

中华人民共和国金融行业标准

JR/T 0133—2015

证券期货业信息系统托管基本要求

Basic requirements of information system colocation

for securities and futures industry

2016-01-13 发布

2016-01-13 实施

中国证券监督管理委员会

发布

目 次

前 言	III
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 总体说明	2
4.1 托管系统	2
4.2 托管系统分级	2
4.3 托管服务类型	2
4.4 托管要求	2
5 二级系统受托方要求	3
5.1 机柜租赁 (A2B1)	3
5.2 机房租赁 (A2B2)	4
5.3 基础资源租赁 (A2B3)	5
5.4 整体外包 (A2B4)	7
6 三级系统受托方要求	8
6.1 机柜租赁 (A3B1)	8
6.2 机房租赁 (A3B2)	9
6.3 基础资源租赁 (A3B3)	10
6.4 整体外包 (A3B4)	12
7 三+级系统受托方要求	13
7.1 机柜租赁 (A3+B1)	14
7.2 机房租赁 (A3+B2)	15
7.3 基础资源租赁 (A3+B3)	16
7.4 整体外包 (A3+B4)	18

前 言

本标准依据 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：中国证监会信息中心、中国期货业协会、中国证券业协会、中国证券登记结算有限责任公司北京数据技术分公司、上海证券通信有限责任公司、深圳证券通信有限公司、上海期货信息技术有限公司、大连飞创信息技术有限公司、郑州易盛信息技术有限公司、上海金融期货信息技术有限公司、国泰君安证券股份有限公司、中国银河证券股份有限公司、首创证券有限责任公司、博时基金管理有限公司、华夏基金管理有限公司、中信建投期货有限公司、中证期货有限公司、摩根大通期货有限公司。

本标准主要起草人：张野、罗凯、刘铁斌、汪萌、路一、魏明、刘云清、张超、崔朝、陈铭、陈闽桂、吴宁、祁刚、朱家根、郭建生、郑俊广、胥海涛、颜梦、赵明、杨威、吴捷、姜云安、俞枫、唐沛来、袁维举、王侃侃、石亚晨、刘稚雅、林琦、张晓勇、黄海康、邵剑秋、姜学红、马卫华、魏利明、王曦、刘天羽、侯雪峰。

证券期货业信息系统托管基本要求

1 范围

本标准规定了证券期货业信息系统托管的基本要求。

本标准适用于在监管规定范围内使用托管服务的证券期货机构和为证券期货机构提供托管服务的证券期货市场核心机构及其下属机构。

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。

GB 50174	电子信息系统机房设计规范
GB 50348	安全防范工程技术规范
JR/T 0059	证券期货经营机构信息系统备份能力标准
JR/T 0060	证券期货业信息系统安全等级保护基本要求（试行）
JR/T 0099	证券期货业信息系统运维管理规范
GB/T 24405.1	信息技术 服务管理 第1部分：规范
GB/T 24405.2	信息技术 服务管理 第2部分：实践规则
GB/T 22080	信息技术 安全技术 信息安全管理体系 要求
GB/T 23359	框架式低压机柜
GB/T 22690	数据通信设备通用机械结构 机柜和插箱

3 术语和定义

下列术语和定义适用于本文件。

3.1

托管 colocation

委托其他机构对信息系统进行管理，即租用其他机构提供的物理空间、基础设施、网络通信设施、软硬件设备、运维服务等资源，放置、建立、管理、维护自身信息系统。

3.2

委托方 clients

托管服务的使用者。

3.3

受托方 assignee

托管服务的提供者。

3.4

证券期货机构 securities and futures institutions

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，以及证券公司、基金管理公司、期货公司、证券期货服务机构等证券期货经营机构。

4 总体说明

4.1 托管系统

可进行托管的系统包括证券期货机构承载证券期货交易、结算相关的各类业务系统（包括承载面向客户和对外服务的最基本、最核心交易业务的系统，以及承载除核心交易业务外与交易业务有数据交换的其他业务的系统）和非业务系统。

4.2 托管系统分级

托管系统按照重要性分为二级、三级、三+级共 3 个级别，其中三+为最高级别。

证券期货机构在进行托管时，应当按照机构类别和信息系统信息安全等级保护定级确定托管级别：

- a) 证券期货机构中的经营机构，其按照信息安全等级保护二级要求进行定级的信息系统属于本标准二级，按照信息安全等级保护三级要求进行定级的信息系统属于本标准三级；
- b) 证券期货机构中的市场核心机构，其按照信息安全等级保护二级要求进行定级的信息系统属于本标准三级，按照信息安全等级保护三级要求进行定级的信息系统属于本标准三+级；
- c) 证券期货机构未进行信息安全等级保护定级备案的信息系统参照本标准二级。

4.3 托管服务类型

托管服务类型是指委托方使用受托方提供的托管服务的类型。包括：

a) 机柜租赁

委托方租用受托方提供的机柜空间运行自身信息系统，由受托方负责基础设施及公共通信网络设施的运维工作，由委托方负责自身系统的运维工作；

b) 机房租赁

委托方租用受托方提供的机房空间运行自身信息系统，由受托方负责基础设施及公共通信网络设施的运维工作，由委托方负责自身系统的运维工作；

c) 基础资源租赁

委托方使用受托方提供的服务器设备、网络设备、安全设备、存储设备等基础硬件产品，或者系统软件等基础软件产品，或者虚拟机平台、存储平台等基础平台，由受托方负责所提供产品或平台的运维工作，由委托方负责自身系统的运维工作；

d) 整体外包

委托方使用受托方提供的证券期货应用系统及其运行所需的基础资源，并由受托方承担相关运维工作。

4.4 托管要求

托管要求如下：

- a) 委托方应选择设立在中华人民共和国境内的受托方；
- b) 委托方在进行托管时，应当明确选择要使用的托管服务类型组合；
- c) 委托方应每年按照相应托管要求评估受托方提供的托管服务，并督促受托方进行相应整改，当受托方提供的托管服务严重违反托管要求时，应及时更换受托方；
- d) 委托方应每年将信息系统托管等级及相关材料向中国证监会报备；
- e) 委托方在签订托管服务合同时，应明确违约责任，并约定受托方须接受中国证监会及其派出机构的信息安全延伸检查；
- f) 受托方应根据托管系统级别及委托方选择的托管服务类型提供满足要求的托管服务。托管系统级别、托管服务类型及托管要求的对应关系如表 1 所示；

- g) 开展三级、三+级系统托管业务的受托方，应设立信息安全管理职能部门，在开展托管业务时两年内宜通过 GB/T 24405 和 GB/T 22080 认证。

表1 托管类型及受托方要求对照表

托管类型	二级系统	三级系统	三+级系统
机柜租赁	A2B1	A3B1	A3+B1
机房租赁	A2B2	A3B2	A3+B2
基础资源租赁	A2B3	A3B3	A3+B3
整体外包	A2B4	A3B4	A3+B4

