

附件 1：软件运维服务考核表

软件运维服务考核表

考核日期：

一级指标	二级指标	三级指标	评价标准	分值	考核得分
组织管理 (20分)	计划组织	方案设计	整体服务方案明确、可行，服务资源配置合理，服务流程明确。	5	
	合同管理	档案管理的完整性	档案管理是否有效完整，相关记录文件、工作计划方案、项目进展和资金支付、工作汇报总结、重大活动和其它有关资料信息。	5	
		合同履行情况	按照合同签订内容履约合同内所涉及的所有条款。	10	
服务过程 (37分)	人员管理	出勤管理	严格执行请销假制度，不得擅自离岗。驻场人员一人请假1天及以内需向甲方请假，驻场技术人员大于1人请假期需向运维负责人请假并报备于甲方（若无驻场人员得满分）。	4	
		人员保证	运维团队离岗离职须通知甲方，并征得甲方取得同意，经同意后三日之内替换人员必须到岗，且为同等级以上技术资质人员。	3	
			团队人数满足投标文件承诺人数和人员安排。	3	
	工作保密	保密协议签署	运维团队与大数据中心签署保密承诺书。	3	
			运维公司与大数据中心签署保密协议。	3	
		离职（离岗）安全管理	离职（离岗）人员不得将本项目涉及网络安全、应用系统安全、数据安全的资料信息带走或者透露给他人，包括但不限于：设备及系统的用户名密码、门禁密码、网络安全配置策略、系统数据等、离岗交接等。	3	
	分工及资质	团队职责	提供项目一线团队评价人员名单分工和资质（提供复印件）。	3	
			提供项目二线团队评价人员名单分工和资质（提供复印件）。	3	
		资质要求	提供运维团队所在公司投标时相关资质（提供复印件）。	3	

应用系统运维 (43分)	服务满意度	数据资源管理服务满意度	服务对象对服务企业支撑数据资源共享、开放管理等工作的满意程度。	3	
		使用人员满意度	服务对象对服务项目的满意程度。	3	
		采购人满意度	采购人对服务项目的满意程度。	3	
	方案报告	定期报告	定期上报月报，年报。（月报、年报上报时间:下月第三个工作日前）	3	
		事件报告	系统运行期间发生的相关事件，须提交事件报告或说明。	3	
	日常工作	日常巡检	检查应用系统、中间件、数据库、数据传输（同步）运行情况，确保应用系统稳定运行。	3	
		重保巡检	重要节假日检查应用系统、中间件、数据库、数据传输运行情况，确保应用系统稳定运行。	3	
		故障处理	对各种数据库、应用系统相关软件的问题及时进行处理，并详细记录形成文档，同时出具故障处理报告。	5	
	运维项目管理	进度控制	对应用系统实现接口开发、功能提升、新功能部署、BUG升级、漏洞补丁，满足质量要求和预期，需要在规定时间内完成。（最长时间不得超过三个月）	5	
	应用系统安全	等保测评整改	配合做好等保测评整改工作，最长整改时间不能超过一个月。	3	
		密码测评整改	配合做好密码测评整改工作，规定时间内完成。	3	
		漏洞整改	配合做好应用系统安全漏洞整改工作，需要在规定时间内完成漏洞整改工作，最长时间不得超过一个月。	5	
备份策略		制订本应用系统的数据备份策略，并且有执行性。	5		
		对应用系统数据进行本地备份并按照备份策略执行，更新频率一天一次。			
应急响应	出现网络安全事件时,1小时内提供应急响应相关服务，发生影响广泛的网络安全事故时，30分钟内提供应急响应相关服务，规定时间内解决故障，及时、安全、稳妥排除故障及隐患。最长时间不超过24小时。	5			
得分总计					

被考核方代表(签字)	
考核方(签字):	

附件2：网络安全运维服务考核表

网络安全运维服务考核表

考核日期：

一级指标	二级指标	三级指标	评价标准	分值	考核得分
组织管理 (20分)	计划组织	方案设计	整体服务方案明确、可行，服务资源配置合理，服务流程明确。	5	
	合同管理	档案管理的完整性	档案管理是否有效完整，相关记录文件、工作计划方案、项目进展和资金支付、工作汇报总结、重大活动和其它有关资料信息。	5	
		合同履约情况	按照合同签订内容履约合同内所涉及的所有条款。	10	
服务过程 (32分)	人员管理	出勤管理	严格执行请销假制度，不得擅自离岗。驻场人员一人请假1天及以内需向甲方请假，驻场技术人员大于1人请假期需向运维负责人请假并报备于甲方（若无驻场人员得满分）。	3	
		人员保证	运维团队离岗离职须通知甲方，并征得甲方取得同意，经同意后三日之内替换人员必须到岗，且为同等级以上技术资质人员。	3	
			团队人数满足投标文件承诺人数和人员安排。	3	
	工作保密	保密协议签署	运维团队与大数据中心签署保密承诺书。	3	
			运维公司与大数据中心签署保密协议。	3	
		离职(离岗)安全管理	离职（离岗）人员不得将本项目涉及网络安全、应用系统安全、数据安全的资料信息带走或者透露给他人，包括但不限于：设备及系统的用户名密码、门禁密码、网络安全配置策略、系统数据等、离岗交接等。	3	
	分工及资质	团队职责	提供项目一线团队评价人员名单分工和资质（提供复印件）。	3	
			提供项目二线团队评价人员名单分工和资质（提供复印件）。	3	
		资质要求	提供运维团队所在公司投标时相关资质（提供复印件）。	2	
	服务满意度	使用人员满意度	服务对象对服务项目的满意程度。	3	
		采购人满意度	采购人对服务项目的满意程度。	3	

网络安全运维服务（48分）	方案报告	定期报告	网络及安全情况定期上报周报、月报，季报（提供纸质版和电子版）。（周报上报时间：每周五10点前，季报、月报上报时间：下月3日前）	3	
		事件报告	网络安全事件，导致事故，须提交事故报告。事件三天内完成正式报告交付，提供纸质版和电子版	3	
	安全值守及重要时期安全保障	值守防护监测	在敏感时期、重大节假日技术人员对服务对象提供7×24小时网络监测服务；落实一系列安全防护措施，保障公共安全和信息安全，有效防范恐怖袭击、黑客攻击、网络病毒等安全事件的发生。	5	
		成果材料	提供服务方案、服务日报、故障总结等书面材料。	3	
	网络安全措施	安全漏洞扫描	对用户系统主机服务器、操作系统、数据库和应用服务等中存在的安全漏洞进行扫描，并输出报告。	5	
		渗透测试	通过模拟恶意黑客攻击的手段，分析方法，对用户网络系统进行安全测试，帮助发现和挖掘系统中存在的漏洞，并输出报告。	5	
		安全加固	根据用户系统情况制定相应测试方案、加固方案与回退方案，通过安装补丁、修改安全配置等方法，增强信息系统抵抗风险的能力，从而提高整个系统的安全性，并输出报告。	3	
		日志安全分析	对用户各类系统产生的日志进行数据分析，及时发现攻击事件和可疑行为，并输出报告	3	
		恶意样本分析服务	通过现场分析的方法对用户主机操作系统和应用运行环境的恶意样本排查，主要包括可疑文件、可疑服务、可疑进程、可疑端口、可疑的网络链接、网站WebShell后门等一系列内容的深入检查和分析，并提供报告和应对方法。	3	
	安全意识培训	网络安全知识培训	开展网络安全知识讲座，增强网络安全意识。	3	
		现场应急演练	现场实操演练安全事件的应急处理，提升应急能力。		
	应急管理	发生网络安全事件及响应	因网络安全防护问题及运维过失问题发生网络安全事件。网络安全事件：核心信息系统应用时段停止工作2小时以内、一般信息系统应用时段停止工作4小时以内、本级专网（互联网）工作时间停网2小	3	

