采购需求及最高限制单价

一、市级政务云规划

1.1市级政务云总体规划

北京市级政务云从2015年开始面向北京市市属行政事业单位的非涉密信息系统提供云计算服务，统一提供云计算、网络、云平台安全及相关配套服务。在政务数据汇聚、融合和公开等方面发挥重要作用。2020年为支撑智慧城市建设，特别是支撑智慧医疗、智慧教育行业发展，市级政务云服务范围扩展至特定行业领域。

市级政务云包括政务云和行业云两部分。政务云分为服务云、办公云、备份节点。服务云位于六里桥和通州两个数据中心，支撑公众服务类系统、大数据类业务系统运行；办公云位于通州，支撑政府内部办公类业务系统运行；备份节点位于密云，实现服务云和办公云的云主机备份、应用系统双活等业务需求。目前我市规划了2个行业云服务医疗健康、终身教育行业。行业云管理行业信息系统和行业业务数据，是我市智慧城市建设的重要组成部分，也是我市信息化关键基础设施之一。

政务云与行业云在运行、管理、安全上坚持统一标准体系、统一监管体系和统一评估体系，实现多云统一管理体系；构建全市统一的政务云数据专区，实现多云数据的汇聚、管理和共享；构建全市统一安全保障和应急监测体系，实现多云节点和全市入云系统的安全监测和应急预警。

市级政务云由市政务和数据局牵头规划和建立统一管理体系，政务云（服务云、办公云、备份节点）由市政务和数据局管理和推广应用。行业云（健康云、教育云）由相关行业主管部门（市卫生健康委、市医保局、市教委）负责组织建设运营和管理推广。

市级政务云共享一套服务目录（含单价），享受相同的服务水平。

1.2政务云（服务云）规划

1.2.1服务云基础环境现状

1.2.1.1 电子政务网络现状

北京市政务网络划分为政务内网和政务外网两部分。

图 1 北京市政务网络总体架构图

北京市电子政务外网是指北京市政府统一建设的数据通信专用网络，覆盖市人大、市委、市政府、市政协、市高院和市检察院和 16 个区政府、经开管委会、市属委办局、人民团体、事业单位及其它部门，并与国家和区级政务外网互联互通，主要满足市级政务部门履行职能的网络通信需要。该专用网络由光缆网、政务外网传输网和政务外网 IP 网组成。网络可承载数据、视频会议和图像监控等业务。

电子政务外网包括 10 网段纵向业务 IP 地址和 172 网段横向共享业务 IP 地址，其互访规则为：允许委办局内部的业务系统地址互访，禁止不同委办局的业务系统地址互访；允许共享域内业务系统地址互访，以及委办局业务系统和终端地址对共享域内地址的访问，禁止共享域地址对委办局业务系统地址的主动访问。

此外，我市已建成市级移动政务管理平台实现了三大运营商的统一接入，各种移动政务应用可基于两个平台快速部署实现。

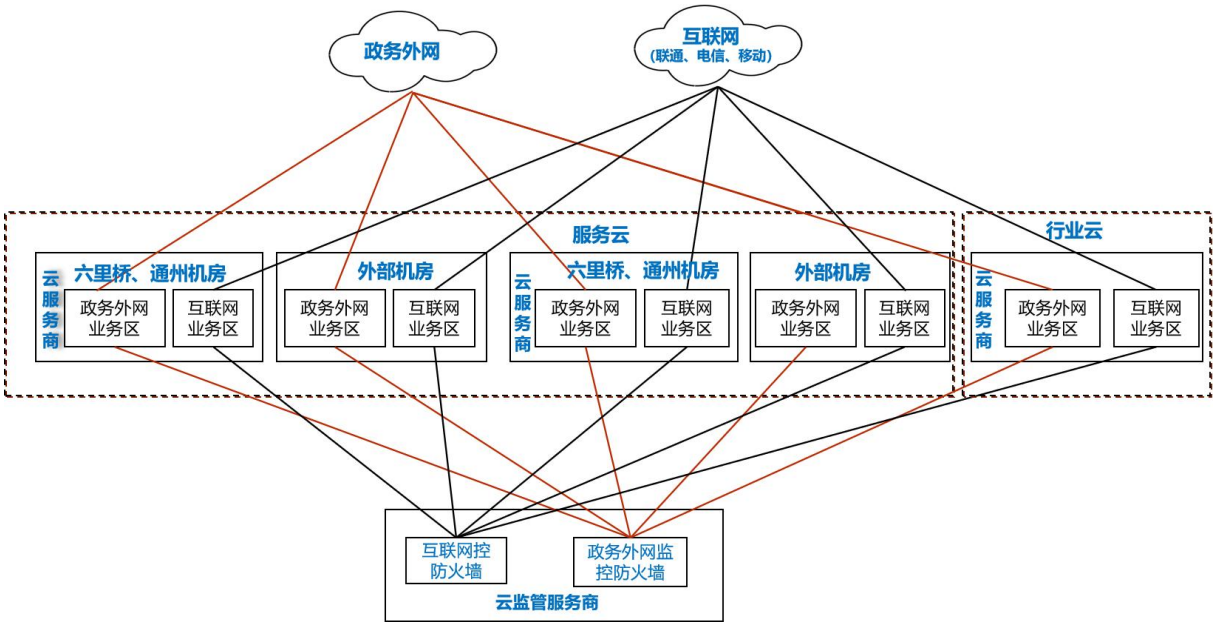
近期，遵照《国家电子政务外网安全接入平台技术规范》的电子政务外网安全接入平台（以下简称“安全接入平台”）已投入使用，该平台采用 IPSec VPN（Internet Protocol Security Virtual Private Network 基于因特网安全协议的虚拟专用网）、SSL VPN（Security Socket Layer Virtual Private Network 基于安全套接层协议的虚拟专用网络）等技术，为不具备专线接入条件的各级政务部门、企事业单位、移动办公人员、现场执法人员等，提供通过互联网、移动通信网等公众网络安全接入政务外网的服务，满足北京市各级政府部门移动办公、现场执法等移动电子政务网络需求。

1.2.2特殊要求

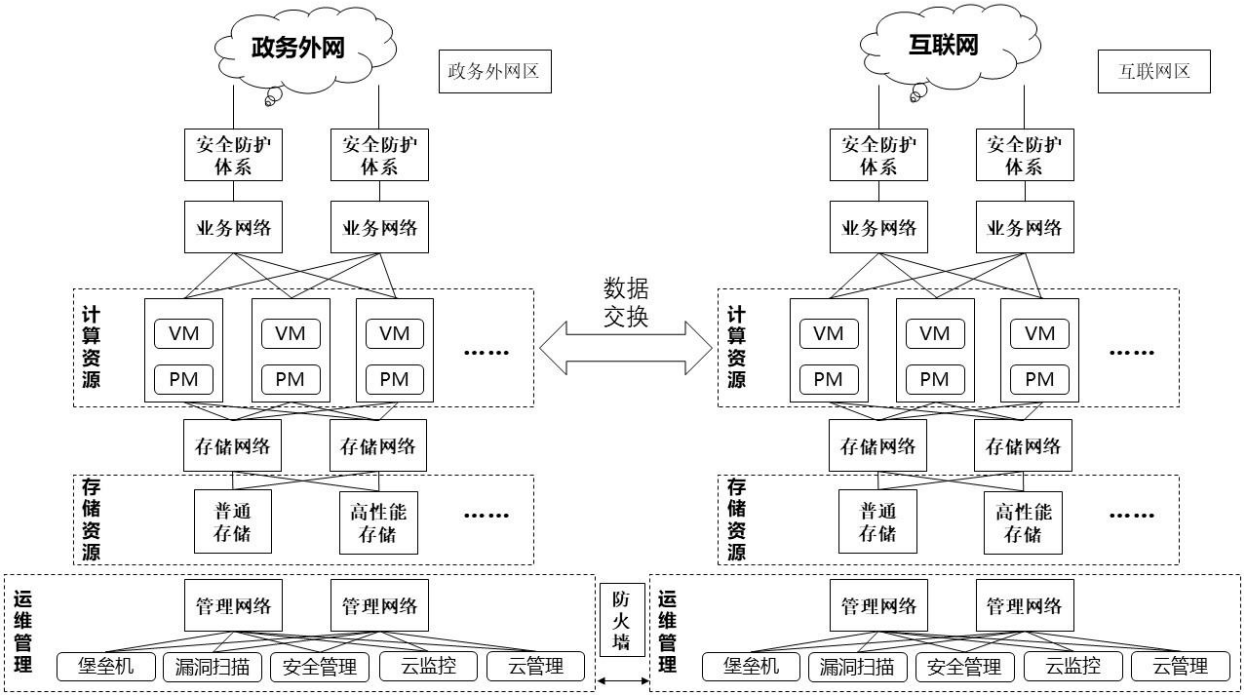
1.2.2.1 服务云总体部署示例

各云服务商云平台网络相互独立。下图是本期工程对云服务商提供的参考方案，各云服

务商可以参考并提出优化方案。



云平台按电子政务网络安全要求划分为电子政务外网和互联网两个区域，两区域间设置安全数据交换区实现不同区域间的数据安全交换。



政务外网区和互联网区之间应隔离。内部业务区域为每个政务云使用单位划分不同的虚拟专有云（VPC）。

1.2.2.2 服从监管的要求

服从监管要求	云服务商需接受云综合监管服务商的监管要求，并提供相关计算、存储、网络等资源监控及安全接口。
	管理单位负责引导、督促、协调各政府部门应用系统入云，并对服务过程进行整体把关。用户在与云服务商签订服务合同前，所选云服务商需经过管理单位