注1：A 代表托管系统级别。其中，A2 代表二级系统，A3 代表三级系统，A3+代表三+级系统。
注2：B 代表托管服务类别。其中，B1 代表机柜租赁，B2 代表机房租赁，B3 代表基础资源租赁，B4 代表整体外包。

5 二级系统受托方要求

5.1 机柜租赁（A2B1）

5.1.1 基础设施要求

基础设施要求如下：

- 机柜所在机房应满足 GB 50174 中 B 级机房要求；
- 机柜的结构尺寸、机电接口、机械性能、外观要求、通风散热等技术指标应满足 GB/T 23359 和 GB/T 22690 的要求；
- 在证券期货交易时段，机柜的电力可用性应达到 99.9%；
- 机柜宜配置两路独立的电源分配模块，并且每个机柜的供电应由独立开关控制；
- 机柜内强弱电线路应以不同标识或颜色区分，应确保线路安置清晰整洁；
- 机柜所在机房区域的温湿度应达到 GB 50174 中 B 级的有关要求；
- 机柜所在机房宜配置环境监控系统，能够对机柜所在机房的支路供电、温度、湿度等关键指标进行自动实时监控和报警；
- 机柜所在区域消防系统应采用高效灭火系统和火灾自动报警系统，并通过当地消防部门验收；
- 受托方应做好机柜所在机房基础设施的日常巡检工作，每日巡检次数不少于三次；
- 受托方应配备 7×24 小时值班基础设施管理员，负责机柜所在机房及机柜基础设施的日常维护、事件应急、故障处置等工作。

5.1.2 网络通信要求

网络通信要求如下：

- 受托方应提供网络线路接入条件，满足委托方交易专网、互联网、数据专线等网络通信需求；

- b) 受托方宜提供至少两家基础通信运营商的线路接入资源,且每家基础通信运营商至少采用两种不同的物理路由接入局端机房;
- c) 机柜网络接入集中网络前应采取有效的安全防护措施,实现机柜网络环境与其它区域网络环境的有效隔离;
- d) 受托方应 7×24 小时对机房公共网络运行情况进行实时监控,受托方未经委托方授权,禁止监听、获取、复制、利用通过网络传输的信息系统数据信息;
- e) 受托方应配备 7×24 小时网络支持人员,负责其提供的机柜公共网络的日常维护、事件应急、故障处置等工作。

5.1.3 安全保卫要求

安全保卫要求如下:

- a) 受托方应为机柜提供电子锁或机械锁。受托方可留有备用钥匙以备应急使用,但应提前获得委托方同意,并记录使用情况;
- b) 受托方应对机柜所在机房设置视频监控设备,监控范围覆盖机柜操作面、机柜所在机房出入口等关键区域。连续视频监控记录应保存至少 90 天;
- c) 受托方宜在机柜所在建筑物入口处安装出入控制和安全防护装置,包括闸机、防爆桶、X 射线安全检查设备等,并对出入人员和所带物品应进行安全检查;
- d) 受托方应对机柜所在区域出入人员身份执行审批审核流程,并记录出入人员信息、进出时间、工作内容等,相关记录应保存至少 360 天;
- e) 受托方应配备 7×24 小时值班保安人员,负责机柜所在机房的安全保卫工作。

5.1.4 运维保障要求

运维保障要求如下:

- a) 受托方应制定并完善对机柜的运维管理相关制度,包括对机柜所在机房、机柜本身、网络通信、安全保卫等运维操作流程、操作手册、故障处理、应急预案、应急联络人联络方式等,并提供给委托方;
- b) 受托方应为委托方提供信息系统运维和监控的场地条件,根据委托方要求,提供公共监控工位,满足委托方运维和监控需要;
- c) 受托方应向委托方告知值班基础设施管理员、网络管理员、保安人员的职责,并公布值班电话。
- d) 受托方在进行重大变更时,应提前至少 10 个工作日通过书面方式通知可能受到影响的委托方。
- e) 受托方应为委托方提供 7×24 小时支持服务,应在 15 分钟内响应委托方提出的服务请求。遇到突发事件,应积极配合委托方共同开展应急处置工作;
- f) 受托方应至少每年一次向委托方提供服务报告,包括监控及巡检、日常维护、应急处理工作等。
- g) 受托方宜做好基础设施演练的年度计划,并按计划予以实施。

5.2 机房租赁 (A2B2)

5.2.1 基础设施要求

基础设施要求如下:

- a) 机房应满足 GB 50174 中 B 级机房要求;
- b) 机房应有独立的双路电源配电柜,在证券期货交易时段,机房的电力可用性应达到 99.9%;
- c) 机房区域的温湿度应达到 GB 50174 中 B 级的有关要求;
- d) 机房宜具备集成的环境监控系统、设备监控系统,对环境、供电、空调、给水排水、消防等重要系统进行自动实时监控和报警;

- e) 机房消防系统应采用高效灭火系统和火灾自动报警系统，并通过当地消防部门验收；
- f) 受托方应做好对机房的基础设施日常巡检工作，每日巡检次数不少于三次；
- g) 受托方应配备 7×24 小时值班基础设施管理员，负责机房的日常维护、事件应急、故障处置等工作。

5.2.2 网络通信要求

网络通信要求如下：

- a) 受托方应提供网络线路接入条件，满足委托方交易专网、互联网、数据专线等网络通信需求；
- b) 受托方宜提供至少两家基础通信运营商的线路接入资源，且每家基础通信运营商至少采用两种不同的物理路由接入局端机房；
- c) 受托方应 7×24 小时对机房公共网络运行情况进行实时监控，受托方未经委托方授权，禁止监听、获取、复制、利用通过网络传输的信息系统数据信息；
- d) 受托方应配备 7×24 小时网络支持人员，负责其提供的机房公共网络的日常维护、事件应急、故障处置等工作。

5.2.3 安全保卫要求

安全保卫要求如下：

- a) 受托方应为机房划定单独区域，并进行物理隔离且设有电子门锁；
- b) 受托方应对机房设置视频监控设备，监控范围覆盖机房区域出入口。连续视频监控记录应保存至少 90 天；
- c) 机房所在建筑物宜设置周界区域，建筑物群体周界宜设置围墙，宜安装入侵报警系统、安全防护系统、防车辆撞击设施等。各安全防范子系统应满足 GB 50348 规定的集成式安全防范系统设计要求和各子系统的设计要求；
- d) 受托方宜在机房所在建筑物入口处安装出入控制和安全防护装置，包括闸机、防爆桶、X 射线安全检查设备等，并对出入人员和所带物品应进行安全检查；
- e) 受托方应对机房所在区域出入人员身份执行审批审核流程，并记录出入人员信息、进出时间、工作内容等，相关记录应保存至少 360 天；
- f) 受托方应配备 7×24 小时值班保安人员，负责机房的安全保卫工作。