			时以内、重要网络安全设备停止工作2小时以内、丢失500条以内个人信息及重要数据、丢失1000条以内其他关键数据丢失等网络安全事件。（如额外造成损失的按照损失价值进行赔偿）		
			出现网络安全事件时，按照应急响应方案，提供应急服务。1小时内提供应急响应相关服务，在规定时间内解决故障，及时、安全、稳妥排除故障及隐患。最长时间不超过24小时。	3	
		发生影响广泛的网络安全事故及响应	因网络安全防护问题及运维过失问题发生重大网络安全事件。重大网络安全事件：核心信息系统应用时段停止工作2小时及以上、一般信息系统应用时段停止工作4小时及以上、本级专网（互联网）工作时间停网2小时及以上、重要网络安全设备停止工作2小时及以上、门户网站或对外应用系统发生恶意挂马事件、丢失500条及以上个人信息及重要数据、丢失1000条及以上其他数据丢失、被省级及以上网络安全主管部门通报等网络安全关键安全事故。（如额外造成损失的按照损失价值进行赔偿）	3	
			发生影响广泛的网络安全事故时，按照应急响应方案，提供应急服务。30分钟内提供应急响应相关服务，在规定时间内解决故障，及时、安全、稳妥排除故障及隐患。最长时间不超过24小时。	3	
得分总计					
被考核方代表（签字）					
考核方（签字）：					

附件3：社会信用信息平台运维管理绩效考核制度

内蒙古自治区社会信用信息平台运维管理绩效考核制度 总则

第一条为规范内蒙古自治区社会信用信息平台（以下简称信用平台）的日常运维工作，加强管理，切实有效提升平台运维质量，保障平台安全稳定运行，特制订本制度。

第二条本制度适用于参与信用平台管理和运维服务的所有人员。

第三条全体运维人员要遵循“实事求是，尽职尽责、团结协作”的原则，遵守保密规定，提高工作效率，遇到问题不推诿，在做好本职工作的同时做好与他人的配合衔接，增强运维的协同性、连续性和有效性。

第四条本制度实施年度积分管理，如有违反相关条款的行为，将扣除相应的运维分值，以积分方式衡量各运维单位的工作质量，按运维得分结算年终运维费用。

第五条内蒙古自治区大数据中心信息技术服务六处（以下简称“信息技术服务六处”）负责内蒙古自治区社会信用信息平台的运维管理工作。

运维范围

第六条信用平台运维管理服务范围包括以下内容：

（一）信用平台硬件运维及软硬件安全维保服务服务范围包括但不限于以下内容：

信用平台硬件运维服务：网络设备、服务器、存储、产品软件、安全设备、虚拟服务器等 387 台（套）运维服务。

信用平台软硬件安全维保服务服务范围包括但不限于以下内容：包括 115 台网络、安全设备、81 台主机设备、4 台存储设备，166 套产品软件和 21 台虚拟服务器设备的原厂、非原厂维保。

（二）信用平台软件运维服务项目服务范围包括但不限于以下内容：

运维服务管理系统、信用信息公共服务系统、信用信息公示系统、信用信息共享应用系统、联合奖惩服务系统、大数据征信系统、信用大数据资产管理系统、

信用大数据挖掘分析系统、企业债券管理系统及其子系统、信用内蒙古 APP 运行维护、信用内蒙古微信公众号运行维护和管理。

（三）信用平台安全运维服务服务范围包括但不限于以下内容：包括联通云互联网区、联通云专网区、征集交换中心区域的服务器；征集交换中心区域的网络设备；征集交换中心区域的安全设备；征集交换中心、联通云区域的数据库及中间件；征集交换中心、联通云区域的应用系统；信用中国（内蒙古）APP 等安全运维服务。

第七条 硬件运维及软硬件安全维保服务单位负责信用平台硬件运维及软硬件安全维保工作，自觉遵守安全管理规定。

第八条 信用平台软件运维服务单位负责信用平台软件运维服务的日常运维工作，自觉遵守安全管理规定。

第九条 信用平台安全运维服务单位负责信用平台安全运维服务项目的日常运维工作，自觉遵守安全管理规定。

运维人员管理

第十条 各单位在签订运维协议一周内，向信息技术服务六处提交项目负责人和实施工程师的姓名、职务、职责分工、联系方式、值班方式等资料。运维期间，如发生人员、职责等变动，应及时向信息技术服务六处提交变更资料。

第十一条 运维人员应具备相关资格证书，上岗前必须与内蒙古自治区大数据中心签署个人安全保密协议，提交个人身份证复印件。运维人员需在运维服务系统实名注册，通过运维管理系统提交运维工作中遇到的问题及需求。

第十二条 运维人员离岗前应由所属单位提出书面申请，交回所有相关文档并签订离岗保密承诺书。

第十三条 运维人员应当自觉遵守保密规定，对运维工作中使用的设备、数据、存储介质的使用、保存、销毁应严格尊重管理规定，不私自留存、买卖、转让、泄露，不携带出工作场所之外。

第十四条 运维人员要遵守内蒙古自治区大数据中心、本公司以及国家和行业规定的其他安全保密规定，如有违反，按照相关规定处置。

运维职责

第十五条 信用平台硬件运维及软硬件安全维保服务日常工作、服务质量和安全管理要求：

（一）日常工作：信用平台硬件运维服务服务内容包括但不限于以下巡检服务、数据库性能调优、故障排查、配置变更、资产管理等。

1、巡检服务：运维公司根据服务内容每月进行在线巡检，对服务器状态(状态灯是否正常、有无硬件报警信息、每个磁盘状态、ARRAY 状态、服务器电源状态)、存储状态（磁盘状态、日志信息、zone 信息等）进行检查，云平台及虚拟主机的状态进行检查，对检查过程中发现的问题进行排查和处理，并做好日常巡检的登记记录，并及时出具巡检报告。

（1）中间件巡检

预防性健康检查：对中间件产品定期进行健康状况检查。

对标准维保服务的最终用户，厂商提供远程巡检服务，服务期内远程巡检每半年一次，远程巡检方式包括：

指导用户自行巡检：厂商为用户提供巡检模板，用户运维人员按照模板中的方法自行进行健康检查，并将巡检报告提方通售后支持邮箱，厂商售后工程师会对用户的自检结果进行诊断，并将诊断结果以及调整建议及时反馈给用户。

电话回访：厂商工程师定期进行电话回访，了解生产系统的运行状况，并针对用户反馈的问题进行记录和诊断。

远程接入巡检：厂商工程师可远程接入最终用户生产系统，对中间件的运行状况进行检查，并提供巡检报告。远程接入巡检，必须征得厂商销售和售后服务负责人的同意。

巡检的内容有：

中间件运行平台的基本信息：操作系统的版本及补丁、操作系统的核心参数

配置；

中间件运行对资源的占用：磁盘、CPU、内存、带宽占用率等；

中间件的负载情况和性能表现；

中间件的关键配置及系统日志。

（2）服务器巡检：

例行巡检：月度/次

A、服务器面板巡检

对服务器进行检查，检查服务器指示灯状态，填写例行巡检表。

B、服务器状态巡检

对存储、服务器的 CPU、内存、网络接口、磁盘、文件系统性能及日志进行检查和分析；填写日常检查表。

C、配套软件巡检

（3）存储状态巡检：

例行巡检：季度/次

A、对存储状态巡检，包括对面板信息、磁盘使用量、控制器、电池等进行检查和分析，如发现异常，及时按照服务流程进行处理。

B、对存储设备进行存储测试，上传下载速率。

C、运维公司对存储进行一次深度巡检，每次巡检服务结束后向内蒙古自治区大数据中心做巡检汇报并于 2 个工作日内提交巡检报告。

每月或重大活动前须进行巡检，巡检完一周内提交巡检报告及改进优化建议，必要时负责或配合实施，巡检由资深人员完成。

（4）网络状态巡检：

例行巡检：季度/次

A、对网络设备状态巡检，包括对设备配置、运行日志、设备版本情况进行检查和分析，如发现异常，及时按照服务流程进行处理。

B、对网络设备进行带宽测试，上传下载速率。

C、运维公司对网络、安全设备进行一次深度巡检，每次巡检服务结束后向内蒙古自治区大数据中心做巡检汇报并于2个工作日内提交巡检报告。

每月或重大活动前须进行巡检，巡检完一周内提交巡检报告及改进优化建议，必要时负责或配合实施，巡检由资深人员完成。

(5) 虚拟化平台巡检：

例行巡检：季度/次

A、对虚拟化平台状态巡检，包括对平台中的主机设备状况、存储状况、网络状况、虚拟主机设备运行情况，平台日志等信息查看，通过平台发现平台的运行状况，根据状况进行及时的调整运维方案。