	确认同意，云服务商应免费配合云服务管理单位的相关审核工作。
	云服务商应按照管理单位要求开放云计算相关平台接口。云服务商需接受包括云综合监管服务商在内的第三方检测、调解，对云综合监管服务商的合理要求需无条件给予配合。
服从管理要求	云服务商应在不影响云平台正常运行的情况下配合云租户选择的第三方安全服务商开展业务系统的安全测试及日常安全运维工作。

1.3行业云规划

行业云由行业主管部门统筹规划，按照购买服务方式，面向特定行业提供服务。

按照全市推进大数据行动计划要求，要加快行业云建设，推动医院、学校数据上“云”的有关要求。行业云采用混合云服务模式，部署行业业务系统，为社会机构（如医院、社区、学校等）非政府机构的系统提供服务，存储社会机构的业务数据，并实现与市大数据平台交互数据。各节点通过专线连接。行业云将参考政务云的建设运营经验，按照我市大数据行动计划相关要求规划，通过购买服务方式实现运营。

通过本次采购确定的云服务商将负责建设健康、教育行业云节点，为健康、教育行业应用及与相关社会化应用等提供云计算服务。

1.3.1健康云规划及特殊要求

1.3.1.1 健康云规划

健康云由行业主管部门统筹规划，按照购买服务方式，面向医疗卫生行业提供服务。

医院业务对系统可用性、可靠性和业务连续性有极高的要求。通过双节点双链路设计，来保证医院业务系统的高可用、高可靠、快速响应，满足系统应用双活需求。

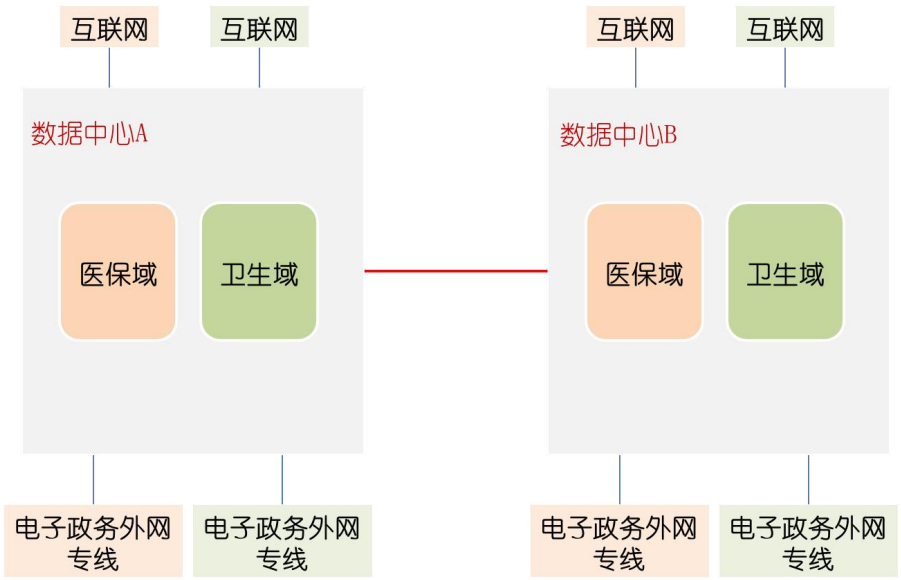
健康云采用混合云服务模式，为社会机构（如医院、社区等）非政府机构的系统提供服务。

1.3.1.2 特殊要求

健康云行业节点应按电子政务网络安全要求划分为电子政务外网和互联网两个区域，两区域间设置安全数据交换区实现不同区域间的数据安全交换。

同时，根据国家医疗保障局下发的《医疗保障信息平台云计算平台规范》要求：由于医疗保障业务的重要性和复杂性，按照专有、独享原则，建设医保云专区，且须规划独立设备、专有网络、专属安全、专属 PaaS 资源等，同时上述资源须能支撑医保业务中台的技术要求。

医保域专区应符合国家医疗保障局下发的《医疗保障信息平台云计算平台规范》（YB-XJ-A01-2019）、《医疗保障信息平台应用系统技术架构规范》（YB-XJ-B01-2019）、《医疗保障信息平台建设指南》、《全国医疗保障系统核心业务区骨干网络建设指南》（医保网信办〔2019〕40 号）、《医疗保障核心业务区网络安全接入规范》（YB-XJ-AQWL.01-2019）。



1.3.2教育云规划及特殊要求

1.3.2.1 教育云规划

教育云参照政务云建设运营模式，按照北京市智慧城市总规、控规要求，部署教育领域相关业务系统，采取购买服务的方式为各类教育教学单位提供服务。教育云主要服务于市级教育系统，主要面向市属高校、直属单位开放使用，包括各类教育教学、管理信息系统以及对外服务系统等（属于市委教育工委、市教委的相关信息系统统一使用市级政务云）。

1.3.2.2 特殊要求

1.基本要求

教育云服务商应同等满足政务云服务商的所有技术和管理要求。

2.网络接入要求

教育云服务商除具备满足业务需要的互联网接入外，应具备北京教育信息网接入，可满足链路带宽上限不低于 40Gbps，实际数据带宽可根据业务需要动态配置。具备中国教育和科研计算机网（CERNET）接入，物理链路带宽不低于 10Gbps，实际数据带宽根据业务需要动态配置。应具备部署政务外网的条件（提供接入设备和预留管线空间）。

3.国产化要求

提供的教育云服务要满足使用单位提出的信创环境运营需要，国产自主可控的软硬件产品比例不低于 40%，并为使用单位提供国产化迁移适配的测试验证环境。

4.接口要求

教育云服务商应向用户单位提供云管理控制台，总览日常运行情况，并实现相关资源配置的线上办理。同时，教育云服务商应无条件开放其云计算平台的接口数据，做好对接工作，包括且不限于：资源配置接口、资源同步接口、资源监控告警接口、资源性能监控接口、消息通知接口等，并接受市级的安全监管和应用与网络绩效监测。

5.教育云扩展服务要求

可提供满足教育系统用户需要的共性服务能力，包括且不限于 IaaS、PaaS、SaaS 层级的服务。

6.业务主管部门要求

严格落实市委教育工委市教委的各项相关要求。

1.4本次征集范围和期限

本次市级政务云征集范围包括服务云、健康云、教育云。入围后须与征集人签订框架协议，本次协议期自框架协议签订之日起两年。

1.5本期总体要求和运营模式

1.5.1总体要求

1.符合《基于云计算的电子政务公共平台顶层设计指南》、《关键信息基础设施安全保护条例》、国家网络安全等级保护第3级相关要求、《云计算服务安全评估办法》、《信息安全技术 云计算服务安全能力要求》（ΓB/T 31168–2023）、《信息安全技术云计算服务安全指南》（ΓB/T 31167–2023）、《云计算关键领域安全指南ς4.0》、《政务云平台建设技术要求》（ΔB 11/T 2169–2023）》及国家主管部门发布的其他标准规范要求。

2.提升云平台对公众服务系统的支撑能力，确保其具备支持高并发和大流量业务应用的服务能力；同时支持云服务商发展云平台ΠααΣ层和ΣααΣ层服务能力。

3.建设基于数据分析的云平台安全管理体系和运维管理体系，为入云系统的稳定性和持续运行，提供全面支撑，为使用单位提供入云系统运行数据的展示能力，确保为使用单位提供的各项服务可监控可管理。

4.建设市级政务云统一管理体系，实现统一标准体系、统一监管体系和统一评估体系、统一评估，构建全市统一的政务云数据专区，实现多云数据的汇聚、管理和共享；构建全市统一安全保障和应急监测体系，实现多云节点和全市入云系统的安全监测和应急预警。