5.2.4 运维保障要求

运维保障要求如下：

- a) 受托方应制定并完善对机房的运维管理相关制度，包括对机房基础设施、网络通信、安全保卫等运维操作流程、操作手册、故障处理、应急预案、应急联络人联络方式等，并提供给委托方；
- b) 受托方应为委托方提供信息系统运维和监控的场地条件，至少提供公共监控工位，满足委托方运维和监控需要；
- c) 受托方应向委托方告知值班基础设施管理员、网络管理员、保安人员的职责，并公布值班电话；
- d) 受托方在进行重大变更时，应提前至少 10 个工作日通过书面方式通知可能受到影响的委托方；
- e) 受托方应为委托方提供 7×24 小时支持服务，应在 15 分钟内响应委托方提出的服务请求。遇到突发事件，应积极配合委托方共同开展应急处置工作；
- f) 受托方应至少每年一次向委托方提供服务报告，包括监控及巡检、日常维护、应急处理工作等；
- g) 受托方宜做好基础设施演练的年度计划，并按计划予以实施。

5.3 基础资源租赁（A2B3）

5.3.1 基础设施要求

受托方应满足同级机柜租赁中的5.1.1基础设施要求或机房租赁中的5.2.1基础设施要求。

5.3.2 网络通信要求

受托方应满足同级机柜租赁中的5.1.2网络通信要求或机房租赁中的5.2.2网络通信要求。

5.3.3 安全保卫要求

受托方应满足同级机柜租赁中的5.1.3安全保卫要求或机房租赁中的5.2.3安全保卫要求。

5.3.4 基础资源租赁产品要求

5.3.4.1 基础硬件产品

基础硬件产品要求如下：

- a) 受托方提供的服务器设备、网络设备、安全设备、存储设备等基础硬件产品应为冗余架构，性能和可用性应满足委托方需求；
- b) 受托方应按照流程为提供的服务器设备、网络设备、安全设备、存储设备等基础硬件产品进行设备信息登记（供货日期，保修日期，序列号，厂家信息等）。

5.3.4.2 基础软件产品

基础软件产品要求如下：

- a) 受托方应提供合法正版的系统软件等基础软件产品，并及时更新软件许可；
- b) 受托方应负责对提供的系统软件等基础软件产品的安装、测试、升级和故障处理。

5.3.4.3 基础平台

基础平台要求如下：

- a) 受托方应为虚拟机平台、存储平台等基础平台，提供安装、调试、培训、运行、升级等维护服务；
- b) 受托方应保证委托方数据在虚拟机平台、存储平台等基础平台上的安全、可靠传输，并保留数据传输日志记录，时间不得少于一年；
- c) 受托方应做好虚拟机平台、存储平台等基础平台的数据备份工作；
- d) 受托方应做好虚拟机平台、存储平台等基础平台的容量管理工作。

5.3.5 运维保障要求

运维保障要求如下：

- a) 受托方应制定并完善对基础资源的运维管理相关制度，包括对基础资源所在机房基础设施、网络通信、安全保卫、基础资源等运维操作流程、操作手册、故障处理、应急预案、应急联络人联络方式等，并提供给委托方；
- b) 受托方应为委托方提供信息系统运维和监控条件，满足委托方运维和监控需要；
- c) 受托方应提供专业监控工具对基础资源租赁产品进行监控；
- d) 受托方应定期对基础资源租赁产品进行巡检，并记录巡检结果；
- e) 受托方应向委托方告知值班基础设施管理员、网络管理员、保安人员、平台运维人员的职责，并确定明确的排班表；

- f) 受托方在进行可能涉及基础资源的变更时，应提前至少 10 个工作日通过书面方式通知可能受到影响的委托方；
- g) 基础资源发生故障时，受托方应按事件处理流程，积极配合委托方共同开展应急处置工作；
- h) 受托方应采取有效措施限制单个委托方对基础资源的使用限度；
- i) 受托方在进行双方合同中约定的关键操作时，应按合同约定的程序执行审批手续，确保双人复核，并进行留痕，相关记录应保存至少一年；
- j) 受托方应采取身份识别控制和权限管理，杜绝非授权和越权访问、更改委托方的数据；
- k) 受托方应持续跟踪厂商提供的系统升级更新情况，检查基础资源系统的补丁是否得到了及时更新；
- l) 受托方应部署防病毒产品和支持防恶意代码软件的统一管理，并定期检查恶意代码库的版本更新情况；
- m) 受托方应采取入侵防范措施，及时检测并阻断对平台系统的入侵行为；
- n) 受托方应为委托方提供 7×24 小时支持服务，应在 15 分钟内响应委托方提出的服务请求。遇到突发事件，应积极配合委托方共同开展应急处置工作；
- o) 受托方应至少每年一次向委托方提供基础资源服务报告；
- p) 受托方应做好数据保密工作，未经授权不得使用、分析、复制委托方数据，不得向第三方透露数据内容；
- q) 双方终止合同，受托方应协助委托方收回所有数据，并保证系统中全部相关数据被删除，并不可恢复。

5.4 整体外包（A2B4）

5.4.1 基础设施要求

受托方应满足同级基础资源租赁中的5.3.1基础设施要求。

5.4.2 网络通信要求

受托方应满足同级基础资源租赁中的5.3.2网络通信要求。

5.4.3 安全保卫要求

受托方应满足同级基础资源租赁中的5.3.3安全保卫要求。

5.4.4 基础资源租赁产品要求

受托方应满足同级基础资源租赁中的5.3.4基础资源租赁产品要求。

5.4.5 应用系统要求

应用系统要求如下：

- a) 受托方应向委托方提供应用系统的交付文档，包括但不限于系统架构、功能说明和用户手册等；
- b) 受托方提供的应用系统应稳定可靠，确保业务的正常运行；
- c) 受托方提供的应用系统的性能和容量应满足委托方的要求；
- d) 受托方提供的应用系统应具备身份识别和权限控制功能；
- e) 受托方提供的应用系统在数据传输、备份、存储等过程中，应具备加密功能；
- f) 受托方提供的应用系统应具备日志记录功能，满足委托方的安全审计要求。

