

电子政务外网云资源扩容服务项目评价指标体系

一级指标	分值	二级指标	分值	三级指标	分值 (100)	评价标准
机构制度建设	20	机构制度建设执行情况	20	管理制度健全性	5	评价承接主体保障项目或服务的相关制度是否全面、完整、合理，是否符合相关法律、法规规定，用以反映和评价承接主体管理制度的合法合规情况及对服务项目顺利实施的保障情况。评价要点： 1. 承接主体是否制定相关管理制度；[0, 1.5] 2. 承接主体是否及时更新相关项目管理制度。[0, 1.5] 3. 承接主体制定的制度是否与大数据中心相关管理制度契合。[0, 2]
				制度执行有效性	5	运维服务过程是否符合相关管理规定，用以反映和评价相关管理制度的有效执行情况。 1. 运维服务过程是否按照甲方要求执行以及是否遵守自身相关制度规定；[0, 0.5] 2. 是否对运维服务过程进行完整记录，包括事件管理过程、问题管理过程、变更管理过程等；[0, 0.5] 3. 服务过程中事故事件处置方案是否有效，根据解决情况判定有效性；[0, 0.5] 4. 运维服务的人员条件、介质管理、机房安全、账号口令、资源管理、运维终端管理、网络安全管理等是否落实到位；[0, 1] 5. 服务过程管控措施是否落实到位，是否出现违规行为。[0, 1] 6. 员工对制度的了解程度，了解员工对制度内容的熟悉程度，包括他们对规则和流程的理解。[0, 0.5] 7. 是否进行制度符合性评估。[0, 1]
				人员安排合理性	5	1. 承接主体是否依据招标文件要求、云计算服务安全评估办法和当前组织架构，建立岗位结构，明确管理岗、技术岗、操作岗等岗位，对运行维护服务中的不同岗位进行明确分工和职责定义；[0, 1] 2. 承接主体是否按照合同要求配备必要的项目人员；[0, 1] 3. 承接主体是否对配备的项目人员进行定期评价；[0, 1] 4. 项目人员是否属于具备相应资质的专业技术

					人员；[0,1] 5. 变更项目人员是否征得购买主体同意；[0, 0.5] 6. 对于值班人员是否制定了严格的值班制度以及交接班制度。[0, 0.5]
				档案管理完整性	5 主要评价承接主体档案管理是否有效完整，是否按照服务项目档案管理的要求执行。 1. 是否对购买主体要求的材料按时提交；[0, 1.5] 2. 在服务过程中形成的材料是否保存完整、及时归档。建立项目档案，记录相关文件、工作计划方案、项目进展、工作汇报总结、重大活动和其它有关资料信息。用以反映和评价承接主体管理制度执行的有效程度。[0, 3.5]
服务满意度	5	服务对象满意度	5	购买主体满意度	2.5 评价购买主体对相关工作的认可情况。包括购买主体对服务方案的满意度、购买主体对服务能力的满意度、定期向购买主体汇报工作开展情况、对运维服务的满意程度等。[0, 2.5] A 档：如计为 100%、B 档：如计为 75%、C 档：如计为 50%、D 档：如计为 0%。 n 题满意度得分 = (A 档占比 × 100%) + (B 档占比 × 75%) + (C 档占比 × 50%) + (D 档占比 × 0%)。 总体满意度 = (n 题满意度% + n+1 题满意度% + n+2 题满意度% + + n+m 题满意度%) ÷ n+m ≈ xx. xx%。 最终满意度得分 = 总体满意度 * 2.5 分
				用户厅局满意度	2.5 评价用户厅局对相关工作的认可情况。包括对服务方案的满意度、对服务能力的满意度、对运维服务的满意程度等。[0, 2.5] A 档：如计为 100%、B 档：如计为 75%、C 档：如计为 50%、D 档：如计为 0%。 n 题满意度得分 = (A 档占比 × 100%) + (B 档占比 × 75%) + (C 档占比 × 50%) + (D 档占比 × 0%)。 总体满意度 = (n 题满意度% + n+1 题满意度% + n+2 题满意度% + + n+m 题满意度%) ÷ n+m ≈ xx. xx%。 最终满意度得分 = 总体满意度 * 2.5 分
综合绩效	2	项目考勤情况	2	项目驻场人员考	2 主要评价承接主体项目驻场人员考勤情况，数据来源为每月承接主体驻场人员迟到的次数和早退的打卡次数，以打卡记录时间为准，扣分 = (n 月迟到或早退打卡次数 / n 月总计应打卡次数 * 2 分) + (n+1 月迟到或早退打卡次数 / n+1 月总计应打卡次数 * 2 分) +。 注：打卡次数为承接主体所有驻场人员合计值。

