管机构提前作好托管准备；在满足保密要求的前提下，托管机构应与相关信息系统供应商取得联系，获取相关技术资料。 4．组织托管队伍：托管机构应根据拟被托管机构的营业部、服务部数量及信息系统状况，分别设置总部、区域中心、各营业部、服务部现场技术岗位。 5．培训托管人员：托管机构应对现场技术岗位人员进行技术培训和交接培训。技术培训应涵盖交接中将涉及到的主要技术问题，包括各项管理细则、各相关系统的密码和权限的修改、数据备份、参数设置等。交接培训主要包括：交接操作流程、交接要点及异常情况的处理等。 6．准备工具：为了便于顺利开展托管工作，技术组应根据拟被托管机构的设备情况，制定托管工作所需设备清单，如：手提电脑、光盘、移动硬盘、必要的软件、保险柜、托管文档及相关表格等，并作好相应准备。 7．整理主要相关单位的联系方式：技术组应根据拟被托管机构信息系统的情况，整理出《交接日相关单位联系方式汇总表》（表20），表中

应包括主要应用系统的开发商及设备供应商、线路运营商、当地证券业协会、当地证监局、深沪交易所等相关单位的联系方式，以便能及时获得支持。 8. 初步评估风险：技术组应根据了解到的拟被托管机构信息系统的情况，对照中国证监会颁布的《证券公司信息技术管理规范》、深沪交易所相关技术管理规范及托管机构技术管理制度的要求，对被托管机构信息系统进行初步风险评估，形成初步风险评估报告。对较为严重的风险情况，技术组应及时报告托管工作组。 9. 制定初步的应急预案：技术组应针对所了解的被托管机构信息系统的风险，制定初步的应急预案。第二节 交接期 第二十一条 交接期是指证监会宣布被托管机构处置日起，托管机构进入被托管机构进行各项交接工作的时期。 第二十二条 托管机构在准备期的主要技术管理责任是向被托管机构的技术总部、中心机房、备份机房及各营业部派出技术人员，对所有的系统、数据、系统用户、权限密码、技术文档、合同、设备等进行登记，对备份数据、技术文档进行封存，对系统用户权限和密码进行审查，并按照审慎原则对重要的系统密码进行接收。 第二十三条 技术组进入被托管机构后，首先应与被托管技术方进行充分沟通，核实被托管机构信息技术管理、信息系统、信息技术人员等方面的情况，并根据实际情况对准备期所作的方案进行调整后，按照交接工作流程与被托管机构完成相关交接工作。 第二十四条 交接工作包括管理交接和系统交接。系统交接按总部、区域中心及营业部、服务部分别进行。 第二十五条 管理交接包括以下工作： 1. 人员交流：技术组应向被托管技术方介绍交接方案，明确双方职责及托管工作要求。 2. 印章交接：被托管技术方如有部

门印章，应将印章移交给托管机构，并填写相关交接表，由托管机构安排专人实施统一管理。 3．人员情况登记：被托管技术方应如实填写《人员基本情况登记表》（表5）、《人员基本情况汇总表》（表6），表中应包括在处置日前半年内离开的信息技术人员。 4．管理制度交接：技术组应向被托管技术方公布托管工作管理制度，说明托管工作管理制度中未涵盖的内容按被托管机构原制度执行，并要求被托技术方提交原信息技术管理制度。 5．核对系统情况：技术组应与被托管技术方逐一核对信息系统情况，完善《交接日信息系统情况登记表》（表7），以便双方能毫无遗漏地作好各系统交接工作。 第二十六条 系统交接包括以下工作： 1．系统备份：系统备份应包括对各应用系统进行全备份，对操作系统的重要系统目录、配置文件、重要的系统文件进行备份，对网络、安全设备的配置文件进行备份等，应用系统的全备份包括应用软件、数据库、参数配置文件、运行日志等，交接完后应填写《交接日系统备份登记表》（表8）。 2．密码交接：密码交接应包括操作系统、数据库、应用系统、网络安全设备等的超级用户密码，及应用系统后台用户密码的交接，交接完后应填写《交接日密码设置修改登记表》（表10）。在进行密码修改前，应对所有系统的用户权限及参数文件进行备份。在更改用户密码后，应检查应用系统相关配置中使用相应用户用于业务处理的情况，对配置文件中相应用户的密码进行修改，并及时作好相应测试，确保系统能正常运行。 3．用户权限核查：在核查各系统用户及其权限前，应备份用户权限配置文件，并在进行核查操作时详细记录操作过程，核查工作主要包括：A、停用不必要用户，系统运行