5.4.6 运维保障要求

运维保障要求如下：

- a) 受托方应满足同级基础资源租赁中的 5.3.5 运维保障要求；
- b) 受托方对受托应用系统的运维工作，应当按照 JR/T 0099 的各项要求开展；
- c) 受托方应配合委托方进行应用系统必要的业务测试；
- d) 受托方在进行可能影响应用系统的变更时，应提前至少 10 个工作日通过书面方式通知可能受到影响的委托方；
- e) 受托方在进行双方合同中约定的应用系统关键数据操作时，应按合同约定的程序执行审批手续，确保双人复核，并进行留痕，相关记录应保存至少一年；
- f) 受托方应至少每年对应用系统进行检查，并形成相关检查记录和评估报告；
- g) 受托方应根据委托方要求，为委托方提供 7×24 小时应用系统客户支持服务，应在 15 分钟内响应委托方提出的服务请求。遇到突发事件，应积极配合委托方共同开展应急处置工作；
- h) 受托方应至少每年一次向委托方提供应用系统服务报告；
- i) 受托方应做好应用系统数据保密工作，未经授权不得使用、分析、复制委托方数据，不得向第三方透露数据内容；
- j) 双方终止合同，受托方应协助委托方收回所有数据，并保证应用系统中全部相关数据被删除，并不可恢复。

6 三级系统受托方要求

6.1 机柜租赁（A3B1）

6.1.1 基础设施要求

基础设施要求如下：

- a) 机柜所在机房应满足 GB 50174 中 A 级机房要求；
- b) 机柜的结构尺寸、机电接口、机械性能、外观要求、通风散热等技术指标应满足 GB/T 23359 和 GB/T 22690 的要求；
- c) 在证券期货交易时段，机柜的电力可用性应达到 99.99%；
- d) 机柜应配置两路独立的电源分配模块，并且每个机柜的供电应由独立开关控制；
- e) 机柜内强弱电线路应以不同标识或颜色区分，应确保线路安置清晰整洁；
- f) 机柜所在机房精密空调至少采用 N+1 方式冗余，机柜所在机房区域的温湿度应达到 GB 50174 中 A 级的有关要求；
- g) 机柜所在机房应配置环境监控系统，能够对机柜所在机房的支路供电、温度、湿度等关键指标进行自动实时监控和报警；
- h) 机柜所在区域消防系统应采用高效灭火系统和火灾自动报警系统，并通过当地消防部门验收；
- i) 受托方应做好机柜所在机房基础设施的日常巡检工作，每日巡检次数不少于六次；
- j) 受托方应配备 7×24 小时值班基础设施管理员，负责机柜所在机房及机柜基础设施的日常维护、事件应急、故障处置等工作。

6.1.2 网络通信要求

网络通信要求如下：

- a) 受托方应提供网络线路接入条件，满足委托方交易专网、互联网、数据专线等网络通信需求；
- b) 受托方应提供至少两家基础通信运营商的线路接入资源，且每家基础通信运营商至少采用两种不同的物理路由接入局端机房；

- c) 机柜网络接入集中网络前应采取有效的安全防护措施,实现机柜网络环境与其它区域网络环境的有效隔离;
- d) 受托方应 7×24 小时对机房公共网络运行情况进行实时监控,受托方未经委托方授权,禁止监听、获取、复制、利用通过网络传输的信息系统数据信息;
- e) 受托方应配备 7×24 小时网络支持人员,负责其提供的机柜公共网络的日常维护、事件应急、故障处置等工作。

6.1.3 安全保卫要求

安全保卫要求如下:

- a) 受托方应为机柜提供电子锁或机械锁。受托方可留有备用钥匙以备应急使用,但应提前获得委托方同意,并记录使用情况;
- b) 受托方应对机柜所在机房设置视频监控设备,监控范围覆盖机柜操作面、机柜所在机房出入口等关键区域。连续视频监控记录应保存至少 90 天;
- c) 受托方应在机柜所在建筑物入口处安装出入控制和安全防护装置,包括闸机、防爆桶、X 射线安全检查设备等,并对出入人员和所带物品应进行安全检查;
- d) 受托方应对机柜所在区域出入人员身份执行审批审核流程,并记录出入人员信息、进出时间、工作内容等,相关记录应保存至少 360 天;
- e) 受托方应配备 7×24 小时值班保安人员,负责机柜所在机房的安全保卫工作。

6.1.4 运维保障要求

运维保障要求如下:

- a) 受托方应制定并完善对机柜的运维管理相关制度,包括对机柜所在机房、机柜本身、网络通信、安全保卫等运维操作流程、操作手册、故障处理、应急预案、应急联络人联络方式等,并提供给委托方;
- b) 受托方应为委托方提供信息系统运维和监控的场地条件,根据委托方要求,提供专用监控工位或监控室,满足委托方运维和监控需要;
- c) 受托方应向委托方告知值班基础设施管理员、网络管理员、保安人员的职责,并公布值班电话;
- d) 受托方在进行重大变更时,应提前至少 20 个工作日通过书面方式通知可能受到影响的委托方;
- e) 受托方应为委托方提供 7×24 小时支持服务,应在 10 分钟内响应委托方提出的服务请求。遇到突发事件,应积极配合委托方共同开展应急处置工作;
- f) 受托方应至少每半年一次向委托方提供服务报告,包括监控及巡检、日常维护、应急处理工作等;
- g) 受托方应做好基础设施演练的年度计划,并按计划予以实施。

6.2 机房租赁 (A3B2)

6.2.1 基础设施要求

基础设施要求如下:

- a) 机房应满足 GB 50174 中 A 级机房要求;
- b) 机房应有独立的双路电源配电柜,在证券期货交易时段,机房的电力可用性应达到 99.99%;
- c) 机房精密空调至少采用 N+1 方式冗余,机房区域的温湿度应达到 GB 50174 中 A 级的有关要求;
- d) 机房应具备集成的环境监控系统、设备监控系统,对环境、供电、空调、给水排水、消防等重要系统进行自动实时监控和报警;

- e) 机房消防系统应采用高效灭火系统和火灾自动报警系统，并通过当地消防部门验收；
- f) 受托方应做好对机房的基础设施日常巡检工作，每日巡检次数不少于六次；
- g) 受托方应配备7×24小时值班基础设施管理员，负责机房的日常维护、事件应急、故障处置等工作。

6.2.2 网络通信要求

网络通信要求如下：

- a) 受托方应提供网络线路接入条件，满足委托方交易专网、互联网、数据专线等网络通信需求；
- b) 受托方应提供至少两家基础通信运营商的线路接入资源，且每家基础通信运营商至少采用两种不同的物理路由接入局端机房；
- c) 受托方应7×24小时对机房公共网络运行情况进行实时监控，受托方未经委托方授权，禁止监听、获取、复制、利用通过网络传输的信息系统数据信息；
- d) 受托方应配备7×24小时网络支持人员，负责其提供的机房公共网络的日常维护、事件应急、故障处置等工作。