				勤情况		[0, 2]
服务情况	7 3	服务数量	1 5	基础设施服务完成情况	3	评价承接主体基础设施服务的完成情况，主要包括： 1. 云服务器提供 vCPU、内存是否达到要求，是否可实现快速灵活、弹性伸缩的计算资源服务。[0, 1] 2. 云存储提供普通块存储是否达到要求，具备数据冗余和缓存加速能力。[0, 1] 3. 云备份提供本地数据备份是否达到要求，具备云主机、主流数据库、文件系统等备份和恢复服务；支持增量备份技术，支持分权管理功能。[0, 1]
				安全保障服务完成情况	2	评价承接主体安全保障服务的完成情况，主要包括： 1. 云安全按照网络安全三级保护要求，提供安全资源池组件，云资源使用部门可根据实际需求灵活选择一种或多种组件，至少提供以下单个组件能力：日志审计，堡垒机，漏洞扫描，防火墙/IPS，WAF/网页防篡改，数据库审计，网络审计，主机安全。以上其中之一。[0, 1] 2. 云监控运维管理是否包含集中告警、统一监控、运维可视化、操作运维中心等功能，是否提供计算、存储、网络资源的实时监控、报表等功能服务。[0, 1]
				链路连接服务完成情况	2	评价承接主体链路连接服务完成情况，主要包括： 1. 政务云需包括政务外网业务区和互联网业务区，两个区域通过网闸隔离，承接主体提供的网闸设备是否满足政务云高效率应用和访问需求；[0, 1] 2. 承接主体是否提供 16 条 10GE 链路，并保障传输链路质量指标符合要求，若对接设备的两端需要使用长距离光模块，则现网政务云侧设备的长距离光模块由乙方提供。[0, 1]
				政务云全过程运营	2	评价承接主体是否提供政务云全过程运营和运维： 是否协助厅局委办制定合理的业务上云实施方案，分配和配置云服务资源，业务上云全过程技术支持、等保测评、密码测评、数字认证、安全服务等技术支持，7×24 小时值班运维等。须按照政务云服务要求建立标准化、规范化的运维管理服务制度和服务流程，严格按照制度和流程要

				及运维完成情况		求提供各项政务云服务，并按照时效性要求对服务事项的各环节进行闭环管理。（未完成一项服务扣 1 分，最高扣 2 分）[0, 2]
				日常运维服务完成情况	2	评价承接主体日常运维工作完成情况。主要包括： 1. 日常巡检: 包含设备、网络巡检，并提供机柜视频监控、门禁、动环监控、消防、代收货等服务；[0, 0.8] 2. 服务热线: 提供 7*24 小时的服务。服务内容为服务受理、故障受理、应急响应、服务请求、询问、事件、变更服务；[0, 0.8] 3. 日常运维: 按照自治区政务云服务要求执行。[0, 0.4]
				重大事件保障服务完成情况	2	评价承接主体在重大节假日、关键事件期间或当购买主体对网络进行重大操作时应其要求提供现场值守支持保障服务的完成情况。（缺少一次重保服务扣 1 分，最高扣 2 分）[0, 2]
				应急演练完成情况	2	评价承接主体是否制定应急演练计划和方案，是否定期开展应急演练，是否形成应急演练总结报告，确保政务云安全稳定运行。（缺少一次应急演练服务扣 1 分，最高扣 2 分）[0, 2]