B、按照项目需求，进行新增虚拟机的部署、迁移、扩容及删除工作。

每月或重大活动前须进行巡检，巡检完一周内提交巡检报告及改进优化建议，巡检由资深人员完成。

2、数据库性能调优：利用工具采集系统运行时的各项监控数据；

分析系统主要的性能瓶颈；

分析系统、网络、应用软件及数据库等各方面资源的使用情况；

确定系统性能现状及性能调整的目标；

定位系统中出现的性能瓶颈；

测试验证针对性能瓶颈进行的改进方案；

产生基于数据库的最佳应用准则的性能调整建议报告；

适用于当前商业规则的软件配置；

为用户提供实施问题的解决方案；

为用户进行现场技能讲解传授；

工程师在现场调优数据库性能和应用性能；

给用户完整的性能调整报告和解决方法；

确保本次调优范围内所有数据库的正常运行。

3、故障排查：厂商的工程师可以远程指导用户进行故障的分析和排查，必

要时可远程接入用户的服务器进行故障诊断处理。

故障排查仅限于厂商的中间件本身，不包括应用系统，可配合用户对中间件相关的软件或系统的故障进行分析。

在厂商工程师的配合下，用户运维人员对出现的故障进行诊断，主要进行以下处理步骤：

故障现象收集：抓取现场日志和监控数据，收集平台、产品版本、使用方式等信息。

故障现象分析与定位：首先分析是否平台、硬件或网络等运行环境问题，然后分析是否是产品不当导致的问题（如配置问题，应用问题等），最后分析是否是产品的问题导致；

提出解决方案：根据故障的原因，给出解决方案。

远程指导用户排除故障：若由运行环境或使用不当导致，则指导用户进行调整。若定位是产品问题，则提供解决方案，打补丁或升级。

针对严重性故障，经厂商工程师诊断认为确属中间件产品的重大缺陷所导致，且短时间内远程无法解决的，可提供现场服务。

4、配置变更：

(1) 配合安全厂家，对设备存在的安全问题，协议认证模式，数据加密验证方式配置进行更改。

(2) 配合相关业务需求，对网络设备配置，出口设备配置进行更改。

(3) 配合其他厂商对设备进行查看。

(4) 配合信源单位，因搬迁导致网络发生变化，对配置进行更改。

5、资产管理：

管理社会信用信息平台资产，维护资产表，配合完成资产筛查、资产信息更新。

（二）信用平台软硬件安全维保服务服务内容包括但不限于通用软件、硬件原厂维保服务包括但不限于以下内容：获得原厂软件授权、特征库升级、版本升

级、补丁服务、7*24 原厂技术支持。

6、软件维保：

（1）中间件的维保服务：

1. 性能调优服务：产品运行一段时间后，或者最终用户的业务发生变化，原有系统无法满足现有业务需要，需提升系统性能

2. 故障诊断与排查服务：厂商的工程师可以远程指导用户进行故障的分析和排查，必要时可远程接入用户的服务器进行故障诊断处理。

3. 小版本的产品升级和补丁服务

产品小版本升级和打补丁，修复产品问题，提升产品的功能或性能。

4. 预防性健康检查：预防性健康检查是对中间件产品定期进行健康状况检查，以便及时发现产品运行的问题。巡检的内容有：

中间件运行平台的基本信息：操作系统的版本及补丁、操作系统的核心参数配置；

中间件运行对资源的占用：磁盘、CPU、内存、带宽占用率等；

中间件的负载情况和性能表现；

中间件的关键配置及系统日志。

（2）数据库的维保服务：

1. 数据库运行维护服务包括数据库主动巡检，故障快速处理、诊断和解决，配合用户做必要的数据库迁移、测试、备份还原、调优、安全测评等，用户咨询、培训、指导等。

2. 健康检查：工程师定期（最小频率为每天）对数据库系统进行例行健康检查，并提交报告，根据健康检查的内容对数据库进行维护和优化。检查的内容包括但不限于以下内容：

检查并分析系统日志及跟踪文件，发现并排除数据库及应用系统的错误隐患；

检查数据库及应用系统的配置健康情况；

发现并排除数据库系统错误隐患；

检查数据库系统是否需要应用最新的补丁集；

检查数据库空间的使用情况，协助进行数据库空间的规划管理；

检查数据库备份的完整性；

监控数据库性能、数据库运行状态、运行效率、是否存在安全隐患；

备份方式是否合理、备份数据是否可恢复；

提供健康检查报告；

每半年进行一次健康检查总结；

3. 数据库性能调优：

利用工具采集系统运行时的各项监控数据；

分析系统主要的性能瓶颈；

分析系统、网络、应用软件及数据库等各方面资源的使用情况；

确定系统性能现状及性能调整的目标；

定位系统中出现的性能瓶颈；

测试验证针对性能瓶颈进行的改进方案；

产生基于数据库的最佳应用准则的性能调整建议报告；

适用于当前商业规则的软件配置；

为用户提供实施问题的解决方案；

为用户进行现场技能讲解传授；

工程师在现场调优数据库性能和应用性能；

给用户完整的性能调整报告 and 解决方法；

确保本次调优范围内所有厂商数据库的正常运行。

4. 运维及培训服务：提供特殊时段（如：春节、劳动节、国庆节、年终、系统停机维护、数据集中及用户认为必须的重要时段）的数据库保障服务；提供产品安装、系统变更和迁移等现场支持服务。

提供故障应急处理及快速恢复现场服务。10 分钟内响应，2 小时以内到达现场。一般问题 1 小时以内解决，涉及数据迁移等长时工作原则上 24 小时以内解

决。每次处理故障后在运维报告中详细记录。

配合用户方进行数据库相关各类测评工作。

每半年进行一次运维工作总结。

提供本地化的服务团队，快速响应用户需求,7×24 小时远程技术支持服务。

对用户方技术人员就数据库相关知识及操作进行相关指导和培训。

运维服务原则上采取现场服务+多方式远程服务。如需驻场服务，双方另行沟通协商。届时就驻场运维地点、范围、内容、要求、费用等进行详细沟通协商。

7、硬件维保

(1) 服务器维保服务

1. 远程技术支持:7x24 小时服务热线响应、专家工程师全天候远程技术支持、服务器硬件、预装操作系统及虚拟机远程技术支持

2. 现场技术支持:

(2) 存储设备的维保服务

服务内容	服务响应时间	描述	备注
热线受理	7×24	7×24: 周一至周日,00:00~24:00 (全天候,节假日无休)	无
远程问题处理	7×24	7×24: 周一至周日,00:00~24:00 (全天候,节假日无休)	远程问题处理服务响应时间定义: 自技术支持中心响应工程师受理用户故障之时起算, 到技术服务工程师首次联系用户开始远程技术支持服务为止
在线技术支持	7×24	网站, 7×24: 周一至周日,00:00~24:00 (全天候)	无
软件更新授权	7×24	网站, 7×24: 周一至周日,00:00~24:00 (全天候)	无

备件先行	7×10×ND	7×10: 周一至周日,08:00~18:00, ND 到达: 下一日到达	无
现场工程师 硬件更换/ 现场问题处 理	7×10×ND	7×10: 周一至周日,08:00~18:00, ND 到达: 下一日到达	无

(3) 网络设备的维保服务

1. 上门现场服务
2. 电话及现场技术支持
3. 故障响应支持
4. 软件维护升级服务

服务内容	服务响应时间	描述	备注
热线受理	7×24	7×24: 周一至周日,00:00~24:00(全天候,节假日无休)	无
远程问题处理	7×24	7×24: 周一至周日,00:00~24:00(全天候,节假日无休)	远程问题处理服务响应时间定义: 自技术支持中心响应工程师受理用户故障之时起算, 到技术服务工程师首次联系用户开始远程技术支持服务为止
在线技术支持	7×24	网站, 7×24: 周一至周日,00:00~24:00(全天候)	无
软件更新授权	7×24	网站, 7×24: 周一至周日,00:00~24:00(全天候)	无
备件先行	7×10×ND	7×10: 周一至周日,08:00~18:00, ND 到达: 下一日到达	无

现场工程师 硬件更换/ 现场问题处 理	7×10×ND	7×10：周一至周 日,08:00~18:00, ND 到达：下一日到达	无
------------------------------	---------	--	---