6.2.3 安全保卫要求

安全保卫要求如下：

- a) 受托方应为机房划定单独区域，并进行物理隔离且设有电子门锁；
- b) 受托方应对机房设置视频监控设备，监控范围覆盖机房区域出入口，连续视频监控记录应保存至少90天；
- c) 机房所在建筑物应设置周界区域，建筑物群体周界应设置围墙，应安装入侵报警系统、安全防护系统、防车辆撞击设施等。各安全防范子系统应满足GB 50348规定的集成式安全防范系统设计要求和各子系统的设计要求；
- d) 受托方应在机房所在建筑物入口处安装出入控制和安全防护装置，包括闸机、防爆桶、X射线安全检查设备等，并对出入人员和所带物品应进行安全检查；
- e) 受托方应对机房所在区域出入人员身份执行审批审核流程，并记录出入人员信息、进出时间、工作内容等，相关记录应保存至少360天；
- f) 受托方应配备7×24小时值班保安人员，负责机房的安全保卫工作。

6.2.4 运维保障要求

运维保障要求如下：

- a) 受托方应制定并完善对机房的运维管理相关制度，包括对机房基础设施、网络通信、安全保卫等运维操作流程、操作手册、故障处理、应急预案、应急联络人联络方式等，并提供给委托方；
- b) 受托方应为委托方提供信息系统运维和监控的场地条件，至少提供专用的监控工位或专用监控室，满足委托方运维和监控需要；
- c) 受托方应向委托方告知值班基础设施管理员、网络管理员、保安人员的职责，并公布值班电话；
- d) 受托方在进行重大变更时，应提前至少20个工作日通过书面方式通知可能受到影响的委托方；
- e) 受托方应为委托方提供7×24小时支持服务，应在10分钟内响应委托方提出的服务请求。遇到突发事件，应积极配合委托方共同开展应急处置工作；
- f) 受托方应至少每半年一次向委托方提供服务报告，包括监控及巡检、日常维护、应急处理工作等；
- g) 受托方应做好基础设施演练的年度计划，并按计划予以实施。

6.3 基础资源租赁（A3B3）

6.3.1 基础设施要求

受托方应满足同级机柜租赁中的6.1.1基础设施要求或机房租赁中的6.2.1基础设施要求。

6.3.2 网络通信要求

网络通信要求如下：

- a) 受托方应满足同级机柜租赁中的6.1.2网络通信要求或机房租赁中的6.2.2网络通信要求；
- b) 受托方应为委托方提供冗余通道，访问委托方租赁的基础资源。

6.3.3 安全保卫要求

受托方应满足同级机柜租赁中的6.1.3安全保卫要求或机房租赁中的6.2.3安全保卫要求。

6.3.4 基础资源租赁产品要求

6.3.4.1 基础硬件产品

基础硬件产品要求如下：

- a) 受托方提供的服务器设备、网络设备、安全设备、存储设备等基础硬件产品应为冗余架构，性能和可用性应满足委托方需求；
- b) 受托方应提供独立的区域，部署服务器设备、网络设备、安全设备、存储设备等基础硬件产品；
- c) 受托方应按照流程为提供的服务器设备、网络设备、安全设备、存储设备等基础硬件产品进行设备信息登记（供货日期，保修日期，序列号，厂家信息等）；

6.3.4.2 基础软件产品

基础软件产品要求如下：

- a) 受托方应提供合法正版的系统软件等基础软件产品，并及时更新软件许可；
- b) 受托方应提供系统软件等基础软件产品的升级手册和升级包，且在提供升级补丁前，配合委托方进行可用性和风险评估；
- c) 受托方应负责对提供的系统软件等基础软件产品的安装、测试、升级和故障处理；
- d) 受托方应提供针对系统软件等基础软件产品的培训。

6.3.4.3 基础平台

基础平台要求如下：

- a) 受托方提供的虚拟机平台、存储平台等基础平台的可用性应不低于99.9%；
- b) 受托方应为虚拟机平台、存储平台等基础平台，提供安装、调试、培训、运行、升级等维护服务；
- c) 受托方应为虚拟机平台、存储平台等基础平台建立灾备系统，并制定应急方案。委托方应配合受托方进行切换演练；
- d) 受托方应保证委托方数据在虚拟机平台、存储平台等基础平台上的安全、可靠传输，并保留数据传输日志记录，时间不得少于一年；
- e) 受托方应做好虚拟机平台、存储平台等基础平台的数据备份工作；
- f) 受托方应做好虚拟机平台、存储平台等基础平台的容量管理工作，并定期提供容量监控报告；
- g) 受托方应采取有效的安全隔离措施，防止基础平台内不同客户间的风险传导。

6.3.5 运维保障要求

运维保障要求如下：

- a) 受托方应制定并完善对基础资源的运维管理相关制度，包括对基础资源所在机房基础设施、网络通信、安全保卫、基础资源等运维操作流程、操作手册、故障处理、应急预案、应急联络人联络方式等，并提供给委托方；
- b) 受托方应为委托方提供信息系统运维和监控条件，满足委托方运维和监控需要；
- c) 受托方应提供专业监控工具对基础资源租赁产品进行监控，并定期提供监控报告；
- d) 受托方应定期对基础资源租赁产品进行巡检，并记录巡检结果；
- e) 受托方应向委托方告知值班基础设施管理员、网络管理员、保安人员、平台运维人员的职责，并确定明确的排班表；
- f) 受托方在进行可能涉及基础资源的变更时，应提前至少 20 个工作日通过书面方式通知可能受到影响的委托方；
- g) 基础资源发生故障时，受托方应按事件处理流程，积极配合委托方共同开展应急处置工作；
- h) 受托方应采取有效措施限制单个委托方对基础资源的使用限度；
- i) 受托方在进行双方合同中约定的关键操作时，应按合同规定的程序执行审批手续，确保双人复核，并进行留痕，相关记录应保存至少一年；
- j) 受托方应采取身份识别控制和权限管理，杜绝非授权和越权访问、更改委托方的数据；
- k) 受托方应持续跟踪厂商提供的系统升级更新情况，检查基础资源系统的补丁是否得到了及时更新；
- l) 受托方应部署防病毒产品和支持防恶意代码软件的统一管理，并定期检查恶意代码库的版本更新情况；
- m) 受托方应采取入侵防范措施，及时检测并阻断对平台系统的入侵行为。应能够检测到对重要服务器进行入侵的行为，能够记录入侵的源 IP、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警；
- n) 受托方应为委托方提供 7×24 小时支持服务，应在 10 分钟内响应委托方提出的服务请求，并在 60 分钟内到场服务。遇到突发事件，应积极配合委托方共同开展应急处置工作；
- o) 受托方应至少每半年一次向委托方提供基础资源服务报告，包括监控及巡检、日常维护、应急处理工作等；
- p) 受托方宜至少每年组织一次基础资源的应急切换演练，并向委托方提供应急演练预案、应急演练报告；
- q) 受托方应做好数据保密工作，未经授权不得使用、分析、复制委托方数据，不得向第三方透露数据内容；
- r) 双方终止合同，受托方应协助委托方收回所有数据，并保证系统中全部相关数据被删除，并不可恢复。