5.促进市区两级共享政务云服务目录，促进区级政务云采购和运营规范化。

1.5.2运营模式

1.云服务商提供组成云平台所必需的软硬件设备，搭建和部署云平台网络，承担建设和运行维护成本，确保互联网带宽的稳定供应。政务外网由服务云管理单位提供。

2.管理单位根据服务云发展的需要，建立云服务商的评估和更新机制，实现云服务商的动态调整、优胜劣汰。

二、云平台建设要求

响应人应根据采购需求对方案进行优化。

2.1云平台能力总体要求

2.1.1云平台技术要求概述

1.云服务商完成云平台本身的网络搭建和部署；互联网及带宽由云服务商提供；政务外网由政务外网管理单位提供路由（带宽足够满足需求），云服务商完成政务外网接入。

2.云计算平台应按照《国家政务信息化项目建设管理办法》（国办发〔2019〕57 号）、《信息安全技术 信息系统密码应用基本要求》（GB/T39786-2021）等国家密码管理相关文件及标准规范要求，进行密码保障能力建设，包括但不限于物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全、密钥管理等层面内容，并为云上系统密码应用及改造提供必要的服务能力。

3.在本轮服务期内，所建设的政务云平台需符合国家及我市信创工作总体要求，提供云服务要满足用户单位提出的信创改造需求。

4.云计算平台应提供完善的接口，包含但不限管理平台、虚拟化平台、用户服务平台、网络、安全、存储系统等标准接口，具备纳管相关物理设备及系统的能力，同时应具备与政务云监管平台和市级政务云运行数据采集管理平台对接的能力。

5.云服务商通过云计算平台框架，为客户的大数据解决方案，构建完善、统一、高度集成的技术架构，对平台沉淀的数据进行整合、分析，并满足包括离线计算、实时分析、流计算等场景在内的大数据应用需要。提供全方位的大数据安全防护的能力，包括多租户的隔离及面向互联网应用的完备的安全防护体系。

6.云平台某宿主机宕机时，其他宿主机应能代替宕机宿主机功能，实现流量无缝切换。

7.机房部署的云平台，应使用连续、独立的机柜，对租赁区域封闭隔离，确保空间独立专享。云平台的云管平台、计算资源池、网络设备、安全设备、网络链路应确保独立专享。不允许云服务商与区级政务云、公有云或其他云平台构建混合云进行统一的资源调度管理，行业云可由管理单位自主规划资源调度管理范围。

8.未经数据所有单位同意，使用单位业务数据不得离开市级政务云机房。

9.实现最小访问权限、终端数据隔离、应用资产隐藏。

2.1.2云平台可用性要求

云服务商提供的云平台整体可用性不低于 99.99%，数据可靠性不低于 99.9999%，同时提供测算依据。

2.1.3数字化运维的管理要求

云服务商应提供可以独立部署的自动化运维平台，支持自动化巡检、云平台补丁自动分发、批量远程脚本执行等功能，及自动告警、运维即时通讯工具、告警升级、工单与故障报告自动分发和认领等功能。

云服务商需要能够对云基础设施、平台软件和业务应用系统提供集中运维管理、监控，包括虚拟化、服务器、存储、网络、安全等，所提供的服务应能够可监控可量化，能实现云资源和流量的监控和分析，实现资源使用情况可视化，为使用单位提供可定制的业务可视化能力，定位事件、问题和故障，实现事前预测及告警、事中及时处理和事后可审计。

2.2云管理平台要求

2.2.1云管理平台要求

1.具有自主知识产权且具有大规模部署案例的国产云平台产品；

2.通过 SDN 控制器实现对网络设备的自动化编排，云平台支持 VxLAN、VLAN 组网模式；

3.云平台管理节点须支持集群部署，可平滑升级扩展；

4.云平台能够提供自服务门户，便于使用单位申请、管理云资源；

5.提供统一事件或故障告警展示中心，直接反映事件或故障发生的时间、触发条件、内容、级别，可对告警事件进行状态确认；

6.应使用非 OEM 的成熟国产商用产品；

7.云平台的软件定义服务能力，能够实现云管理平台对用户计算资源、网络资源、存储资源、安全资源自动化调度及管理；

8.云管理平台能够根据云管理单位要求、使用单位要求进行定制开发，并应至少具备以下扩展能力：提供云服务商运维管理功能、用户运维门户定制化、申请审批等流程定制化、报表定制化、云资源使用监控和分析、应用系统运行监控、第三方产品管理定制化等；

9.提供大屏、中屏、移动端展示能力，支持用户定义多种不同的展示内容，支持容量、性能、资源统计、告警等对象的自定义大屏展示，且可以定义每个内容的不同呈现形式。

云服务商应在响应文件中描述云管理平台方案,描述云管理平台服务功能和定制开发能力，并承诺在此后按照云管理单位要求、使用单位要求进行定制开发。

2.2.2服务能力扩展要求

服务能力扩展要求	云服务商应具备为使用单位提供基础软件支撑服务、云迁移服务、安全防护服务、安全检测监测、CDN 加速、对象存储和数据备份服务。
	云服务商应在服务期限内，增强 PaaS 层的服务能力，具备提供云数据库、云缓存、消息队列服务等 PaaS 服务的能力，具备支撑市级大数据平台的能力，提供标准、统一的数据接口供使用单位和管理单位调用。云服务商应基于云平台技术特点，提供业务系统到 PaaS 服务的迁移规范，指导业务系统适应 PaaS 应用的改造工作。
	云服务商应及时跟踪云计算发展趋势，特别是业界发生云安全相关事件时，及时报告给管理单位参考。

2.2.3多云节点管理要求

同一云服务商的不同云节点间应通过光纤直连，实现数据高速传输，满足云资源（计算、存储、网络等）统一管理、运维，云主机互备、应用系统双活等业务需求，按照统一业务流程、统一监管、统一接口标准，形成统一的政务云管理和技术体系。技术要求如下：

1.同构云管理平台要求

Portal：人性化 portal 设计、完善 portal 管理功能、可以根据角色定义不同的视图；

资源统一管理：能够管理同构平台中的所有设备和资源信息、能够自定义资源信息的 CI 项、支持 ESXI 管理、虚拟机模板管理；

总体资源视图：能够以图表的形式展现出同构平台中所有资源信息（计算资源、存储资源和网络资源等）、能够分项展示出各个资源详细信息（每个虚拟化平台、每个存储和每个机器信息等）、可以按多个维度进行汇总并导出 excel；

逻辑拓扑视图：自动根据资源定义展现出同构平台的某个环境逻辑视图和环境信息、功能区域可以增删改、逻辑视图可以根据资源变化自动更新、可以点击视图某台机器显示详细信息和登录窗口；

资源变化趋势视图：能够统计单位时间内资源变化趋势、如果资源变化较大到达阀值进行预警；

资源信息检索、可以自定义 CI 项，进行精确或模糊查询、查询结果可以导出 EXCEL；

运维日历：可以显示每个环境的任务安排、可以申请使用环境，审批，并自动标注；

自动化部署：自动根据申请单选择相应模板部署虚拟机并配置 IP、预留脚本接口，自动配置系统参数和安装软件、IP 资源自动管理，自动分配和回收。

2.服务目录

服务目录内容：服务目录的服务项可以进行增删改、服务目录属性管理；

工作流程：工作流转过程可以自定义，自定义分级，自由调整工作流节点，自定义多级审批、并行和串行的工作流程、实现系统服务层的接口或其他服务能力进行调用，实现工作流程中的任务自动化处理或半自动化处理；

服务流程自动监控流转：支持流程自动监控和流转、任务流转自动触发 RTX 或邮件通知；

辅助操作：人性化设计，任务负责人可以支持延期、跳过和终止等操作。

3.工单管理

工单处理：支持自动分配和手工分配工单、可以自动分发到角色定义人员、自动通过 RTX 或邮件通知相关人员；

工单状态：自动显示工单流程状态和处理状态、用户登陆后自动发出提示、超期自动警告、工单完成后对资源状态的自动变化，与流程的集成；

工单记录：自动记录工单处理过程、可以显示工单流转过程、可以查询工单状态；

工单统计分析：自动汇总各项工作任务量、自动汇总部门内支持人员工作量、以报表形式展现任务量和工作量。

4.报表管理

可按照项目、部门统计环境信息（总量、已用、未用和变化趋势）、可按照项目、部门统计工作量信息、可按照项目、部门统计工单信息。

（1）工单报表

能够按照任务类型和人员对工作量的进行统计分析，支持对工单中各业务类型用柱状图或是饼图等直观图形体现，业务数据直观明了，通过数据报表功能，能够清楚的了解每个员工的工作状态；

（2）资源报表

能够以图表形式展示出当前环境的计算资源、存储资源、ip 资源和每个虚拟化平台资源信息；并且能够按照设备类型、资源用途和部门等维度进行分类汇总资源信息。

5.信息发布

系统需要有完善的信息发布管理平台，建立信息发布平台，可以发布公告、知识（视频、PPT 等）、通知并辅助整个系统完成服务目录和工单流程过程，是业务流程过程中的消息能够及时导致个人的邮件和 RTX 通信工具；