一段时间后，确认不必要时删除。B、按最小权限原则进行权限调整。C、用户设置采用专人专户。D、如果存在使用超级用户用于后台处理的情况，建立具有所需权限的用户替代超级用户，并修改相应的配置文件。核查完用户权限后，应填写《交接日系统用户权限登记表》（表11）和《交接日员工操作权限登记表》（表12）。 4．当前数据备份：应备份各系统中至处置日的所有当前数据和历史数据，及交易所当日下发的清算文件、证券余额对账文件等，并逐项填写《交接日数据备份登记表》（表14），备份完成后应检查备份数据的完整性、可读性，并作好备份数据的异地备份。 5．核查历史数据：现场技术岗位应检查被托管机构总部、区域中心信息系统和所有营业部柜台系统自系统建设或开业至今的所有历史数据的备份情况，包括存放位置及备份方式，并对备份数据进行有效性、完整性、连续性检查，填写《交接日历史数据备份登记表》（表15）。（如发现存在原始数据篡改、删除等问题，应该立即上报托管工作组处理） 6．技术资料交接：需交接的资料至少应包括以下各项：系统运行维护日志；应急预案；各系统技术文档；信息系统设备清单；信息系统合同及合同执行情况；各系统运行维护费用支付方式、支付情况；各系统开发商、设备供应商、电信部门、电力部门、物业部门、合作银行等单位的联系方式。交接完成后须分别填写《交接日系统硬件台账》（表16）、《交接日系统软件台账》（表17）、《交接日技术资料登记表》（表18）、《交接日信息技术合同台账》（表19）、《交接日相关单位联系方式汇总表》（表20）、《交接日通讯线路资料表》（表21）。 7．设备清查：应根据被托管方提供的固定资产台

账，由托管双方共同对电子类设备进行清查，清查时应记录设备状况、所用系统及存放地点，完善《交接日系统硬件台账》（表16）、《交接日系统软件台账》（表17）等相关表单。 8. 组织全面查杀病毒及木马：在进行系统交接后，技术组应负责组织被托管机构信息技术人员进行全网病毒查杀，具体流程要求如下：A、升级系统补丁及杀毒软件。B、将局域网与公司主干网断开，对每台机器进行断网病毒查杀后方可恢复网络连接。C、做好杀毒情况汇总、上报工作，并填写《交接日系统防病毒检查表》（表22）。 9. 由专业的信息安全技术人员对被托管机构信息系统进行完整、全面的安全评估，找出潜在技术风险，并提出整改方案，在规定时间内监督被托管方完成。 10. 系统全面联调检测：在进行系统交接及病毒清查、软件升级和安全检查后，为了确保系统正常运行，技术组应组织被托管机构进行所有系统的联网调试，及时解决系统中存在的问题，并填写《交接日系统检测登记表》（表23）。 第二十七条 交接工作中应注意的事项：1. 技术组和现场技术岗位应严格按照交接流程规定的时间和要求，有序逐项开展交接，不得擅自违反。 2. 若无法在规定的时间内完成交接，或无法获得要求的交接内容，现场技术岗位当日应将情况反馈至技术组，由技术组上报至托管工作组。 3. 交接工作完成之后，技术组应负责对交接工作整体情况进行总结，以书面形式向托管工作组汇报。 4. 技术组应根据各类交接清单形成《交接日信息技术工作交接汇总表》（表24），并将各类交接清单作为该表的附件，经托管工作组批准后，一同分别报送当地证监局、托管工作组、被托管公司及营业部留存。 5. 在交接过程中应注意防范风险

，做好数据和软件的备份，确保系统正常运行。 第二十八条 交接中异常情况的处理： 1. 密码修改异常：如果对超级用户（包括等效超级用户）及后台用户进行密码修改后，进行相应测试时，发现系统不能正常运行，且确认为因修改密码引起，在取得系统开发商技术支持后仍不能更改成功，则恢复原密码，同时应填写《系统故障风险登记表》（表39）上报至技术组。 2. 无法获得原有超级用户密码：因相应技术人员已离开被托管机构而无法获得密码，则应上报托管工作组，由托管工作组与被托管机构采取措施，联系相应技术人员。若因被托管机构信息技术人员忘记超级用户密码或无法联系上相应技术人员，则上报托管工作组，经托管工作组同意后，使用解密工具或联系系统开发商及其他技术机构进行密码破解，破解成功后，及时修改密码，同时应填写《系统故障风险登记表》（表39）上报至技术组。 3. 停用用户异常：在停用等效超级用户及认为不必要的用户后，发现系统运行异常，则恢复相应用户，并要求相应用户进行密码修改，同时应填写《系统故障风险登记表》（表39）上报至技术组。若修改密码异常，则参照超级用户密码修改异常处理流程进行处理。 4. 权限修改异常：修改用户权限后，发现系统运行异常，则增加相应所需权限，并填写《系统故障风险登记表》（表39）上报至技术组。 5. 数据备份异常：在使用应用系统的备份功能进行数据备份不成功时，寻求开发维护人员支持，若仍不能成功，则直接进行文件备份或目录备份，并填写《系统故障风险登记表》（表39）上报至技术组。 6. 历史备份数据移交异常：在历史备份数据的移交过程中，如果出现历史备份数据不全、无历史备份数据、因备份介质损