		服务质量	37	提供服务质量达标情况	4	评价承接主体提供的云计算平台、机房物理的质量是否达标： 1. 云计算平台必须通过网络安全等级保护三级测评（测评结论为良或基本符合及以上），测评完成后提供网络安全等级保护备案证明和测评报告；云计算平台必须提供满足租户应用系统通过网络安全等保三级测评的安全组件和安全服务能力，租户可根据实际需求从云服务清单中选用租户安全组件，配合租户完成应用系统三级等保测评工作；须为政务云上部署的全部业务提供虚拟机级别数据备份服务；[0, 2] 2. 承接主体提供的机房物理环境和云计算平台必须通过商用密码应用安全性评估，评估完成后提供商用密码应用安全性评估报告。[0, 2]
				安全管理质量达标情况	7	评价承接主体安全管理是否达标。 1. 承接主体是否按照政务云要求合理配置和管理相关基础设施，支撑政务云运行的设备应具备冗余能力，不得因设备故障或性能不足影响政务云安全、稳定、正常运行。乙方负责协调调度设备厂商做好技术保障服务，定期组织专业人员对机房设备资产、配套设施、备品备件及维护耗材进行检查，发现问题和隐患及时申报、及时整改并出具整改分析报告；[0, 2] 2. 承接主体是否按照等级保护要求，根据云上业务系统需求提供安全资源组件服务，协助完成安全资源组件部署、测试，并对云上业务系统应用安全策略进行评估，提供安全指导、培训服务，提供安全资源组件使用故障诊断和排查等运维服务，对安全资源池进行日常巡检、管理监测和有效利用率分析评估，保证安全资源池稳定运行；[0, 2] 3. 根据国家互联网信息办公室、国家发展和改革委员会、工业和信息化部、财政部发布的《云计算服务安全评估办法》的要求提供云服务，有效保障政务云安全和供应链安全；[0, 1] 4. 承接主体提供的所有云服务资源是否按甲方的要求进行拆分，分别部署在政务外网区和互联网区两个区域，每个区域所需的资源量由甲方指定，在各厅局委办业务上云时按需灵活使用各区域的资源。若使用已达到预估资源数量，可以根据甲方的要求快速扩容政务云，以保障政务云安全稳定正常运行；[0, 1] 5. 是否提供独立的政务外网云资源池，为自治区政务服务专用，不与其他非政务服务用户资源共

					用，政务外网的云资源除了与政务外网连接外，不与其他资源连接。[0, 1]
				政务云资源安全运行管理质量达标情况	3 评价承接主体政务云资源安全运行管理质量是否达标。 承接主体所提供的政务云资源的安全运行管理，是否制定政务云安全运行管理制度和保障措施，定期开展安全自查工作，按照重保要求制定并执行重保实施方案和应急预案，制定应急演练计划和方案，定期开展应急演练，确保政务云安全稳定运行。[0, 3]
				事件 / 故障处理有效情况	6 评价承接主体对故障/事件处理有效情况。主要包括： 1. 承接主体是否对系统故障的诊断及时准确；[0, 2] 2. 故障恢复后对系统运行是否无影响；[0, 2] 3. 故障解决后提供故障分析报告，查明故障原因并提出预防方案。[0, 2]
				重大事件保障服务质量达标情况	4 评价承接主体在重大节假日、关键事件期间或当购买主体对网络进行重大操作时应其要求提供保障服务质量。主要包括： 1. 是否按照重保要求制定并执行重保实施方案和应急预案；[0, 2] 2. 是否重保期结束后提供服务报告。[0, 2]