6.4 整体外包（A3B4）

6.4.1 基础设施要求

受托方应满足同级基础资源租赁中的6.3.1基础设施要求。

6.4.2 网络通信要求

受托方应满足同级基础资源租赁中的6.3.2网络通信要求。

6.4.3 安全保卫要求

受托方应满足同级基础资源租赁中的6.3.3安全保卫要求。

6.4.4 基础资源租赁产品要求

受托方应满足同级基础资源租赁中的6.3.4基础资源租赁产品要求。

6.4.5 应用系统要求

应用系统要求如下：

- a) 受托方应向委托方提供应用系统的交付文档,包括但不限于系统架构、功能说明和用户手册等;
- b) 受托方提供的应用系统应稳定可靠,确保业务的正常运行;
- c) 受托方提供的应用系统的性能和容量应满足委托方的要求;
- d) 受托方提供的应用系统的设计和部署应满足 JR/T 0099 的要求;
- e) 受托方提供的应用系统应为委托方提供监控工具或者接口,满足委托方的监控需要;
- f) 受托方提供的应用系统应具备身份识别和权限控制功能;
- g) 受托方提供的应用系统在数据传输、备份、存储等过程中,应具备加密功能;
- h) 受托方提供的应用系统应具备日志记录功能,满足委托方的安全审计要求;
- i) 受托方提供的应用系统应满足委托方对于信息系统隔离的要求。

6.4.6 运维保障要求

运维保障要求如下：

- a) 受托方应满足同级基础资源租赁中的 6.3.5 运维保障要求;
- b) 受托方对受托应用系统的运维工作,应当按照 JR/T 0099 的各项要求开展;
- c) 受托方应配合委托方进行应用系统必要的业务测试;
- d) 受托方应向委托方告知值班基础设施管理员、网络管理员、保安人员、平台运维人员、应用系统人员的职责,并确定明确的排班表;
- e) 受托方在进行可能影响应用系统的变更时,应提前至少 20 个工作日通过书面方式通知可能受到影响的委托方;
- f) 受托方在进行双方合同中约定的应用系统关键数据操作时,应按合同规定的程序执行审批手续,确保双人复核,并进行留痕,相关记录应保存至少一年;
- g) 受托方应至少每半年对应用系统进行检查,包括应用系统可用性、参数配置、系统性能容量、权限设置、系统版本等,并形成相关检查记录和评估报告;
- h) 受托方应为委托方提供 7×24 小时应用系统客户支持服务,应在 10 分钟内响应委托方提出的服务请求,并在 60 分钟内到场服务。遇到突发事件,应积极配合委托方共同开展应急处置工作;
- i) 受托方应至少每半年一次向委托方提供应用系统服务报告,包括监控及巡检、日常维护、应急处理工作等;
- j) 受托方应提供应用系统的应急预案,当故障发生时,能恢复原来的工作状态。组织用户至少每年进行一次故障应急演练;
- k) 受托方应做好应用系统数据保密工作,未经授权不得使用、分析、复制委托方数据,不得向第三方透露数据内容;
- l) 双方终止合同,受托方应协助委托方收回所有数据,并保证应用系统中全部相关数据被删除,并不可恢复。

7 三+级系统受托方要求

7.1 机柜租赁（A3+B1）

7.1.1 基础设施要求

基础设施要求如下：

- a) 机柜所在机房应满足 GB 50174 中 A 级机房要求；
- b) 机柜的结构尺寸、机电接口、机械性能、外观要求、通风散热等技术指标应满足 GB/T 23359 和 GB/T 22690 的要求；
- c) 在证券期货交易时段，机柜的电力可用性应达到 99.99%；
- d) 机柜应配置两路独立的电源分配模块，并且每个机柜的供电应由独立开关控制；
- e) 机柜内强弱电线路应以不同标识或颜色区分，应确保线路安置清晰整洁；
- f) 机柜所在机房精密空调至少采用 N+1 方式冗余，机柜所在机房区域的温湿度应达到 GB 50174 中 A 级的有关要求；
- g) 机柜所在机房应配置环境监控系统，能够对机柜所在机房的支路供电、温度、湿度等关键指标进行自动实时监控和报警；
- h) 机柜所在区域消防系统应采用高效灭火系统和火灾自动报警系统，并通过当地消防部门验收；
- i) 受托方应做好机柜所在机房基础设施的日常巡检工作，每日巡检次数不少于六次；
- j) 受托方应配备 7×24 小时值班基础设施管理员，负责机柜所在机房及机柜基础设施的日常维护、事件应急、故障处置等工作。

7.1.2 网络通信要求

网络通信要求如下：

- a) 受托方应提供网络线路接入条件，满足委托方交易专网、互联网、数据专线等网络通信需求；
- b) 受托方应提供至少两家基础通信运营商的线路接入资源，且每家基础通信运营商至少采用两种不同的物理路由接入局端机房；
- c) 机柜网络接入集中网络前应采取有效的安全防护措施，实现机柜网络环境与其它区域网络环境的有效隔离；
- d) 受托方应 7×24 小时对机房公共网络运行情况进行实时监控，受托方未经委托方授权，禁止监听、获取、复制、利用通过网络传输的信息系统数据信息；
- e) 受托方应配备 7×24 小时网络支持人员，负责其提供的机柜公共网络的日常维护、事件应急、故障处置等工作；

7.1.3 安全保卫要求

安全保卫要求如下：

- a) 受托方应为机柜提供电子锁或机械锁。受托方可留有备用钥匙以备应急使用，但应提前获得委托方同意，并记录使用情况；
- b) 受托方应对机柜所在机房设置视频监控设备，监控范围覆盖机柜操作面、机柜所在机房出入口等关键区域。连续视频监控记录应保存至少 90 天；
- c) 受托方应在机柜所在建筑物入口处安装出入控制和安全防护装置，包括闸机、防爆桶、X 射线安全检查设备等，并对出入人员和所带物品应进行安全检查；
- d) 受托方应对机柜所在区域出入人员身份执行审批审核流程，并记录出入人员信息、进出时间、工作内容等，相关记录应保存至少 360 天；
- e) 受托方应配备 7×24 小时值班保安人员，负责机柜所在机房的安全保卫工作。