8、安全设备原厂维保服务内容：获得原厂软件授权、特征库升级、版本升级、补丁服务、7*24 原厂技术支持、故障部件更换、备品备件服务

(1) 提供原厂全年 7*24 响应服务，4 小时到达现场完成技术支持服务，并按照服务内容中的具体要求提供安全设备的硬件更换及软件免费升级服务；

(2) 提供紧急故障处理服务，当系统发生紧急故障时，应及时响应并进行故障处理；

(3) 能够及时提供维保设备的补丁程序；

(4) 所有安全设备硬件故障的维修服务方式均为现场服务，包括维修、维护、更换部件。

9、硬件设备非原厂维保服务内容：7*24 技术支持、维修更换服务

(三) 质量要求：

10、响应程度：所有软件、硬件、安全运维以及维保根据故障级别均提供 7*24 小时响应服务。

故障级别	响应时间	故障解决时间
I 级：属于紧急问题，其具体现象为：系统崩溃导致业务业务停止、数据丢失	30 分钟，2 小时内提交故障处理方案	12 小时内
II 级：属于严重问题：其具体现象为出现部分部件失效、系统性能下降但能正常运行，不影响正常业务运作。	30 分钟，2 小时内提交故障处理方案	24 小时内
III 级：属于较严重问题；其具体现象为：出现系统报错或警告，但业务系统能继续运行且性能不受影响。	30 分钟，2 小时内提交故障处理方案	48 小时内
IV 级：属于普通问题；其具体现象为：系统技术功能、安装或配置咨询，或其他显然不影响业务的预约服务。	30 分钟，2 小时内提交故障处理方案	5 天内

11、运维成果要求：通过运维服务协助内蒙古自治区社会信用信息平台检查设备目前的状态，并分析其潜在的问题，进而给出解决这些问题的建议和方法。这样可以利用运维方面的经验，协助内蒙古自治区社会信用信息平台检查出数据中心可能存在的潜在问题，最大限度地减少运维不当所带来的危害。提出日常维护系统的进一步建议，避免产生新的问题。通过安装有效的诊断工具，在出现问题时，维护人员能更快、更有效的定位问题、解决问题，减少对业务的影响。

12、运行安全要求：内蒙古自治区社会信用信息平台各信息系统的运行安全包括系统风险管理、审计跟踪、备份与恢复和应急处理等四个方面。系统的运行安全是信息系统安全的重要环节，只有信息系统的运行过程中的安全得到保证，才能保障内蒙古自治区社会信用信息平台业务平台的运行安全。

第十六条 信用平台软件运维服务日常工作、服务质量和安全管理要求：

（一）日常工作包括但不限于为信用平台的软件维护服务，日常维护（驻场服务），数据服务工作和培训服务等。

13、日常维护（驻场服务）：

1. 快速故障排除服务：提供远程接入服务、现场支持服务、系统恢复和故障解决服务。

2. 远程接入服务：远程接入支持服务：在采购人允许的前提下，运维方提供远程接入服务。该服务主要针对于通过电话指导不能解决的故障，通过远程接入手段，进行故障诊断，查找故障出现的原因，指导驻场人员处理故障。

3. 现场支持：现场故障分析排除服务：对于通过电话支持、远程支持和驻场人员都不能解决的应用系统故障，工程师需迅速提供现场支持服务，安排经验丰富的技术支持工程师赴现场分析故障原因，制定故障解决方案，并最终排除故障。

4. 系统恢复和故障解决服务：对软件故障进行排除及相应的系统恢复。

5. 第三方故障配合服务巡检与报告服务：当硬件故障或因第三方原因引起的信用平台故障时，运维方将配合采购人，直至应用系统恢复。

14、巡检与报告服务：提供巡检服务和报告服务。定期对软件健康性进行检

查并提供巡检报告，在维护期内，技术人员实施定期巡检服务。内容包括：

1. 每周系统功能巡检
2. 每日数据库巡检
3. 每日完成数据备份
4. 每日数据共享定时任务巡检
5. 每月系统程序包备份
6. 系统升级更新
7. 每周编写运维工作周报

15、性能优化服务：结合系统实际运行情况和用户需要，对信用平台进行性能优化和调试，提升信用平台各方面的综合性能。包括以下几个方面：

1. 平台占用资源优化；
2. 平台运行效率优化；
3. 平台软件配置优化；
4. 平台现有功能优化。

16、数据服务工作：

数据上报和下发：通过平台快速连接到自治区各级部门和盟市信用主管部门，实现数据源到平台的无缝化衔接。同时不断加强数据服务过程管理，提升报送下发实效和质量，实现自治区双公示、五归集、特定信用信息等数据集中归集和治理，主要完成以下数据上报和下发工作。

（1）数据上报：

1. 每日双公示数据上报国家工作
2. 每日处理国家双公示系统中的错误数据
3. 每日处理国家双公示系统中的待确认数据
4. 每月核查国家抽取下发的双公示瞒报数据
5. 每周五类行政管理数据上报国家工作
6. 每周信用承诺上报国家工作

7. 每日联合惩戒和守信激励数据上报国家工作

(2) 数据下发:

1. 每周国家向省前置机下发本省主体名称和统一社会信用代码
2. 每日国家下发信用修复结果数据工作
3. 每日国家下发异议处理数据工作
4. 每年国家下发的企业公共信用综合评价结果

数据采集和共享:

(1) 数据采集

持续进行数据源部门数据接入,明确数据采集方式、采集周期,依据部门职能范围、政策法规和信息化建设程度维护部门信息目录。

1. 每日双公示. 五类行政管理信息. 特定信用信息以及其他信用信息数据报送工作支撑

2. 每日双公示待确认数据核对
3. 每日双公示主体比对失败数据核对
4. 每日双公示错误数据处理
5. 每月双公示抽取瞒报待查数据
6. 每周五类行政管理信息. 特定信用信息主体比对失败数据核对
7. 每周五类行政管理信息. 特定信用信息错误数据处理
8. 自治区区直部门前置机对接沟通及数据处理
9. 自治区区直部门接口对接沟通及数据处理

(2) 采集周期

以作业的方式对数据采集任务进行调度。考虑到数据的整合内容、步骤很多且需要经常按照同一模式执行配置好的整合流程,满足分布的数据整合过程,因此需要一个计划调度功能。通过创建作业可以实现流程的调度执行。调度方式非常灵活,可以是一次执行,也可以是反复按时间间隔执行,完全满足采集数据周期多种多变的情况。

（3）信息目录维护

完成部门信用事项和信用指标在系统中的初始化配置和维护管理。依据部门职能范围、政策法规和信息化建设程度维护部门信用信息目录，完成部门目录和指标项的初始化和更新管理，包括以下功能：

1. 部门信用目录的调研和梳理；
2. 部门信用目录的编制、审核与确认；
3. 部门信用目录和信用指标的系统初始化。

（4）数据共享工作

依据信用事项的服务要求，按时按需对盟市及自治区直属部门共享信用数据，主要为：

1. 每周通过前置库给自治区区直部门共享数据
2. 每周通过前置库给盟市共享数据
3. 不定期按需配置共享接口

数据统计分析：定期需要对数据进行多维度的挖掘分析，利用数据洞察形成领导辅助决策报告；对信用指标细粒度的监控管理，多角度全方位直观的掌握信用现状；基于已有数据的预警、分析、评价和趋势预测；信用分析数据模型的构建，数据对标。主要统计以下数据：

1. 每周共享平台网站数据统计
2. 每月双公示月通报
3. 每季度双公示季度评估
4. 每季度高质量季度考核统计工作
5. 每月信易贷省级节点地方信息归集共享应用情况
6. 每月信易贷省级节点工作进展的报告
7. 日常随机数据统计

数据接口开发和数据对接：在大数据集成基础上，根据业务发展需要完成数据应用场景和规则分析，实现对外数据服务接口的开发与维护。主要提供两种业

务接口，包括数据交换接口、WebService 接口。通过这两种业务接口的方式，实现与已有数据和信息的整合。

（1）数据交换接口，数据交换接口主要为使用者与应用系统、应用与应用之间的数据传递、转换提供规范。

（2）WebService 接口，通过定制标准 WebService 接口，实现信用信息共享平台与其他业务系统之间的数据集成和交换。系统需对 WebService 接口进行规范，加强身份认证和信息安全管理，建立接口管理平台，接口的配置、开通、注销以及接口监控都通过这个系统完成。

完成内蒙古自治区社会信用信息平台与上级及本级信息化系统的对接和数据维护，从各数据源进行数据的抽取、转换和处理，按照统一标准传输至数据中心，并可接收数据中心返回的各类信息，从而实现双向数据交换对接。