（1）能够发布通知和公告信息；

（2）能够配合系统发布环境使用信息；

（3）能够支持业务流转中产生的消息和任务通知。

6.知识库

自动收录日常工作中遇到问题，自动关联相似问题，实现问题快速处理；知识库结构合理、分类清晰和内容完整；能够自动关联相关问题的处理过程；能够人工审核和手工维护；免登陆问题查询；可以分享到首页。

7.权限管理

系统需要有完善权限管理：

（1）够集成用户域控的用户管理并根据系统需求定义角色；

（2）能够设置定义角色、权限和批量管理用户；

（3）分级管理，用户及权限，权限可细化到功能点或菜单。

8.平台管理

包括界面管理、功能管理、菜单管理。

9.外部接口

提供集成 RTX 接口，可以给任务人发消息和通知；

提供集成邮箱接口，可以给任务人发消息和通知；

提供预留 OA 系统接口。

10.字典管理

提供完善的字典管理功能、可以根据字典定义系统设置。

11.角色管理

提供能够集成域控的用户管理、能够设置定义角色和权限、每个角色都有定制的登录显示视图、能够批量管理用户、分级管理，用户及权限，权限可细化到功能点或菜单。

2.2.4云平台数据开放要求

云服务商应按照云管理单位提出的接口要求和接口标准完成云管理平台与云管理单位指定的第三方监管平台（包括但不限于政务云监管平台、市级政务云运行数据采集管理平台）的对接，并在响应方案中响应该接口要求。

主要接口内容应至少包括：

（1）运行状态类相关接口

对云平台运行时的状态参数进行持续监测，如云计算平台状态、客户服务状态以及虚拟机和虚拟网络状态等。

（2）业务服务类相关接口

获取云平台业务服务相关数据，如入云业务系统、云平台资产、租用服务器等信息。

（3）安全审计类相关接口

对云平台的安全审计日志进行收集，如云计算平台系统操作日志审计、客户业务操作日志审计等。

（4）重大变更类相关接口

通过对云平台变更时的状态参数进行持续监测，如云计算平台内核、内存以及带宽等变更情况。

（5）告警类相关接口

对云平台的告警相关数据进行持续监测，如安全事件告警、运行故障告警以及性能告警等。

能够支持多种安全监管接口技术要求，以提供相关安全监管数据。安全监管接口类型包括网络流量接口、网络协议接口、虚拟机接口和应用程序编程接口（API）等。

（6）网络流量接口

云服务商应在云平台边界处支持按需引流，云计算平台的边界交换机、路由器应支持将所有或部分指定的边界流量牵引至云平台安全运行数据采集汇聚方的设备，应支持镜像端口引流。云服务商应确保网络流量在本地保存，不低于一个月。

（7）网络协议接口

应开启服务器、网络设备、安全设备等的 Syslog 接口，通过网络将 Syslog 消息发送到指定 Syslog 接收服务器。

应开启设备的 SNMP 协议管理接口，对部分指定网络设备进行监管。

应分配合适的以太网接口，保证网络可达并能监测到监管云平台相关设备设施。

（8）虚拟机接口

支持云计算平台上传虚拟机镜像并生成虚拟机实例。

（9）应用程序编程接口（API）

支持“查询-响应”和“触发器”两种方式。通过“查询-响应”的方式向云服务商查询云计算平台各种属性，例如云计算平台状态、云客户配额、虚拟机状态等。“触发器”方式，对外提供 API 服务接口，云服务商自身发生重大变更事件时“触发”上报机制。

2.2.5云平台运行数据管理和汇聚要求

云平台运行数据是指云平台运行过程中产生的资产数据、环控数据、边界全流量数据，

网络协议数据、日志数据、监控数据等。云服务商应按照按要求提供云平台运行数据、采集接口及必要的设施，保障按时提供数据、数据完整性达到95%。响应人应在平台建设完成后1个月以内实现按以下描述的方式提供数据，因特殊原因无法实现传输的数据，应采用人工方式按要求保质保量提供数据。云平台运行数据质量将纳入云服务商综合评估。

（1）资产数据

数据分类	中文名称	定义	数据类型	数据格式	更新周期
资产数据	资产分类	资产分类代码	字符型	an4	周
	设备名称	物理设备名称	字符型	an1..100	周
	序列号	设备唯一S/N号	字符型	an1..100	周
	设备品牌	品牌名称	字符型	an1..100	周
	设备型号	设备型号名称	字符型	an1..100	周
	主机规格	主要硬件规格	字符型	an1..400	周
	内部IP	内部IP地址	字符型	an7..40	周
	云服务商	云服务商	字符型	an4	周
	网络类型	连接网络	字符型	an4	周
	运行状态	运行状态	字符型	an4	周
	启用日期	开始使用日期	字符型	an10	周
	撤出日期	停止使用日期	字符型	an0..10	周
	所在机房	设备所在机房	字符型	an4	周
	机柜编号	设备所在机柜编号	字符型	an1..100	周
	机柜位/U标	设备所在机柜中位置	字符型	an1..100	周
	功率	设备功率	数值型	n1..10,2	周
	电源类型	电源类型	字符型	an4	周
	管理类型	管理类型	字符型	an4	周
	管理单位	设备管理单位名称	字符型	an1..200	周
	管理人	设备管理人姓名	字符型	an1..100	周
	业务系统名称	运行业务系统名称	字符型	an1..200	周
	管理人联系方式	管理人联系电话	字符型	an1..20	周
	备注	其它内容	字符型	an0..800	周

（2）环控数据

云服务商投资建设的机房环境相关设备，应对接云机房环控系统，并提供相应的环控数据。

数据分类	中文名称	定义	数据类型	数据格式	更新周期
温湿度传感器	机房	设备所在机房	字符型	an4	5分钟
	所在位置	传感器在机房具体位置	字符型	an1..100	5分钟
	温度	温度	数值型	n1..6.2	5分钟
	湿度	湿度	数值型	n1..6.2	5分钟
发电机	发电机编号		字符型	an1..50	5分钟
	所在位置		字符型	an1..100	5分钟
	故障状态	故障状态	字符型	an1..100	5分钟

	油位容量	油位容量	数值型	n1..6.2	5 分钟
	运行状态	运行状态	字符型	an1..100	5 分钟
ADU 电池监控模块	编号				5 分钟
	机房	设备所在机房	字符型	an4	5 分钟
	所在位置		字符型	an1..100	5 分钟
	电流	电流	数值型	n1..6.2	5 分钟
	总电压	总电压	数值型	n1..6.2	5 分钟
	后备时间	后备时间	数值型	n1..6.2	5 分钟
UPS	机房	设备所在机房	字符型	an4	5 分钟
	所在位置		字符型	an1..100	5 分钟
	输入频率	输入频率	数值型	n1..6.2	5 分钟
	环境温度	环境温度	数值型	n1..3.2	5 分钟
	环境湿度	环境湿度	数值型	n1..3.2	5 分钟
	输出频率	输出频率	数值型	n1..6.2	5 分钟
	电池总电压	电池总电压	数值型	n1..6.2	5 分钟
	电池总电流	电池总电流	数值型	n1..6.2	5 分钟
	电池温度	电池温度	数值型	n1..6.2	5 分钟
	电池后备时间	电池后备时间	数值型	n1..6.2	5 分钟
	电池剩余容量	电池剩余容量	数值型	n1..3.2	5 分钟
	电池总电流	电池总电流	数值型	n1..6.2	5 分钟
	UPS 供电状态	UPS 供电状态	字符型	an1..50	5 分钟
	UPS 运行状态	UPS 运行状态	字符型	an1..50	5 分钟
	电池运行状态	电池运行状态	字符型	an1..50	5 分钟
	市电输入告警状态	市电输入告警状态	字符型	an1..50	5 分钟
	电池告警状态	电池告警状态	字符型	an1..50	5 分钟
采集器	机房	设备所在机房	字符型	an4	5 分钟
	所在位置		字符型	an1..50	5 分钟
	漏水状态	漏水状态	字符型	an1..50	5 分钟
	红外状态	红外状态	字符型	an1..50	5 分钟
	继电器输出	继电器输出	字符型	an1..50	5 分钟
列头柜	机房	设备所在机房	字符型	an4	5 分钟
	机柜编号	机柜编号	字符型	an1..50	5 分钟
	A 相电压	A 相电压	数值型	n1..6.2	5 分钟
	B 相电压	B 相电压	数值型	n1..6.2	5 分钟
	C 相电压	C 相电压	数值型	n1..6.2	5 分钟
	A 相电流	A 相电流	数值型	n1..6.2	5 分钟