7.1.4 运维保障要求

运维保障要求如下：

- a) 受托方应制定并完善对机柜的运维管理相关制度，包括对机柜所在机房、机柜本身、网络通信、安全保卫等运维操作流程、操作手册、故障处理、应急预案、应急联络人联络方式等，并提供给委托方；
- b) 受托方应为委托方提供信息系统运维和监控的场地条件，根据委托方要求，提供专用监控工位或监控室，满足委托方运维和监控需要；
- c) 受托方应向委托方告知值班基础设施管理员、网络管理员、保安人员的职责，并公布值班电话；
- d) 受托方在进行重大变更时，应提前至少 30 个工作日通过书面方式通知可能受到影响的委托方；
- e) 受托方应为委托方提供 7×24 小时支持服务，应在 5 分钟内响应委托方提出的服务请求。遇到突发事件，应积极配合委托方共同开展应急处置工作；
- f) 受托方应至少每半年一次向委托方提供服务报告，包括监控及巡检、日常维护、应急处理工作等；
- g) 受托方应做好基础设施演练的年度计划，并按计划予以实施。

7.2 机房租赁（A3+B2）

7.2.1 基础设施要求

基础设施要求如下：

- a) 机房应满足 GB 50174 中 A 级机房要求；
- b) 机房应有独立的双路电源配电柜，在证券期货交易时段，机房的电力可用性应达到 99.99%；
- c) 机房精密空调至少采用 N+1 方式冗余，机房区域的温湿度应达到 GB 50174 中 A 级的有关要求；
- d) 机房应具备集成的环境监控系统、设备监控系统，对环境、供电、空调、给水排水、消防等重要系统进行自动实时监控和报警；
- e) 机房消防系统应采用高效灭火系统和火灾自动报警系统，并通过当地消防部门验收；
- f) 受托方应做好对机房的基础设施日常巡检工作，每日巡检次数不少于六次；
- g) 受托方应配备 7×24 小时值班基础设施管理员，负责机房的日常维护、事件应急、故障处置等工作。

7.2.2 网络通信要求

网络通信要求如下：

- a) 受托方应提供网络线路接入条件，满足委托方交易专网、互联网、数据专线等网络通信需求；
- b) 受托方应提供至少两家基础通信运营商的线路接入资源，且每家基础通信运营商至少采用两种不同的物理路由接入局端机房；
- c) 受托方应 7×24 小时对机房公共网络运行情况进行实时监控，受托方未经委托方授权，禁止监听、获取、复制、利用通过网络传输的信息系统数据信息；
- d) 受托方应配备 7×24 小时网络支持人员，负责其提供的机房公共网络的日常维护、事件应急、故障处置等工作。

7.2.3 安全保卫要求

安全保卫要求如下：

- a) 受托方应为机房划定单独区域，并进行物理隔离且设有电子门锁；
- b) 受托方应对机房设置视频监控设备，监控范围覆盖机房区域出入口。连续视频监控记录应保存至少 90 天；

- c) 机房所在建筑物应设置周界区域，建筑物群体周界应设置围墙，应安装入侵报警系统、安全防护系统、防车辆撞击设施等。各安全防范子系统应满足 GB 50348 规定的集成式安全防范系统设计要求和各子系统的设计要求；
- d) 受托方应在机房所在建筑物入口处安装出入控制和安全防护装置，包括闸机、防爆桶、X 射线安全检查设备等，并对出入人员和所带物品应进行安全检查；
- e) 受托方应对机房所在区域出入人员身份执行审批审核流程，并记录出入人员信息、进出时间、工作内容等，相关记录应保存至少 360 天；
- f) 受托方应配备 7×24 小时值班保安人员，负责机房的安全保卫工作。

7.2.4 运维保障要求

运维保障要求如下：

- a) 受托方应制定并完善对机房的运维管理相关制度，包括对机房基础设施、网络通信、安全保卫等运维操作流程、操作手册、故障处理、应急预案、应急联络人联络方式等，并提供给委托方；
- b) 受托方应为委托方提供信息系统运维和监控的场地条件，至少提供专用的监控工位或专用监控室，满足委托方运维和监控需要；
- c) 受托方应向委托方告知值班基础设施管理员、网络管理员、保安人员的职责，并公布值班电话；
- d) 受托方在进行重大变更时，应提前至少 30 个工作日通过书面方式通知可能受到影响的委托方；
- e) 受托方应为委托方提供 7×24 小时支持服务，应在 5 分钟内响应委托方提出的服务请求。遇到突发事件，应积极配合委托方共同开展应急处置工作；
- f) 受托方应至少每半年一次向委托方提供服务报告，包括监控及巡检、日常维护、应急处理工作等；
- g) 受托方应做好基础设施演练的年度计划，并按计划予以实施。

7.3 基础资源租赁（A3+B3）

7.3.1 基础设施要求

受托方应满足同级机柜租赁中的 7.1.1 基础设施要求或机房租赁中的 7.2.1 基础设施要求。

7.3.2 网络通信要求

网络通信要求如下：

- a) 受托方应满足同级机柜租赁中的 7.1.2 网络通信要求或机房租赁中的 7.2.2 网络通信要求；
- b) 受托方应为委托方提供冗余通道，访问委托方租赁的基础资源。

7.3.3 安全保卫要求

受托方应满足同级机柜租赁中的 7.1.3 安全保卫要求或机房租赁中的 7.2.3 安全保卫要求。

7.3.4 基础资源租赁产品要求

7.3.4.1 基础硬件产品

基础硬件产品要求如下：

- a) 受托方提供的服务器设备、网络设备、安全设备、存储设备等基础硬件产品应为冗余架构，性能和可用性应满足委托方需求；
- b) 受托方应提供独立的区域，部署服务器设备、网络设备、安全设备、存储设备等基础硬件产品；

- c) 受托方应为提供的服务器设备、网络设备、安全设备、存储设备等基础硬件产品提供备机、备件服务，或原厂维保服务；
- d) 受托方应按照流程为提供的服务器设备、网络设备、安全设备、存储设备等基础硬件产品进行设备信息登记（供货日期，保修日期，序列号，厂家信息等）。

7.3.4.2 基础软件产品

基础软件产品要求如下：

- a) 受托方应提供合法正版的系统软件等基础软件产品，并及时更新软件许可；
- b) 受托方应提供系统软件等基础软件产品的升级手册和升级包，且在提供升级补丁前，配合委托方进行可用性和风险评估；
- c) 受托方应负责对提供的系统软件等基础软件产品的安装、测试、升级和故障处理；
- d) 受托方应提供针对系统软件等基础软件产品的培训。