数据治理：

（1）完成数据的异常处理、统计、分析和质量评估，开展数据的匹配、融合和交互式修复工作；

（2）各数据源部门的数据采集、更新、处理和汇集情况统计分析；

（3）数据质量和缺失情况分析；

（4）共享数据统计分析；

（5）数据源部门数据比对分析。

17、培训服务：提供系统操作使用培训和技术交流，为自治区信用管理部门以及各数据源部门（行业监管部门）在本次运维服务周期内提供不少于 5 次的关于平台管理、日常操作、双公示报送等相关的培训服务，其中不少于全区双公示数据报送业务培训 1 次，为各盟市提供双公示业务培训 4 次。

1、培训内容：为了科学合理的组织好本平台项目的培训工作，运行维护期间按需完成培训。

2、培训形式：根据用户多、范围广的培训需求，将培训方式分为现场培训和集中培训、专项培训。

18、咨询服务：充分了解所涉及的产品、服务或领域知识。提供专业和有价值的建议和帮助，及时收集问题和需求，并及时回答和解决。对于一些常见问题或需求，进行培训和指导，帮助用户更好地使用产品或服务。主要包括但不限于以下几种咨询服务工作：

- 1 数据报送系统技术支持服务
- 1 数据代报服务
- 1 信用网站内容错敏信息处理服务
- 1 信用核查服务
- 1 业务咨询

（二）服务质量：

19、服务级别：

指标	描述	单位	参考数据
事件平均响应时间	事件响应总时间/事件次数	分钟	≤30 分钟
事件按时解决率	事件按时解决次数/事件总次数×100%	百分比	≥90%
事件响应超时率	事件响应超时次数/事件总数×100%	百分比	<10%
事件平均用户满意度	事件平均用户满意度=Σ满意度/统计次数	百分比	≥90%
关键应用系统运行率	关键应用系统运行率=[（周期时长-各关键应用系统中断总时长-各关键应用系统计划停用总时长）/（周期时长-各系统计划停用总时长）]×100%	百分比	≥99%

20、响应程度：

所有软件、硬件、安全运维以及维保根据故障级别均提供 7*24 小时响应服务。

故障级别	响应时间	故障解决时间
------	------	--------

I 级：属于紧急问题，其具体现象为：系统崩溃导致业务业务停止、数据丢失	30 分钟，2 小时内提交故障处理方案	12 小时内
II 级：属于严重问题：其具体现象为系统性能下降但能正常运行，不影响正常业务运作。	30 分钟，2 小时内提交故障处理方案	24 小时内
III 级：属于较严重问题；其具体现象为：出现系统报错或警告，但业务系统能继续运行且性能不受影响。	30 分钟，2 小时内提交故障处理方案	48 小时内
IV 级：属于普通问题；其具体现象为：系统技术功能、安装或配置咨询，或其他显然不影响业务的服务。	30 分钟，2 小时内提交故障处理方案	5 天内

21、运维成果要求：

软件运维服务要求的交付物包括但不限于以下内容：

《年度技术服务方案》、《年度技术服务工作总结报告》、《月度工作报告、月报表、月度数据归集和统计分析报告》、《周工作报告、周报表》等。

22、运行安全要求：

1. 数据备份：定期进行数据备份，以防止数据丢失或损坏。备份数据应存储在安全的位置，并采取适当的加密措施。

2. 访问控制：实施严格的访问控制策略，确保只有授权人员才能访问敏感数据和系统。使用多因素身份验证，确保只有经过验证的用户才能访问系统。

3. 应急响应计划：制定详细的应急响应计划，以便在发生安全事件时迅速采取行动。计划应包括故障排除步骤、数据恢复策略和与其他部门和机构的协调措施。

第十七条信用平台安全运维服务日常工作、服务质量和安全管理要求：

（一）日常工作：

23、安全事件监测及安全审计

安全监测：服务方需对信用平台内外网系统提供 7*24 小时远程安全事件监测，监测类型至少包括以下内容：

（1）网页木马监测

采用特征分析和沙箱行为分析技术对网站进行木马监测，监测精度高达 99%，从而实现快速、准确的发现和定位网页木马，确保用户在第一时间发现感染的木马并及时消除。

（2）网页篡改监测

通过远程定时监测技术，可以有效的监测网页篡改行为，特别是一些越权篡改、暗链篡改等情形。并针对篡改方式提供篡改截图取证功能，提升事件处理效率。

（3）网站可用性监测

基于远程监测技术可以有效的监测到域名劫持、DNS 中毒、ISP 线路等原因导致的网站可用性问题。提供多线路监测技术，使用户对网站的可用性获得更为全面详细的数据，如业务中断、访问延时、不同 ISP 服务质量等。

（4）网页关键字监测

采用中文关键词以及语义分析技术对网站进行敏感关键字监测，实现精确的敏感字识别，确保网站内容符合互联网相关规定，避免出现敏感信息以及被监管部门封杀。

（5）WEB 漏洞监测

定期自动监测网站的漏洞，并跟踪漏洞的修复情况从而使网站的漏洞得以快速修复，降低网站被入侵的风险。

安全审计内容包括：

（1）有害程序事件：计算机病毒事件、蠕虫事件、特洛伊木马事件、僵尸网络事件、混合攻击程序事件、网页内嵌恶意代码事件和其它有害程序事件；

（2）网络攻击事件：拒绝服务攻击事件、后门攻击事件、漏洞攻击事件、网络扫描窃听事件、干扰事件和其他网络攻击事件；

（3）信息破坏事件：信息篡改事件、信息假冒事件、信息泄漏事件、信息窃取事件、信息丢失事件和其它信息破坏事件；

(4) 设备设施故障：软硬件自身故障、外围保障设施故障、人为破坏事故、和其它设备设施故障；

(5) 其他事件

服务周期和范围：对信用内蒙古门户网站等内外网系统进行 7*24 小时在线监测，根据监控情况形成信用平台系统运行状态每周提交一次安全报告并制定审计策略和定期的安全审计报告。

24、安全事件应急响应服务：在紧急事件发生后迅速采取措施和行动，针对征集交换中心、联通云中心物理环境和应用系统出现的一般技术人员无法迅速解决的异常紧急事件提供安全技术支持，控制事态发展；根据出现的问题及时调整安全策略，根据现场保留情况尽可能对进行追查，帮助运维人员在以后的维护中正确解决问题。紧急事件响应服务主要包括准备、识别事件、抑制、解决问题、恢复以及后续跟踪。紧急事件主要包括：病毒和蠕虫事件、黑客入侵事件、误操作或设备故障事件等。

25、系统漏洞扫描服务：定期开展信息系统漏洞扫描服务，并出具漏洞扫描报告。漏洞扫描测试主要用于识别网络、操作系统、数据库管理系统的脆弱性，发现软件和硬件中已知的弱点，如非法账号、弱口令、权限配置错误、系统补丁、文件目录及文件系统安全、不必要的端口和服务等，以决定系统是否易受到已知攻击的影响。

漏洞扫描范围至少应包括：

(1) 操作系统

Windows、发行版 Linux、AIX、UNIX 通用、Solaris、FreeBSD、HP-UX、BSD 等主流操作系统。

(2) 数据库

Oracle、MySQL、MSSQL、Sybase、DB2、Informix 等主流数据库。

(3) 常见应用服务

Apache、IIS、Tomcat、Weblogic 等主流应用服务，常见 FTP、EMAIL、DNS、

TELNET、POP3、SNMP、SMTP、Proxy、RPC 服务等。

(4) Web 应用程序

ASP、PHP、JSP、.NET、Perl、Python、Shell 等语言编写的 WEB 应用程序。

(5) 网络设备

常见的路由器、交换机等设备。

服务范围：检测范围包括征集交换中心和联通云中心的全部网络设备、安全设备、主机、数据库及中间件。

服务周期：每月对检测对象进行一次漏洞扫描，一年十二次。

26、渗透测试服务：通过专业安全服务工程师模拟黑客的行为方式，采用漏洞发现技术和攻击技术对信息系统进行非破坏性的测试，结合实际软件环境提出安全修复建议。

渗透测试范围至少包括

(1) 操作系统

Windows、发行版 Linux、AIX、Solaris、FreeBSD 等主流系统。

(2) 应用系统

Oracle、MySQL、MSSQL、Sybase、DB2、Informix 等主流数据库，Apache、IIS、Tomcat、Weblogic 等主流 WEB 服务器，FTP、DNS 等主流应用服务器。