	B 相电流	B 相电流	数值型	n1..6.2	5 分钟
	C 相电流	C 相电流	数值型	n1..6.2	5 分钟
	A 相负载率	A 相负载率	数值型	n1..3.2	5 分钟
	B 相负载率	B 相负载率	数值型	n1..3.2	5 分钟
	C 相负载率	C 相负载率	数值型	n1..3.2	5 分钟
电量仪	机房	设备所在机房	字符型	an4	5 分钟
	所在位置		字符型	an1..100	5 分钟
	总有功电度量	总有功电度量	数值型	n1..6.2	5 分钟
	总无功电度量	总无功电度量	数值型	n1..6.2	5 分钟

（3）网络协议数据

数据分类	中文名称	定义	更新周期
tcp	时间戳	绝对时间 第一个包的时间	5 分钟
	时间	入库时间	5 分钟
	采集引擎		5 分钟
	节点名称		5 分钟
	节点类型		5 分钟
	源 IP		5 分钟
	源端口		5 分钟
	目的 IP		5 分钟
	目的端口		5 分钟
	是否建立连接	1 为建立连接，三次握手成功；0 未建立连接	5 分钟
	连接次数		5 分钟
	会话总长	整个会话的 lenth 求和	5 分钟
	应用层协议		5 分钟
HTTP/HTTPS	时间戳	绝对时间	5 分钟
	时间	入库时间	5 分钟
	代理 IP		5 分钟
	节点名称		5 分钟
	节点类型	政务外网 互联网 重要信息系统	5 分钟
			5 分钟
	源 IP		5 分钟
	源端口		5 分钟
	目的 IP		5 分钟
	目的端口		5 分钟
	主机		5 分钟
	请求全路径	Host+路径	5 分钟
	返回码	字符型	5 分钟
	真实 IP	x-forwarded-for	5 分钟
	COOKIE		5 分钟
	请求方法	Post，get 等	5 分钟

	http 类型	取值 1 为只有请求，2 为只有响应，3 为请求响应皆有	5 分钟
	请求头	完整请求头部信息	5 分钟
	响应头	完整响应头部信息	5 分钟
	来源页面		5 分钟
	响应服务器	Ngix ，Apache 等	5 分钟
	请求内容		5 分钟
	响应内容		5 分钟
	入流量		5 分钟
	出流量		5 分钟
DNS	时间戳	绝对时间	5 分钟
	时间	入库时间	5 分钟
	代理 IP		5 分钟
	节点名称		5 分钟
	节点类型		5 分钟
	源 IP		5 分钟
	源端口		5 分钟
	目的 IP		5 分钟
	目的端口		5 分钟
	查询域名		5 分钟
	DNS 类型	1 为只有请求 2 为只有响应，3 为请求响应皆有	5 分钟
	查询类型	A、AAAA、PTR 等	5 分钟
	请求类型	0，1，2，5	5 分钟
	返回码	0，1，2，3 等	5 分钟
	请求资源记录类型	IN、Chaos 等	5 分钟
	响应	Standard query response 0x04d2A 198.41.0.4	5 分钟
	资源记录被缓存的秒数		5 分钟
	域名级别		5 分钟
	响应数据		5 分钟
	响应数据长度		5 分钟
	域名长度		5 分钟
	资源记录数		5 分钟
	请求域名数量		5 分钟
	顶级域名		5 分钟
	额外资源记录数		5 分钟
	授权资源记录数		5 分钟
	响应的 ip 总数	解析结果的 IP 个数	5 分钟
smtp	时间戳	绝对时间	5 分钟
	时间		5 分钟
	代理 IP		5 分钟

	节点名称		5 分钟
	节点类型		5 分钟
	源 IP		5 分钟
	源端口		5 分钟
	目的 IP		5 分钟
	目的端口		5 分钟
	邮件类型	1 为发邮件,2 为发邮件时的认证	5 分钟
	用户	邮箱账户	5 分钟
	是否加密		5 分钟
pop3	时间戳	绝对时间	5 分钟
	时间		5 分钟
	代理 IP		5 分钟
	节点名称		5 分钟
	节点类型		5 分钟
	源 IP		5 分钟
	源端口		5 分钟
	目的 IP		5 分钟
	目的端口		5 分钟
	用户	邮箱账户	5 分钟
	类型	1 为收取邮件,2 为收邮件时的认证，每次收取都要认证。	5 分钟
	是否加密		5 分钟
imap	时间戳	绝对时间	5 分钟
	时间	入库时间	5 分钟
	代理 IP		5 分钟
	节点名称		5 分钟
	节点类型		5 分钟
	源 IP		5 分钟
	源端口		5 分钟
	目的 IP		5 分钟
	目的端口		5 分钟
	用户（账户）	邮箱账户	5 分钟
	是否加密		5 分钟
FTP	时间戳		5 分钟
	源 IP		5 分钟
	源端口		5 分钟
	目的 IP		5 分钟
	目的端口		5 分钟
	传输模式		5 分钟
	文件名字		5 分钟
	文件 md5		5 分钟

（4）日志数据

数据分类	中文名称	定义	数据类型	数据格式	更新周期

安全设备日志	产生日期	安全设备日志产生的日期和时间	字符型	an19	5 分钟
	报警名称	安全设备日志报警名称	字符型	an1..100	5 分钟
	发生源 IP	上报安全设备 IP	字符型	an7..40	5 分钟
	代理 IP	上报安全设备代理 IP	字符型	an0..40	5 分钟
	设备名称	安全设备名称	字符型	an1..100	5 分钟
	序列号	设备唯一 S/N 号	字符型	an1..100	5 分钟
	设备类型	安全设备类型	字符型	an1..100	5 分钟
	源 IP	安全报警源 IP	字符型	an7..40	5 分钟
	源端口	安全报警源端口	字符型	n1..5	5 分钟
	目的 IP	安全报警目的 IP	字符型	an7..40	5 分钟
	目的端口	安全报警目的端口	字符型	n1..5	5 分钟
	日志等级	安全报警等级	字符型	an1..100	5 分钟
	报警类型	安全报警类型	字符型	an1..100	5 分钟
	日志	安全报警日志内容	字符型	an0..8000	5 分钟
主机日志	产生日期	主机日志产生日期	字符型	an19	5 分钟
	云主机 ID	云主机唯一标识	字符型	an1..50	5 分钟
	主机名称	主机名称	字符型	an1..100	5 分钟
	主机 IP	主机 IP	字符型	an7..40	5 分钟
	操作系统类型	主机操作系统	字符型	an1..40	5 分钟
	日志名称	主机日志名称	字符型	an1..100	5 分钟
	日志类型	主机日志类型	字符型	an1..100	5 分钟
	日志正文	主机日志内容	字符型	an1..8000	5 分钟

（5）云平台数据

数据分类	中文名称	定义	数据类型	数据格式	更新周期
云平台规格数据	云服务商	云服务商	字符型	an4	天
	机房	设备所在机房	字符型	an4	天
	云平台所属厂商	如华为、H3C 等	字符型	an1..100	天
	云平台网络类型	连接网络	字符型	an4	天
	CPU 总量	云平台可提供的 CPU 总核数	数值型	n1..12	天
	CPU 分配量	云平台当前已分配出的 CPU 核数	数值型	n1..12	天
	内存总量	云平台可提供的内存总量	数值型	n1..16.2	天
	内存分配量	云平台当前已分配出的内存总量	数值型	n1..16.2	天
	普通存储总量	云平台可提供的普通存储的总量	数值型	n1..16.2	天
	普通存储分配量	云平台当前已分配出的普通存储总量	数值型	n1..16.2	天
	高性能存储总	云平台可提供的高性能存储	数值型	n1..16.2	天

	量	总量			
	高性能存储分配量	云平台当前已分配出的高性能存储总量	数值型	n1..16.2	天
	静态存储总量	云平台可提供的静态存储总量	数值型	n1..16.2	天
	静态存储分配量	云平台当前已分配出的静态存储总量	数值型	n1..16.2	天
	互联网带宽总量（	云平台可提供的互联网带宽总量	数值型	n1..16.2	天
	互联网带宽分配量	云平台当前已分配出的互联网带宽总量	数值型	n1..16.2	天
云平台网络接入IP数据	网络类型	连接网络	字符型	an4	天
	云服务商	云服务商	字符型	an4	天
	机房	设备所在机房	字符型	an4	天
	运营商	网络运营商	字符型	an1..100	天
	IP地址/IP地址段	外网IP地址/地址段	字符型	an1..800	天
	主链路带宽	主链路带宽数值	数值型	n1..16.2	天
	备份链路带宽	备份链路数值	数值型	n1..16.2	天