7.3.4.3 基础平台

基础平台要求如下：

- a) 受托方提供的虚拟机平台、存储平台等基础平台的可用性应不低于 99.95%；
- b) 受托方应为虚拟机平台、存储平台等基础平台，提供安装、调试、培训、运行、升级等维护服务；
- c) 受托方应为虚拟机平台、存储平台等基础平台建立灾备系统，并制定应急方案。委托方应配合受托方进行切换演练；
- d) 受托方应保证委托方数据在虚拟机平台、存储平台等基础平台上的安全、可靠传输，并保留数据传输日志记录，时间不得少于一年；
- e) 受托方应做好虚拟机平台、存储平台等基础平台的数据备份工作；
- f) 受托方应做好虚拟机平台、存储平台等基础平台的容量管理工作，设定报警阈值，并定期提供容量监控报告；
- g) 受托方应采取有效的安全隔离措施，防止基础平台内不同客户间的风险传导。

7.3.5 运维保障要求

运维保障要求如下：

- a) 受托方应制定并完善对基础资源的运维管理相关制度，包括对基础资源所在机房基础设施、网络通信、安全保卫、基础资源等运维操作流程、操作手册、故障处理、应急预案、应急联络人联络方式等，并提供给委托方；
- b) 受托方应为委托方提供信息系统运维和监控条件，满足委托方运维和监控需要；
- c) 受托方应提供专业监控工具对基础资源租赁产品进行监控，并定期提供监控报告；
- d) 受托方应定期对基础资源租赁产品进行巡检，并记录巡检结果；
- e) 受托方应向委托方告知值班基础设施管理员、网络管理员、保安人员、平台运维人员的职责，并确定明确的排班表；
- f) 受托方在进行可能涉及基础资源的变更时，应提前至少 30 个工作日通过书面方式通知可能受到影响的委托方；
- g) 基础资源发生故障时，受托方应按事件处理流程，积极配合委托方共同开展应急处置工作；
- h) 受托方应采取有效措施限制单个委托方对基础资源的使用限度；
- i) 受托方在进行双方合同中约定的关键操作时，应按合同规定的程序执行审批手续，确保双人复核，并进行留痕，相关记录应保存至少一年；

- j) 受托方应采取身份识别控制和权限管理，杜绝非授权和越权访问、更改委托方的数据；
- k) 受托方应持续跟踪厂商提供的系统升级更新情况，检查基础资源系统的补丁是否得到了及时更新；
- l) 受托方应部署防病毒产品和支持防恶意代码软件的统一管理，并定期检查恶意代码库的版本更新情况；
- m) 受托方应采取入侵防范措施，及时检测并阻断对平台系统的入侵行为。应能够检测到对重要服务器进行入侵的行为，能够记录入侵的源 IP、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警；
- n) 受托方应为委托方提供 7×24 小时支持服务，应在 5 分钟内响应委托方提出的服务请求，并在 30 分钟内到场服务。遇到突发事件，应积极配合委托方共同开展应急处置工作；
- o) 受托方应至少每半年一次向委托方提供基础资源服务报告，包括监控及巡检、日常维护、应急处理工作等；
- p) 受托方宜至少每年组织一次基础资源的应急切换演练，并向委托方提供应急演练预案、应急演练报告；
- q) 受托方应做好数据保密工作，未经授权不得使用、分析、复制委托方数据，不得向第三方透露数据内容；
- r) 双方终止合同，受托方应协助委托方收回所有数据，并保证系统中全部相关数据被删除，并不可恢复。

7.4 整体外包（A3+B4）

7.4.1 基础设施要求

受托方应满足同级基础资源租赁中的7.3.1基础设施要求。

7.4.2 网络通信要求

受托方应满足同级基础资源租赁中的7.3.2网络通信要求。

7.4.3 安全保卫要求

受托方应满足同级基础资源租赁中的7.3.3安全保卫要求。

7.4.4 基础资源租赁产品要求

受托方应满足同级基础资源租赁中的7.3.4基础资源租赁产品要求。

7.4.5 应用系统要求

应用系统要求如下：

- a) 受托方应向委托方提供应用系统的交付文档，包括但不限于系统架构、功能说明和用户手册等；
- b) 受托方提供的应用系统应稳定可靠，确保业务的正常运行；
- c) 受托方提供的应用系统的性能和容量应满足委托方的要求；
- d) 受托方提供的应用系统的设计和部署应满足 JR/T 0059 的要求；
- e) 受托方提供的应用系统应为委托方提供监控工具或者接口，满足委托方的监控需要；
- f) 受托方提供的应用系统应具备身份识别和权限控制功能；
- g) 受托方提供的应用系统在数据传输、备份、存储等过程中，应具备加密功能；
- h) 受托方提供的应用系统应具备日志记录功能，满足委托方的安全审计要求；
- i) 受托方提供的应用系统应满足委托方对于信息系统隔离的要求；

7.4.6 运维保障要求

运维保障要求如下：

- a) 受托方应满足同级基础资源租赁中的 7.3.5 运维保障要求；
 - b) 受托方对受托应用系统的运维工作，应当按照 JR/T 0099 的各项要求开展；
 - c) 受托方应配合委托方进行应用系统必要的业务测试；
 - d) 受托方应向委托方告知值班基础设施管理员、网络管理员、保安人员、平台运维人员、应用系统人员的职责，并确定明确的排班表；
 - e) 受托方在进行可能影响应用系统的变更时，应提前至少 30 个工作日通过书面方式通知可能受到影响的委托方；
 - f) 受托方在进行双方合同中约定的应用系统关键数据操作时，应按合同规定的程序执行审批手续，确保双人复核，并进行留痕，相关记录应保存至少两年；
 - g) 受托方应至少每季度对应用系统进行检查，包括应用系统可用性、参数配置、系统性能容量、权限设置、系统版本等，并形成相关检查记录和评估报告；
 - h) 受托方应为委托方提供 7×24 小时应用系统客户支持服务，应在 5 分钟内响应委托方提出的服务请求，并在 30 分钟内到场服务。遇到突发事件，应积极配合委托方共同开展应急处置工作；
 - i) 受托方应至少每季度一次向委托方提供应用系统服务报告，包括监控及巡检、日常维护、应急处理工作等；
 - j) 受托方应提供应用系统的应急预案，当故障发生时，能恢复原来的工作状态。组织用户至少每年进行一次故障应急演练；
 - k) 受托方应做好应用系统数据保密工作，未经授权不得使用、分析、复制委托方数据，不得向第三方透露数据内容；
 - l) 双方终止合同，受托方应协助委托方收回所有数据，并保证应用系统中全部相关数据被删除，并不可恢复。
-