坏无法读取历史备份数据、因资料不全无法读取数据以及其他无法确认历史数据的完整性和有效性的异常情况，须填写《系统故障风险登记表》（表39）上报至技术组。7．数据查询异常：在进行数据查询时，发现数据含义不清且无说明文档，或数据不全，应填写《系统故障风险登记表》（表39）上报至技术组。8．数据上传异常：在营业部将数据上交总部时，如果内部网络不能上传文件，则采用快递方式，同时填写《系统故障风险登记表》（表39）上报至技术组。9．重要资料交接异常：在交接过程中被托管机构如不能按交接要求提供重要相关资料，则应填写《系统故障风险登记表》（表39）上报至技术组。10．清查病毒异常：因查杀病毒引起系统不正常时，联系开发商重装系统，并应填写《系统故障风险登记表》（表39）上报至技术组。第三节 稳定期 第二十九条 稳定期是指托管机构已与被托管机构完成交接工作，双方共同维持信息系统稳定运行的时期。 第三十条 托管机构在稳定期的主要技术管理责任是对系统进行风险检查，消除系统隐患，按照规范要求组织好系统的运行，确保系统稳定运行；同时按照托管工作的进度要求，做好客户保证金第三方存管的系统准备和上线组织。 第三十一条 稳定期在系统运行维护过程中应注意以下事项：1．操作人员必须严格遵守信息应用系统的操作规程，操作用户须专人专用，严禁泄露操作口令，严禁越权操作，操作口令应定期更换，并满足口令强度要求。2．各岗位操作权限应根据岗位职责严格按最小化原则进行设置，并定期进行检查修改。3．交易期间，除经技术组审批不得不进行的故障处理外，严禁任何人以任何理由直接登录数据库进行操作，严禁参数修改。4．尽量启

用系统软件提供的安全审计留痕功能，并记录好运行日志。5．信息系统上线前需进行全面测试，评估上线风险，做好相应的应急和备份计划，并通过规定流程审批获准后才能上线运行，6．完善规范化的日常操作流程，关键操作建立复核机制。7．建立关键系统的配置和变更文档，及时作好参数备份，确保运行环境的可恢复性。8．加强值班管理，作好实时监控。9．开市交易期间，禁止对总部端数据进行大批量的数据查询和统计，防止系统堵塞而影响正常业务。第三十二条 技术组在稳定期应及时对被托管机构的信息系统进行风险评估，形成信息系统整体风险评估报告，向托管工作组报告。第三十三条 信息系统整体风险评估报告应包括对信息系统技术模式、运行状况及技术管理状况的评估。第三十四条 对信息系统技术模式的评估应包括以下几方面：1、网络拓扑结构：重点关注交易网、办公网、互联网之间的隔离情况及安全策略。2、应用系统技术架构：重点关注前后台分离、传输加密、系统漏洞及缺陷等情况。3、系统环境：如周边控制、安全措施等情况。第三十五条 对信息系统运行状况的评估应包括以下几方面：1．对关键设备备份情况进行评估：关键设备备份情况应包括关键服务器、主干路由器、主干交换机、工作站等设备的备份情况；重要通信线路备份及带宽情况；交易所报盘线路“天地”备份情况等。2．对系统设备性能状况进行评估：应根据《信息技术日报表》（表41）、《系统运行维护记录表》（表30）、《系统软件台账》（表33）、《系统硬件台账》（表32），评估被托管机构信息系统主要设备状况及资源使用情况。3．对故障应急处理能力进行评估：应对已有的应急资源、应急能力进行评估，

应急资源包括应急人员、应急设施（备）、装备和物资等，应急能力包括现有人员的技术、经验和接受的培训等。 第三十六条 对技术管理状况进行评估是指根据被托管机构的管理制度、工作流程、技术资料、人员分工及现有系统用户使用情况等，评估被托管信息系统的管理状况。 第三十七条 托管各期的详细工作要求及具体操作步骤请参照《交接工作流程表汇总》（附件二）。 第三十八条 在托管期，为了保证系统的稳定运行，原则上不进行新的系统建设，如有特殊需要，应遵照《新系统建设管理细则》（附件一）进行。 