（6）服务数据

数据分类	中文名称	定义	数据类型	数据格式	更新周期
业务系统数据	使用单位编号		字符型	an1..50	天
	单位地址邮编				天
	云平台	云服务商	字符型	an4	天
	部署节点	北京城市副中心、北京市政务服务中心	字符型	an1..50	天
	机房	设备所在机房	字符型	an4	天
	信息系统编号	使用单位编号之后，以001开始，顺序编制	字符型	an1..50	天
	信息系统名称	以工单中所填业务系统名称为主要依据	字符型	an1..200	天
	入云测试日期		字符型	an10	天
	联系人姓名		字符型	an1..50	天
	联系人手机号		字符型	an1..20	天
	联系人电子邮箱		字符型	an1..50	天
	联系人座机		字符型	an0..20	天
	技术人联系人姓名		字符型	an0..50	天
	技术联系人手机号		字符型	an0..20	天
	前置审批情况		字符型	an1..200	天
	功能描述	说明该应用平台的主要功能	字符型	an1..8000	天
	系统类型	业务生产系统、内部办公、公众服务、门户网站、移动APP、视频系统、其他	字符型	an1..50	天

	信息系统定级情况	一级、二级、三级、未定级	字符型	an1..50	天
	信息系统运行时间	7*24 小时、5*8 小时、其他	字符型	an1..50	天
	系统服务对象		字符型	an1..200	天
	系统服务范围		字符型	an1..200	天
	网络性质	政务外网、互联网、政务外网及互联网，**专线**	字符型	an1..50	天
	系统互联情况及涉及单位	与本单位其他系统连接、与其他单位系统连接、无互联	字符型	an1..50	天
	其他说明		字符型	an1..200	天
	上线日期		字符型	an10	天
	退出日期		字符型	an10	天
	退出原因		字符型	an1..200	天
	信息系统访问地址	该应用的完整访问地址(互联网请填写基于域名的完整访问路径，政务外网基于 IP 地址的完整访问路径)	字符型	an1..200	天
	应用厂商	应用开发商	字符型	an1..200	天
云主机规格数据	信息系统编号	使用单位编号之后，以 001 开始，顺序编制	字符型	an1..50	天
	云主机名称	云服务商所设定云主机名称	字符型	an1..200	天
	云主机 ID	云主机唯一标识	字符型	an1..50	天
	内部 IP	云主机内部 IP 地址	字符型	an7..40	天
	云主机类型	云主机类型	字符型	an4	天
	运行状态	云主机运行状态	字符型	an4	天
	云平台	云服务商	字符型	an4	天
	所属区域编码	设备所在机房	字符型	an4	天
	网络类型	连接网络	字符型	an4	天
	创建日期	云主机创建日期	字符型	an10	天
	删除日期	云主机删除日期	字符型	an10	天
	CPU 核数	云主机所分配的 CPU 核数	数值型	n1..12	天
	内存分配量	云主机的内存分配量	数值型	n1..16.2	天
	普通存储分配量	云主机的普通存储分配量	数值型	n1..16.2	天
	高性能存储分配量	云主机的高性能存储分配量	数值型	n1..16.2	天
	静态存储分配量	云主机的静态存储分配量	数值型	n1..16.2	天
	本地视频存储分配量	云主机的本地存储分配量	数值型	n1..16.2	天
	异地存储分配量	云主机的异地存储分配量	数值型	n1..16.2	天
互联网链路带宽服务数据	信息系统编号	使用单位编号之后，以 001 开始，顺序编制	字符型	an1..50	天
	互联网 IP	业务系统所对应互联网 IP	字符型	an7..40	天
	系统域名	互联网 IP 对应的域名	字符型	an1..100	天
	带宽	上云用户所租用互联网带宽	数值型	n1..16.2	天
	起始日期	上云用户业务系统入云，使用互	字符型	an10	天

		联网带宽时间			
	截止日期	上云用户业务系统退云，不再使用互联网带宽时间；	字符型	an10	天
主机负载均衡服务数据	信息系统编号	使用单位编号之后，以 001 开始，顺序编制	字符型	an1..50	天
	内网 IP	业务系统所开资源的 IP 地址(内网)，一般为多个	字符型	an7..40	天
	外网 IP	业务系统通过互联网被访问的 IP 地址（外网）	字符型	an7..40	天
	负载 IP	业务系统所对应的负载均衡服务器的 IP	字符型	an7..40	天
	开放端口	业务系统的开放端口	数值型	n1..5	天
	开通日期	主机负载均衡服务的开通时间	字符型	an10	天
	关闭日期	主机负载均衡服务的结束时间	字符型	an10	天
VPN 服务数据	系统编号	使用单位编号之后，以 001 开始，顺序编制	字符型	an1..50	天
	VPN 类型	表格中下拉菜单可选 SSL VPN 和 Ipsec VPN 两种类型	字符型	an1..50	天
	账号	为上云用户所建 VPN 服务帐号	字符型	an1..50	天
	可访问范围（IP 或 IP 地址段）	通过 VPN 帐号可访问的 IP 地址段	字符型	an1..800	天
	开通日期	VPN 帐号开通时间	字符型	an10	天
	关闭日期	VPN 帐号删除时间	字符型	an10	天
WAF 防护服务数据	信息系统编号	使用单位编号之后，以 001 开始，顺序编制	字符型	an1..50	天
	IP 地址	WAF 所防护 IP 地址	字符型	an7..40	天
	端口	IP 地址所防护的端口	数值型	n1..5	天
	防护类型	如 WEB 防护（默认或自定义）	字符型	an1..50	天
	开通日期	WAF 防护开通时间	字符型	an10	天
	关闭日期	WAF 防护关闭时间	字符型	an10	天
远程接入服务数据	系统编号	使用单位编号之后，以 001 开始，顺序编制，由云监管服务商编制，反馈云服务商	字符型	an1..50	天
	账号	上云用户单位通过远程接入服务进入自有云空间的帐号	字符型	an1..50	天
	可访问范围（IP 或 IP 地址段）	通过帐号进入自有空间可访问的 IP 地址段	字符型	an1..800	天
	开通日期	远程接入服务帐号的开通时间	字符型	an10	天
	关闭日期	远程接入服务帐号的关闭时间，	字符型	an10	天
云机房专线接入服务数据	信息系统编号	使用单位编号之后，以 001 开始，顺序编制	字符型	an1..50	天
	网络运营商	网络运营商	字符型	an1..50	天
	专线用途	银行业务，区县业务，部委财政	字符型	an1..200	天

		网络，其他业务			
	起始时间	专线完成时间 开始使用时间	字符型	an10	天
	结束时间	专线取消时间	字符型	an10	天
	线路本端地址	云平台端地址	字符型	an7..40	天
	线路对端地址	专线对端地址	字符型	an7..40	天
	配线柜编号		字符型	an1..100	天
	云机柜编号		字符型	an1..100	天
	接入设备名称		字符型	an1..100	天
	接入设备端口		数值型	n1..5	天

（7）服务数据

数据分类	中文名称	定义	数据类型	数据格式	更新周期
云主机监控数据	云主机 ID	云主机唯一标识	字符型	an1..50	5 分钟
	监控时间	监控数据时间	字符型	an19	5 分钟
	内部 IP	云主机内部 IP 地址	字符型	an1..40	5 分钟
	CPU 使用率	采集周期内该云主机的 CPU 使用率峰值	数值型	n1..3,2	5 分钟
	内存使用率	采集周期内该云主机的内存使用率峰值	数值型	n1..3,2	5 分钟
	普通存储使用率	采集周期内虚机存储使用率	数值型	n1..3,2	5 分钟
	高性能存储使用率	采集周期内虚机存储使用率	数值型	n1..3,2	5 分钟
	静态存储使用率	采集周期内虚机存储使用率	数值型	n1..3,2	5 分钟
	本地视频存储使用率	采集周期内虚机存储使用率	数值型	n1..3,2	5 分钟
	异地视频使用率	采集周期内虚机存储使用率	数值型	n1..3,2	5 分钟
	磁盘写峰值	采集周期内每秒向设备写入的峰值	数值型	n1..16.4	5 分钟
	磁盘读峰值	采集周期内每秒从设备读取的峰值	数值型	n1..16.4	5 分钟
	带宽上行峰值	采集周期内该云主机的上行网络速率峰值	数值型	n1..16.8	5 分钟
	带宽下行峰值	采集周期内该云主机的下行网络速率峰值	数值型	n1..16.8	5 分钟
应用系统网络出口使用数据	业务系统编号	使用单位编号之后，以 001 开始，顺序编制	字符型	an1..50	5 分钟
	网络类型	连接网络	字符型	an4	5 分钟