(3) WEB 程序

ASP、PHP、JSP、.NET、Perl、Python、Shell 等语言编写的 WEB 程序。

(4) 网络设备

常见厂商的路由器、交换机等设备

渗透测试

每月至少开展一次，整改后 8 小时内复测，内容至少包括：

(1) 认证和授权类

暴力攻击、认证不充分、会话定置、会话期限不充分、凭证/会话预测、授权不充分

（2）命令执行类

LDAP 注入、SSI 注入、SQL 注入、Xpath 注入、操作系统命令、格式字符串攻击、缓冲区溢出

（3）信息泄漏类

可预测资源定位、路径遍历、目录索引、信息泄露

（4）逻辑攻击类

功能滥用、拒绝服务

（5）客户端攻击类

跨站点脚本编制、内容电子欺骗

服务范围：检测范围包括但不限于基础管理系统、综合管理系统、数据治理系统、信用大数据挖掘分析系统、信用内蒙古、法人应用系统、自然人应用系统、大屏展示系统、CA 认证系统、运维管理系统等共 28 套应用系统。

服务周期：每月对检测对象进行一次渗透测试，一年十二次。

27、流量分析服务：利用协议分析工具对全网重要节点进行数据包抓取并结合人工分析，微观的对全网传输的各种安全协议进行评估；评估内容应包括“异常 IP 流量分析”、“内网传输协议分析”、“故障诊断”、“内网木马病毒过滤检测”、网络流量阈值、可疑域名等；对采购人指定的应用进行实时监控和质量分析。

网络协议分析服务：网络协议分析服务内容至少包括“异常 IP 流量分析”、“内网传输协议分析”、“故障诊断”“内网木马病毒过滤检测”、网络流量阈值、可疑域名等

服务范围：检测范围包括征集交换中心和联通云中心的全部网络设备、安全设备、主机、数据库及中间件。

服务周期：每月对检测对象进行一次协议分析，一年十二次。

28、日志分析：对各类系统（如防火墙、IDS、WEB 服务器、WAF、数据库审计流控等）产生的日志进行数据分析，及时发现攻击事件和可疑行为，提供日志分析报告。

网络协议分析服务：网络协议分析服务内容至少包括：“攻击综述”、“可疑攻击分析”“攻击回溯分析”“攻击影响分析”“攻击结果分析”“攻击解决建议”等内容

服务范围：检测范围包括征集交换中心和联通云中心的全部网络设备、安全设备、主机、数据库及中间件。

服务周期：每月对检测对象进行一次日志分析，一年十二次。

29、APP 安全评估服务：全面、定期对内蒙古自治区社会信用信息平台自有 APP（包含 IOS、Android 版本）进行安全评估，发现 APP 存在的安全隐患。

APP 安全评估的主要内容包括：客户端程序安全、敏感信息安全、密码软键盘安全性、安全策略、手势密码安全性、进程保护、通信安全、业务安全。

检查内容

（1）Android 系统 APP 程序的安全测试包括如下内容：

1) 使用工具对 APP 程序进行自动化扫描，对吸费、暗跑流量等恶意行为进行识别；

2) 对 apk 文件进行反编译分析，测试 apk 文件是否被植入恶意代码等。

（2）iOS 系统 APP 程序的安全测试包括如下内容：

1) 使用工具对 APP 程序进行全面渗透测试；

2) 对 APP 程序进行黑盒测试，检测不安全存储及内部通讯组件漏洞；

3) 从 APP 客户端到服务器端进行安全检测。

服务范围

检测范围包括信用内蒙古 APP 共 1 个 APP。

服务周期

每季度对检测对象进行一次 APP 评估，一年四次。

30、安全运维：通过人工加工具的方式对内蒙古自治区大数据中心所有信息系统及安全设备进行安全运维。运维内容包括资产识别及梳理、安全设备日常维护及监控、收集与分析网络及安全设备、服务器、数据库、中间件、应用系统的

日志，对安全设备、网络设备、服务器提供业务操作巡检、状态巡检、安全策略配置巡检服务，实施日常安全运维服务：完成安全设备、网络设备、服务器、应用系统安全事件监控；病毒监测、查杀及网络防病毒维护；漏洞扫描、安全加固、补丁安装，实施健康检查服务：完成安全设备、业务系统的健康检查服务。

服务范围：检测范围包括信用平台全部信息系统及安全设备等。

服务周期：每月对检测对象进行一次安全运维，一年 12 次。

31、安全加固支持服务：对于安全评估中发现的问题，结合实际情况，协助用户进行整改和安全加固，在加固过程中尽量减少对业务系统以及局域网应用的影响。加固对象一般包括主机操作系统、数据库系统、中间件、网络设备、安全设备等。

安全加固内容

（1）网络设备

OS 升级、帐号和口令管理、认证和授权策略调整、网络与服务加固、访问控制策略增强、通讯协议、路由协议加固、日志审核策略增强、加密管理加固、设备其他安全配置增强

（2）主机操作系统

系统漏洞补丁管理、帐号和口令管理、认证、授权策略调整、网络与服务、进程和启动加固、文件系统权限增强、访问控制管理、通讯协议加固、日志审核功能增强、防 DDOS 攻击增强、剩余信息保护、其他安全配置增强

（3）数据库

漏洞补丁管理、帐号和口令管理、认证、授权策略调整、访问控制管理、通讯协议加固、日志审核功能增强、其他安全配置增强

（4）应用程序

漏洞补丁管理、帐号和口令管理、认证、授权策略调整、通讯协议加固、日志审核功能增强、其他安全配置增强

服务范围

检测范围包括征集交换中心和联通云中心的全部网络设备、安全设备、主机、数据库及中间件。

服务周期

每季度一次，一年四次。

32、重保服务：在一些需提供重要时期安全保障服务，具体要求如下：

在攻防演习及重要时期(法定节假日、重大会议等)期间，提供安全专家值守服务，实时监测、分析、研判、处置各类网络攻击，保障业务系统安全稳定运行。以“事前准备、事中保障(值守、监控、应急、处置)、事后总结(复盘、提升)”的思路来保障用户信息系统的安全。

派遣安全服务工程师进行 7*24 或者 5*8 不间断的现场值守，以便发现安全问题时，可以及时进行处理。

33、安全培训服务：根据每季度安全评估的情况，每季度进行业务安全培训。培训内容包括办公人员安全意识、安全技能、信息安全体系框架、最新的安全热点事件分析等方向。

服务周期：每季度一次，一年四次。

34、安全管理制度梳理服务：根据信用平台运维的实际情况，对信用平台运维安全管理制度进行完善和补充。

服务周期：一年，按需提供。

(二) 服务质量：

35、服务级别：

指标	描述	单位	参考数据
事件平均响应时间	事件响应总时间/事件次数	分钟	≤30 分钟
事件按时解决率	事件按时解决次数/事件总次数×100%	百分比	≥90%
事件响应超时率	事件响应超时次数/事件总数×100%	百分比	<10%
事件平均用户满意度	事件平均用户满意度=Σ满意度/统计次数	百分比	≥90%
信息网络运行率	[(周期时长-网络节点中断时长-计划停	百分比	≥99%

	用时长) / (周期时长 - 计划停用时长)] ×100%		
关键应用系统运行率	关键应用系统运行率=[(周期时长-各关键应用系统中断总时长-各关键应用系统计划停用总时长) / (周期时长-各系统计划停用总时长)] ×100%	百分比	≥99%

36、响应程度：

所有软件、硬件、安全运维以及维保根据故障级别均提供 7*24 小时响应服务。

故障级别	响应时间	故障解决时间
I 级：属于紧急问题，其具体现象为：系统崩溃导致业务业务停止、数据丢失	30 分钟，2 小时内提交故障处理方案	12 小时内
II 级：属于严重问题：其具体现象为出现部分部件失效、系统性能下降但能正常运行，不影响正常业务运作。	30 分钟，2 小时内提交故障处理方案	24 小时内
III 级：属于较严重问题；其具体现象为：出现系统报错或警告，但业务系统能继续运行且性能不受影响。	30 分钟，2 小时内提交故障处理方案	48 小时内
IV 级：属于普通问题；其具体现象为：系统技术功能、安装或配置咨询，或其他显然不影响业务的预约服务。	30 分钟，2 小时内提交故障处理方案	5 天内

37、运维成果要求：

安全运维服务要求的交付物包括但不限于以下内容：

《信用平台资产统计列表》、《信用平台系统安全监测报告》、《信用平台系统漏洞扫描报告》、《信用平台系统网络协议分析报告》、《信用平台系统安全审计报告》、《信用平台系统渗透测试报告》、《信用平台 APP 渗透测试报告》、《信用平台系统加固指导建议》、《信用平台安全培训》、《信用平台系统安全评估总结报告》、《重要时期安全保障工作方案》、《重要时期安全保障工作总结》。