				况		
				链路连接服务质量达标情况	4	评价承接主体链路连接服务质量达标情况，主要包括： 1. 承接主体提供的网闸设备的技术参数及性能指标是否符合要求。[0, 2] 2. 承接主体提供的 16 条 10GE 链路是否保障传输链路质量指标符合要求。[0, 2]
				输出成果达标情况	5	评价承接主体提交的周报、月报、重大事件保障服务总结报告、故障分析报告等其他输出成果质量是否达标。主要包括： 1. 周报应包含本周工作完成情况，以及对下周的工作安排；[0, 1] 2. 月报应将周报统一整合并进行概括总结；[0, 1] 3. 重大事件保障服务总结报告应包含活动前的安全检查以及活动期间的安全值守情况；[0, 1] 4. 故障分析报告应包含故障概况（简洁明了，标明时间）、原因分析、故障定性、整改建议及预防措施；[0, 1] 5. 与云资源扩容项目政务云相关的其他输出成果质量达标情况等。[0, 1]
				工单流程合理性	4	评价承接主体项目工单流程合理性。主要包括： 1. 考核项目工单流程是否完整规范，内容要素是否齐全。[0, 2] 2. 对于定期评价工单考核完成率 100%。[0, 2]
		服务时效	19	服务响应及时性	4	评价承接主体不同响应支持服务的及时程度。主要包括： 1. 驻场人员是否提供 7*24 小时值班运维服务。[0, 1] 2. 是否提供 7*24 小时远程技术支持服务（电话支持服务）。[0, 1] 3. 电子邮件支持服务响应时间：一般问题的解决方案响应不超过 2 小时，紧急故障响应时间小于 30 分钟。[0, 1]

					4. 现场技术支持服务响应时间：紧急故障到场时间小于 2 小时、严重系统故障到场时间小于 3 小时、一般系统故障、某些功能不会使用或操作问题到场时间 4 小时。[0, 1]	
			故障响应及时性	4	评价承接主体对故障响应及时程度。主要包括： 1. 故障判断为紧急故障、严重系统故障时，是否在 10 分钟的时间内立即响应；[0, 2] 2. 故障判断为一般系统故障、某些功能不会使用或操作问题时，是否在 20 分钟的时间内立即响应。[0, 2]	
			故障恢复及时性	6	评价承接主体是否在规定处理时限内完成故障处理工作。主要包括： 1. 紧急故障的业务恢复时限为 4 小时；[0, 2] 2. 严重故障、一般系统故障的业务恢复时限为 8 小时；[0, 2] 3. 某些功能不会使用或操作问题的业务恢复时限为 8 小时。[0, 2]	
			输出成果提交及时性	5	评价承接主体提交服务报告（输出成果）的及时程度，如：是否 3 个工作日内交付云服务与线路、交付云服务后是否 3 个月内提交密码评估报告，是否按购买主体要求按时提交报告、每月 10 号前提交月度运维、每次重保结束后 3 日内提交总结报告、操作方案不少于提前 5 日提交材料等。（未按时间完成一项服务扣 1 分，最高扣 5 分）[0, 5]	
		安全保障	2	项目整体安全保障服务	2	评价承接主体项目服务过程中安全保障程度。主要包括： 1. 人员安全：所有参与项目的成员都需要签署保密承诺书，进行在岗人员基本信息登记，包括人员基本情况、工作情况、涉密情况等；离岗人员需做好工作交接，进行离岗基本信息登记。[0, 0.5] 2. 应急预案：提前制定全面的应急预案，涵盖可能遇到的各种紧急情况（如数据泄露、自然灾害等）。预案应详细列出每种情况下应采取的具体步骤、责任分配以及联络机制。一旦发生紧急情况，必须及时准确地编制并提交情况报告，记录事件发生的经过、影响范围、已采取的应对措施及后续计划。[0, 0.5] 3. 供应链安全：确保从供应商处获得的产品具有高稳定性和可靠性。可以通过考核是否建立严格的质量控制标准等方式来评价。对用于生产或服务

					务的关键设备是否进行定期维护检查，确保其运行状态良好，避免因设备故障导致的服务中断或安全事故。应考虑设备的冗余设计，以增强系统整体的稳定性。[0, 0.5] 4. 运维管理安全：根据消防安全要求，本项目在合适的位置配置足够数量且适用类型的灭火器，并定期检查确保其处于可用状态。严格管理办公区域内的易燃易爆物品，确保这些物质按照规定储存、使用，并远离火源。是否组织员工参加消防安全培训，提高火灾防范意识和自救能力。[0, 0.5]
--	--	--	--	--	--