	监控时间	监控数据时间	字符型	an19	5 分钟
	带宽上行峰值	采集周期内该云主机的上行网络速率峰值	数值型	n1..16.8	5 分钟
	带宽下行峰值	采集周期内该云主机的上行网络速率峰值	数值型	n1..16.8	5 分钟
VPN/远程接入登录数据	业务系统编号	使用单位编号之后，以 001 开始，顺序编制	字符型	an1..50	5 分钟
	网络类型	连接网络	字符型	an4	5 分钟
	监控时间	监控数据时间	字符型	an19	5 分钟
	类型	SSL VPN、Ipsec VPN、远程接入	字符型	an1..50	5 分钟
	账号	为上云用户所建帐号	字符型	an1..50	5 分钟
	会话 ID	vpn 或远程接入建立连接会话的唯一标识	字符型	an1..50	5 分钟
	登入时间		字符型	an19	5 分钟
	退出时间		字符型	an0..19	5 分钟
运维监测数据	检测类型	机房巡检、云平台运维、网络运维、安全运维			
	监测内容		字符型	an1..50	5 分钟
	是否正常		字符型	an19	5 分钟
	监测时间		字符型	an1..50	5 分钟
	监测人		字符型	an1..50	5 分钟
安全漏洞扫描数据	安全漏洞名称	安全漏洞名称	字符型	an1..50	周
	漏洞类型	主机漏洞、数据库漏洞、WEB 漏洞、中间件级其他组件漏洞等	字符型	an1..50	周
	安全漏洞风险等级	安全漏洞风险等级，一般分为高、中、低	字符型	an1	周
	云主机 ID	发现漏洞的云主机的 ID	字符型	an1..50	周
	信息系统编号	发现漏洞的信息系统的 ID	字符型	an1..50	周
	监测时间	进行安全扫描的时间	字符型	an1..50	周
	是否通知相关单位	是否对相关单位进行通知	字符型	an1	周
	漏洞是否整改	漏洞整改详情（完成整改、部分整改、未整改）	字符型	an1..4	周
	漏洞整改时	完成漏洞整改时间	字符型	an1..50	周

	间				
安全补丁安装数据	安全补丁名称	安全补丁名称	字符型	an1..50	周
	云主机 ID	安装补丁的云主机 ID	字符型	an1..50	周
	补丁类型	Windows 补丁、Linux 补丁、各类数据库补丁、中间件补丁	字符型	an1..50	周
	补丁发布时间	安全补丁正式发布的时间	字符型	an1..50	周
	补丁安装时间	安全补丁安装时间	字符型	an1..50	周
	监测人		字符型	an1..50	周
安全预警监测数据	监测类型	漏洞发布、补丁发布	字符型	an1..50	周
	监测内容	安全相关监测内容，例：如监测类型为漏洞发布，此处内容未漏洞详细信息，监测类型为补丁发布，此处内容为发布的安全补丁的详细信息	字符型	an1..50	周
	是否已通知相关单位	是、否	字符型	an1	周
	监测时间				周
	监测人				周
安全攻击监测数据	攻击名称	安全攻击名称	字符型	an1..50	周
	云主机 ID	攻击涉及云主机 ID	字符型	an1..50	周
	信息系统编号	攻击涉及信息系统编号	字符型	an1..50	周
	是否已通知相关单位	是、否	字符型	an1	周
	监测时间				周
	监测人				周

2.3云平台技术要求

2.3.1虚拟化平台要求

1.虚拟机之间可以做到隔离保护,其中每一个虚拟机发生故障都不会影响同一个物理机上的其它虚拟机运行，每个虚拟机上的用户权限只限于本虚拟机之内，以保障系统平台的安全性；

2.虚拟机可以实现物理机的全部功能，如具有内存、CPU、网卡、存储等资源，可以指定单独的 IP 地址、MAC 地址等；

3.当虚拟机 Windows、Linux 操作系统出现故障时，可以自动重启或者迁移该虚拟机，保障业务连续性；

4.支持将多个物理服务器组成集群，可基于 CPU、内存、磁盘等资源利用率进行动态资源调整；

5.支持平台巡检功能，支持生成巡检报告并导出；

6.虚拟化软件可以在线进行版本升级，不同版本之间可以相互兼容；

7.多台物理机可以实现虚拟化集群，集群内的物理机数量可以按需扩展；

8.支持异构虚拟化能力，支持 VMware、KVM、PowerVM 等多种虚拟化技术。

2.3.2云网络系统要求

1.数据中心网络支持双活网络架构，满足应用双活的网络要求；

2.实现数据中心大二层架构组网,支持虚拟机二层迁移；

3.为入云系统划分安全区域，合理制定访问规则；

4.核心骨干设备、出口设备、骨干线路等需要支持冗余备份，云内骨干线路带宽≥40Gb 带宽，服务器业务≥10Gb 带宽，核心骨干设备可以保证大规模业务迁移，无缝扩容需求；

5.支持对云平台内的网络设备进行统一管理；

6.网络控制器需集群部署，升级时业务不中断；

7.支持 IPV6 地址分配，满足业务系统 IPV6 改造要求；确保政务云政务外网区、互联网区应配置独立的 IPv6 资源池承载 IPv6 应用。网络设备、存储设备、安全设备以及计算机服务器操作系统、虚拟化软件等基础设施均支持 IPv6;云平台北向、南向接口应支持 IPv6 访问；基础服务、数据服务、数据库服务、应用服务、安全服务等云服务应支持 IPv6。 数据交换区应支持 IPv6 数据交换和安全防护。

8.政务外网的带宽接入由云管理单位解决，互联网带宽由云服务商解决，为提升跨网访问体验，云服务商互联网接入应采用多线接入链路，确保在一条线路出现故障时，其他线路可以继续提供服务，从而避免服务中断。

9.根据政务网络安全管理、信息安全等级保护等要求，部署和划分互联网区和政务外网区，两个区域之间应按照要求进行安全隔离并提供必要的安全保障，分别承载政务外网和互联网应用，政务外网应用与互联网应用实现安全隔离和数据交换；

10.云平台需满足基于 SDN、VxLAN 技术提供相关网络服务，SDN 可以与云平台能实现自动化动态的网络资源调配和隔离，支持与互联网、电子政务外网及行业部门专网的连接。

2.3.3云存储系统要求

1.高性能存储与普通存储可按应用需求选择不同磁盘类型，实现数据按需存储；

2.支持多种存储类型，包括块存储、对象存储、文件存储等；

3.高性能存储与普通存储应具备较强的扩展能力,存储系统可扩展容量支持 PB 级扩展；

4.高性能存储单盘技术指标 IOPS 10000-25000 ，普通存储单盘技术指标 IOPS 2000-5000 ；

5.高性能存储与普通存储采用先进的磁盘容错技术，在硬盘故障后可实现快速重构，避免重构过程中其他硬盘损坏导致的数据丢失风险；

6.高性能存储与普通存储可靠性达到 99.9999%；

7.备份存储具有可靠的数据保护机制，确保不会因硬盘故障等原因导致数据丢失。

2.3.4平台高可靠要求

1.云平台使用的网络安全设备、服务器、存储等设备都应具备高可靠性及冗余性，即单个设备或单个节点出现故障时，其他设备/节点可以立刻接管任务，保证云平台整体的业务连续性不低于99.99%。

2.云平台具备高可用和动态迁移功能，发生物理设备故障后，虚拟机可以自动迁移到其他可用资源上运行，确保业务系统不受物理设备故障影响。

3.云平台提供备份/快照功能，能对云平台中的物理和虚拟服务器进行备份，防止存储故障导致数据丢失。

2.3.5数据级备份要求

云服务商需具有本地和同城异地数据级备份能力，并配合使用单位完成数据级容灾演练及恢复等工作。备份系统应满足如下要求:

1.备份介质本身具备高可用性和冗余性。

2.备份方式包括完整备份、差异备份和增量备份。

3.支持Windows系列操作系统、Linux主流系统操作系统、主流数据库软件、主流中间件软件、结构化数据以及非结构化数据等备份对象。

4.支持建立统一的备份管理系统，用来管理本地备份和异地备份。

5.云服务商应提供对备份过程状态、备份结果提供运维监控保障服务，确保备份任务执行成功以及备份的数据完整性。

2.3.6应用双活要求

云服务商建设的云平台应具备提供同城应用级双活服务。当重要业务系统所在的机房发生重大事故时，可以在规定的时间内实现业务恢复，具体参照《信息系统灾难恢复规范》(GB/T 20988-2007)。云服务商需要配合使用单位和灾备中心完成应用层容灾演练及恢复等工作。

云平台应具备支撑同城容灾、应用层双活、数据库主备的平台能力，且能够为使用单位提供跨云服务商云计算平台、跨数据中心的系统双活、容灾服务的支撑能力，如同一地点的不同云平台间，或服务云与行业云间。

云服务商能够为使用单位提供跨云平台的业务发放能力，可以通过图形界面向不同云平台进行业务发放，也可以管理不同云平台的资源，包括资源集中展现、云平台资源的开关启停等功能。