38、运行安全要求：

安全运维服务所使用的各类设备或工具具备合法的使用权，需要在采购人内部部署使用的设备或工具必须符合国家有关部门的要求，并符合政府部门系统的安全要求；

必须保证服务所使用的 WEB 扫描、主机漏洞扫描、渗透测试软件产品、安全加固系统等都具有在中国境内的正式合法使用权。

使用的安全运维工具满足以下功能要求：

序号	指标		规格参数	
1	基本要求		采用 B/S 设计架构，无须安装客户端，可通过浏览器远程对产品进行管理；	
2	授权许可请（提供含响应供应商盖章确认的承诺函）		服务期内服务工具需部署在本地，防止敏感数据泄露	
			提供无授权限制的资产发现功能授权许可，资产包括主机和网站。	
			提供无授权限制的主机漏洞扫描和漏洞管理功能授权许可。	
			提供无授权限制的网站风险与威胁监测功能授权许可。	
			提供无授权限制的内网和互联网蜜罐诱捕功能授权许可。	
			提供 150 个授权的服务器 Agent 安全功能授权许可。	
3	资产测绘和管理功能	资产发现探测	主机资产识别	支持自动扫描 IP 资产信息，包括：“存活 IP、设备厂商、操作系统、端口、应用、数据库、中间件、服务版本”等资产指纹特征；
4			网站资产识别	支持自动识别网站资产信息，包括：“中间件信息、web 框架信息、CMS&OA、程序语言”等指纹信息，支持爬取网站后台、ICP 备案编号、网站标题、网站返回码等属性；
5			二级域名扫描	支持二级域名扫描功能，输入一级域名进行一键扫描，通过搜索互联网数据，自动获取到该域名的二级域名、网站标题、解析 IP 地址；提供界面截图证明。
6			IP 反查域名监测	输入 IP 或者网段，通过搜索互联网数据，自动获取到 IP 对应的域名、url 链接、网站标题、返回状态码；提供界面截图证明。

7			网站资产相关度分析	通过爬取企业单位已知的网站页面，分析网页中是否包含企业单位相关的网站链接，从而发现未知网站；可配置“网段、域名”等命中规则，自动判断是否属于企业单位的网址；提供界面截图证明。
8		资产深度管理	下线资产监测	可及时发现未存活 IP、未存活端口以及访问延迟的网站，可查看未存活 IP 列表、未存活端口列表，可对未存活的资产进行移除操作
9			新增资产趋势	可按最近一周、最近一个月、最近一个季度可查新增的主机 IP 资产、网站资产，掌握资产新增趋势
10			资产认领	资产责任人可认领 IP、网站资产，可显示资产认领状态，未认领的资产无法进行编辑。
11	网站风险与威胁监测功能	网站风险监测	web 漏洞监测	支持网站漏洞评估能力，提供多种 Web 应用漏洞的安全检测，如“SQL 注入、跨站脚本、文件包含、CSRF、目录遍历”等网站脆弱性漏洞。
12			网站应用监测	支持监测网站的可用性、域名劫持等事件
13		网站威胁检测	黑链/篡改事件监测	高频率监测站点是否存在被黑客植入黑链、篡改的事件，系统需要保留植入黑链、篡改的快照页面，监测频率低至 5 分钟/次
14			全站敏感词事件监测	用户可对不同网站自定义不同的敏感词库，并对企业、单位的网站进行全站页面爬取，发现敏感词字眼。
15			敏感文件事件泄露监测	可监测发布到网上的 pdf、word、excel 文件中是否包含“身份证号、邮箱、手机号码、用户名/密码”等敏感信息，可在系统上查看泄露的信息以及敏感文件下载链接。提供界面截图证明。

16		主机漏洞管理	漏洞生命周期管理	支持漏洞跟踪管理，能够自动对漏洞状态进行处置，自动识别“新增、已修复、未修复”的漏洞，同时支持人工方式进行漏洞状态处置，以及编写漏洞备注，提供界面截图证明。
17		主机配置核查	配置核查能力	支持 20 种以上常见设备和应用的配置检查，包括操作系统、应用中间件、数据库。
18			配置核查支持类型	操作系统，支持 Windows2003/2008/2012/2016/2019/7/8/10/11；支持 linux（Centos、Redhat、suse 等）；应用服务，支持 Linux、Windows 下的 Apache、Weblogic、TOMCAT、Websphere、Nginx，以及 windows2003/2008/2012/下 IIS6/7/8；数据库，支持 Linux、Windows 下 Oracle8i/9i/10/11g、Mysql。
19	内网威胁监测功能	无侵入式全网病毒监测	trunk 部署病毒监测节点	无需在用户服务器上安装 agent，可通过 trunk 方式将诱捕能力发布到全内网各 vlan 网段，实现在全内网中部署大量高交互病毒监测诱饵，无侵入式部署不影响用户业务运行，同时极大提高黑客攻击病毒监测诱饵的概率。
20			跨三层监测探针扩展监测	探针支持 trunk 接入客户网络，可通过 trunk 方式将诱捕能力发布到全内网各 vlan 网段，实现在全内网中部署大量高交互病毒监测诱饵，同时支持软件和硬件版本的流量牵引探针。
21			病毒诱饵类型	支持高交互病毒监测诱饵，并可同时启用：“samba、ftp、ssh、rdp、telnet、mssql、mysql、mongoDB、postgresql、tomcat、weblogic、jenkins、redis、hadoop、memcache、solr、activeMQ、struts2、wordpress、nginx、jboss、joomla、smtp”等，以上服务须为真实应用服务，能够正常交互，欺骗攻击者，提供界面截图证明。
22		病毒处置功能	失陷主机微隔	不需要联动第三方设备、不需要在主机上安装 agent 脚本，就能对失陷主机进行网络隔离，隔离后失陷主机无法访问同网段以及其它网段 IP，防止失陷主机继续对东

			离	西向主机进行病毒传播、横向攻击等行为，提供界面截图证明。
23			取消微隔离	在 web 管理界面上，支持对已隔离的失陷主机取消微隔离，恢复失陷主机的网络访问权限
24	互联网威胁诱捕功能	蜜罐仿真	默认仿真蜜罐	支持至少 10 种可自定义 logo 和公司名称的仿真蜜罐，仿真蜜罐类型包括但不限于：“齐治堡垒机、启明堡垒机、深信服 VPN、泛微 OA、通达 OA、u8crm、wiki、mailcow、bbs 论坛、订单管理系统”。提供界面截图证明。
25			完全仿真蜜罐	支持通过反向代理的方式，接入用户自身搭建的应用系统，从而实现完全仿真真实业务系统，生成完全仿真蜜罐，提供界面截图证明。
26			智能克隆仿真蜜罐	支持智能克隆仿真功能，可以通过自学习的模式对真实业务系统进行遍历访问，形成机器记忆，与真实业务系统一样可进行前后端的数据交互，包括但不限于以下动态交互类型：“搜索查询、登陆验证、账号注册”等，高迷惑性地吸引攻击者攻击蜜罐，要求拟态仿真蜜罐系统为纯静态系统，无需额外提供蜜罐定制服务，提供由厂商盖章确认的拟态仿真配置过程和截图证明。
27		攻击吸引	引流防御	可将访问真实业务系统的流量引流到仿真蜜罐，使攻击无法命中真实业务系统，真正有效消耗攻击资源，并直接保护真实资产。提供界面截图证明。
28			互联网诱饵	可在 web 管理界面上自定义生成 github 互联网诱饵，可自定义添加蜜罐 IP 地址、github 项目说明、项目提交人信息、邮箱信息等内容，以便黑客可以从互联网上搜索到自定义信息内容，从而转向攻击蜜罐。
29		威胁感知	入侵攻击链检测	参考 MITREATT&CK，采用多种取证技术手段，还原黑客攻击入侵蜜罐的过程，形成黑客攻击链，攻击链检测包含：“针对蜜罐的探测扫描、渗透攻击、攻陷蜜罐、在蜜罐上安装后门远程控制程序、利用蜜罐进行跳板攻击”等入侵过程，提供界面截图证明。
30			还原攻击	支持还原攻击者的网络数据包，包括 icmp、tcp、udp 等协议的攻击包，可查看攻击者发起的具体攻击请求数据，

			数据包	比如 SQL 注入、XSS 攻击的 http 请求头部信息。
31			时间轴告警	支持时间轴告警分析：可根据基于告警时间/攻击类型/地理位置等对攻击行为进行筛查，其中攻击类型可分类为：“可疑访问、尝试登陆、端口扫描、攻击尝试、强力攻击、异常进程、暴力破解、登陆成功、命令执行、可疑文件、恶意文件、跳板攻击”等类型，对于攻击事件分析起关键作用。
32		攻击溯源	攻击者社交信息溯源	支持记录攻击者的“黑客社交画像”信息，包括社交账号、手机号、昵称、用户 ID、头像等信息，支持多种黑客社交画像，至少包括：QQ、百度、哔哩哔哩等 6 种不同类型的社交账号。提供界面截图证明。
33			攻击者唯一指纹溯源	可基于显卡成像参数、CPU 等硬件信息，计算攻击者唯一身份指纹，就算攻击者换了 IP 也可以通过该指纹确定攻击者。
34			设备指纹溯源	设备指纹溯源至少包括：操作系统信息、浏览器指纹、浏览器类型、mac 地址、设备厂商、屏幕分辨率、浏览器历史记录、计算机名。
35			威慑反制	可警告攻击者，比如灌输国家网络安全法、告知已获得相关溯源信息，发挥蜜罐威慑作用，使攻击者放弃后续的攻击行为；可灵活指定对某个攻击源 IP 地址发起威慑反制。提供界面截图证明。
36		攻击反制	拒绝服务反制	可使攻击者浏览器拒绝服务，可灵活指定对某个攻击源 IP 地址发起拒绝服务反制。
37			数据库诱骗反制	可使攻击者在连接数据库类模拟应用时，识别攻击者身份信息。包括但不限于：计算机名称、使用浏览器版本、浏览器历史记录、浏览器上记录的访问账号等。
38			木马诱骗	可使攻击者下载某个文件时，替换成木马文件，诱骗攻击者下载安装；可在 web 管理界面上灵活指定对某个攻

			反制	击源 IP 地址发起木马远控反制。提供界面截图证明。
39			漏洞攻击反制	支持一键扫描攻击源 IP 地址，探测攻击者主机的开放端口信息、弱口令、漏洞等。
40	服务器 Agent 安全防护功能	服务器 Agent 告警要求	主动威胁监测	在用户的服务器、业务系统上安装安全监控软件，主动监测恶意文件（webshell、病毒木马）、挖矿病毒、可疑进程、异常行为等，发现可疑的入侵事件，并实时将告警同步到服务平台，提供界面截图证明。
41			检测任务自定义	支持自定义下发服务器入侵检测任务，可指定扫描某个文件目录，以及实时检测变更或者新增的可疑文件
42		服务器 Agent 防御要求	恶意文件检测	恶意文件检测包含：Webshell 网马、病毒木马、攻击脚本、宏病毒文件等
43			挖矿病毒检测	支持检测挖矿病毒，识别挖矿程序文件、挖矿进程名称、进程号、运行参数、CPU 运行异常状态、网络连接状态、病毒程序打开的文件
44			网站篡改检测	可检测网站文件的篡改行为，包括：“创建、写入、修改权限、重命名、删除”等篡改行为。提供界面截图证明。
45	风险统计	报表管理	站点报表	支持生成各个主机的安全监测报表、各个网站的安全监测报表，报表类型包括：excel、word、html。
46			综合报表	支持生成主机安全监测综合报表、网站安全监测综合报表，报表类型包括：excel、word、html。
47			监测维度报表	支持生成某个监测维度报表，包括：敏感词事件报表、敏感文件事件报表、黑链事件报表、失陷主机事件报表、可用性事件报表、域名劫持事件报表、漏洞列表等各个监测维度的报表
48		监测中心	监测中心	展示整体安全监测概况，呈现主机资产信息以及主机监测雷达图，包含：“弱口令、可入侵漏洞、高风险漏洞”等概况；呈现攻击监测诱饵监测概况，包含：“失陷主机统计、攻击链统计、威胁趋势”等。

49			大屏展示	支持大屏展示功能，可视化呈现监测中心的数据，包括主机资产监测概况、攻击监测诱饵监测概况，大屏界面能够自动刷新监测数据，实时展示最新监测结果。
50	其他功能	多级用户管理	二级用户关联资产运维	一级用户可创建与管理二级用户，并可给二级用户关联资产。 多级用户管理，一级用户可查看与管理二级用户所有资产风险信息，二级用户只能查看与管理自身的资产风险信息。提供界面截图证明。
51		告警	微信告警	支持微信告警，提供界面截图证明。
52			邮件告警	支持邮件告警，可自定义告警邮箱
53		系统管理	用户管理	支持创建三类角色用户：管理员、操作员、审计员，支持账号安全策略设置，可设置密码最长天数、最小天数、登录失败锁定次数、登录超时时间、登录 IP 地址白名单等安全策略。

第十八条 项目运维过程中属于涉密区域的，运维人员应遵守如下安全要求：

1. 严禁将涉密区域的设备与互联网相连。
2. 严禁将笔记本电脑、手机终端等电子设备接入涉密区域的网络。
3. 严禁在涉密区域与互联网电脑之间交叉刻录光盘等操作。
4. 严禁在涉密区域使用 U 盘、移动硬盘等电子设备。
5. 未经审核登记，严禁将数据光盘、涉密移动硬盘等带出涉密区域。
6. 严禁使用涉密区域之外的计算机处理信用平台的敏感信息。
7. 严禁运维人员私自流转、复印、考核信息技术服务六处的内部文件、文档等。
8. 严禁在涉密区域安装、使用与工作无关的软件。

运维实施

第十九条 运维工作实行工作派单制度，任何技术支撑服务工作的变更应有派发工单流程。

第二十条 运维人员在对某项具体事务安排有异议的，应主动与信息技术服务六处相关负责人沟通达成一致意见，未经同意自行处理引起安全、数据丢失等问题的，由运维单位承担责任。

第二十一条 工作人员在运维工作过程中，要及时备份数据，如因失误、沟通不畅或实施流程不当等原因导致信用平台数据损坏、丢失或应用系统崩溃等严重问题，由运维单位承担责任。

第二十二条 对于阶段性安全整改工作，各运维单位应按照内蒙古自治区大数据中心的安全整改意见及时整改，如因整改不及时导致安全事故，应由运维单位承担责任。

第二十三条 接收工单和提交工单的运维工作人员应积极主动沟通、相互配合尽快解决问题。具体要求如下：

1. 运维人员应履行积极主动沟通义务，沟通方式不限于电话、微信等方式，

重要问题处理应注意保留过程痕迹。

2. 提交工单方应履行告知义务，被告知对象至少应包括信息技术服务六处相关技术工程师。

3. 接受工单方应积极主动与信息技术服务六处技术工程师、提交工单方沟通，如因工作推诿延误处理的，由接受工单方负责。

第二十四条 运维人员在工作过程中，如发现设备无法联接、无法登录、非法入侵、非法登录等任何异常情况，应第一时间告知信息技术服务六处相关负责人。

应急处理

第二十五条 各运维单位应设立值班人员制度，值班人员应 24 小时待机，确保对突发事件的及时响应。

第二十六条 运维人员在工作中如遇到紧急问题，应及时告知信息技术服务六处相关负责人，如因没有告知而导致重大数据丢失、毁坏等问题，应承担相应责任。

第二十七条 如遇紧急情况，相关运维单位在接到通知后，应在 1 小时之内到达现场，如在规定时限内未到现场应承担相应责任。

第二十八条 每个季度应进行一次异地备份数据的恢复演练，由云服务运营商和软件运维相关人员负责，并出具应急演练报告。

第二十九条 如遇紧急问题，责任单位应首先制定保护数据的方案，将数据损失降到最低，如因处理不当造成重要数据丢失、损失的由运维单位承担责任。

第三十条 如遇到突发性病毒蔓延、互联网入侵等重大问题，经信息技术服务六处相关负责人同意，相关运维单位应及时采取网络隔离、关网等紧急举措。

考核

第三十一条 各运维单位初始运维分值为满分 100 分，运维人员在实际工作中，如违反本制度相关规定将扣除相应分值。

第三十二条 运维人员如违反“运维范围、运维人员管理、运维职责、运维实施、应急处理”相关条款，每违反一条扣除所属单位 1 分，违反严重的扣 3 分。

第三十三条 本制度规定的运维分值年末得分将与本年度的运维费用关联。具体费用支付方法详见合同约定。