2.3.7云平台兼容能力

云平台应兼容符合安全可靠测评结果的国产化软件产品，应采用支持国产化应用替代的云平台技术。

2.4云平台安全保障要求

2.4.1云平台安全建设要求

1.云服务商所提供云平台应符合国家及行业标准、规范。云服务商应参照《信息安全技术 网络安全等级保护定级指南》(GB/T22240-2020）对云平台进行定级备案，参照《信息安全技术 网络安全等级保护基本要求》(GB/T22239-2019）第三级安全要求进行建设，投入使用前必须通过网络安全等级保护第三级测评，并完成公安部门备案手续。

2.云服务商所提供云平台应根据《云计算服务安全评估办法》的要求，通过云计算服务安全评估。

3.云服务商所提供云平台应根据《国家政务信息化项目建设管理办法》（国办发〔2019〕57 号)、《信息安全技术 信息系统密码应用基本要求》(GB/T39786-2021）设计云平台密码应用方案，建设运行密码保障系统，并定期进行商用密码应用安全性评估。同时，云平台应能够按需提供身份认证服务、签名验签服务、密码计算服务、传输加密服务和密钥管理服务等符合国家密码应用要求的密码云服务。

4.承担云平台层面（主要包括物理资源、计算资源、存储资源、网络资源）以及云平台数据防篡改、防丢失的安全责任。

5.在单一云平台内部，云服务商需要实现不同用户间业务应用系统及数据的安全隔离。

6.云服务商需要分别搭建互联网区和政务外网区，两个区域采用独立的物理网络系统、安全系统和云操作系统软件。

7.云服务商应建立云平台应急体系，定期开展演练工作，保障灾难发生时，指导或协助云平台使用单位开展系统应急工作，能够保留数据、恢复系统及数据。

8.云服务商应采用符合国家密码管理部门要求的密码技术保护云平台及数据的安全性，包括但不限于网络和通信安全、设备和计算安全、应用和数据安全、密钥管理等。

9.云服务商应遵守管理单位和使用单位关于个人数据/敏感数据/重要数据保护/隐私保护相关规定。

10.云服务商应建立监控机制，可检测虚拟机之间的资源隔离是否失效、是否存在非授权新建虚拟机或者重新启用虚拟机、恶意代码感染及在虚拟机间蔓延的情况，并进行告警。

11.云服务商应根据云租户要求对物理资源和虚拟资源按照策略做统一管理调度与分配。

12.云计算平台应具有虚拟机内存隔离措施，云租户的虚拟机应使用独占的内存空间。

13.云服务商应对虚拟机的网络接口的带宽进行设置，并进行监测。

14.云服务商应屏蔽虚拟资源故障，某个虚拟机宕机后不影响虚拟机监视器及其他虚拟机。

15.云服务商应及时通报其安全事件、提供安全事件分析报告、漏洞和补丁修复或升级。

16.云服务商应建立密钥管理机制，采用技术和管理措施，从密钥的生成、存储、分发、导入、导出、使用、备份、恢复、归档与销毁等全流程各环节 保障密钥安全。

2.4.2云平台安全保障能力

云服务商建设的云平台应满足《信息安全技术网络安全等级保护基本要求》（GB/T22239-201 9)、《信息安全技术 网络安全等级保护测评要求》(GBT28448-2019)、《关于加强党政部门云计算服务网络安全管理的意见》(中网办发文〔2014〕14 号）及国家主管部门发布的其他标准规范要求。

根据国家、北京市、政府行业的等级保护相关政策和标准要求，结合使用单位信息系统具体情况，提供等级保护合规咨询服务。通过等级保护差距分析，发现信息系统的安全现状与需要达到的安全等级或目标的差异，并配合完成信息系统的定级、备案和整改等工作，加强和完善使用单位在管理和技术方面的安全保障能力。

1.风险评估能力

根据 GB/T20984-2022《信息安全技术 信息安全风险评估方法》等国家标准及相关技术规范进行安全评估。基于多角度、多纬度的全面评估，细粒度呈现系统的安全现状。

2.漏洞扫描能力

漏洞扫主要是通过评估工具以远程扫描的方式对评估范围内的系统和网络进行安全扫描，查找网络结构、网络设备、服务器主机、数据和用户账号/口令等安全对象目标存在的安全风险、漏洞和威胁。

3.渗透测试能力

渗透测试是对使用单位的信息系统，通过专业的信息安全工具，进行扫描，而后根据分析结果，由资深安全技术工程师模拟黑客工作方式对发现的漏洞进行验证性渗透测试的服务。目的在于发现目标系统中的安全漏洞，在安全事件发生前发现安全漏洞，防范于未然，最大程度减少系统遭受黑客攻击的可能。

4.安全基线配置核查能力

安全基线配置核查是由安全专业人员根据评估范围，基于国家信息安全等级保护标准要求，采用人工检查用表（Checklist)、脚本程序或基线扫描工具对评估目标范围内的网络安全设备、主机系统、数据库、中间件等进行安全基线配置合规检查，并提供安全加固建议。

5.流量监控能力

对政务云互联网出口、互联网核心、政务外网出口、政务外网核心等关键区域进行流量监控和存储，通过数据包的角度，针对网络故障、业务问题和安全事件，进行事前预防、事中分析、事后回溯的智能化运维。

2.4.3多云节点安全保障能力

同一云服务商多云节点的安全保障应从云边界安全、云基础设施安全、云数据安全、云应用安全、云平台安全及云间安全等方面整体考虑云安全建设，互相协调，共同构建一个完整闭环的云安全体系。

1.云边界安全。在网络和区域边界，实现安全隔离防护，提高边界安全的可靠性；基于

零信任等技术建设多云集中管理平台，通过统一身份认证和细颗粒度安全策略，实现应用级安全防护，达到对数据、应用、网络等安全事件的集中监控管理；定期开展安全评估。

2.云基础设施安全。机房基础设施、硬件资源池及物理线路等基础设施方面应遵守我市政务云管理及相关国标规定。

3.云数据安全。应根据业务需求和数据重要程度进行在线数据备份和异地容灾备份，定期进行数据恢复和系统一键切换等应急演练；根据数据重要程度、敏感程度等进行数据的分割存储，将数据分别保存在服务云的多个节点，根据需要进行云间数据交换；基于北京市大数据平台共享交换数据，通过技术手段减少云间数据交换频率和数据量。

4.云应用安全。根据政务信息系统安全保护等级配置不同的安全策略，减少跨等级数据交换数量，提高访问效率，并严格监控数据交换；通过统一多云管理平台，实时了解各应用的关键云主机的运行状态，如数据库云主机等。

5.云计算平台安全。通过统一多云管理平台同时监控多个云节点的安全事件，实现自动告警和联动控制，实现主动安全防御。

6.云间安全服务。采取数据安全分级和加密、建设专线等方式保障其安全性，包括根据数据重要性和敏感程度，进行数据分级传输和加密，实现过程控制和双向安全防护；通过数据共享平台实现云间数据同步、断点重传、数据迁移、数据加密等功能，保证传输过程中的真实性和可靠性；在多云节点间建设专用线路或者 VPN 专网，实现传输链路的独占性，防止数据被监听、复制、篡改和植入。

2.5云平台数据安全要求

1.云服务商承担云平台数据防篡改、防丢失的安全责任。

2.业务数据未经使用单位同意，不得离开云机房。云服务商未经允许不得对云平台上的任何数据进行非法截取、加工、分析处理或提供给第三方机构。

3.云服务商在未经过用户邮件、书面材料确认前提下，不能查看、修改、拷贝用户业务系统文件和数据；各业务系统、数据归属于使用单位，云服务商无权支配。

4.云平台内所有设备的维修、报废等处理须经过云管理单位审批。

2.6时间进度要求

1.云服务商应在入围结果公告发布之日起 90 个自然日内完成云平台建设和测试等工作。

2.云服务商在服务期内应根据用户方的扩容需求，可在 7 个自然日内完成云平台的资源扩容。

三、云服务要求

3.1服务目录和取费要求

3.1.1服务目录与市集采目录的关系

根据《北京市政府采购集中采购目录及标准（2023 年版）》，“云计算服务”被纳入到北京市政府采购集中采购目录中，内容包括：云计算服务中的基础服务，包括计算服务、存储

服务、网络服务。

本次云服务目录按照市集采目录规定的范围制定，包括基础服务目录、云基础安全保障服务目录。通过采购确定服务单价，作为使用单位申报预算、执行采购的依据。未来市区、行业共享同一服务目录。

3.1.2目录内容概述及取费要求

1.基础服务是应由云服务商提供的服务，包括计算、存储、网络等服务，通过本次采购确定该目录的服务单价，并纳入北京市政府采购目录。

2.云基础安全保障服务是云服务商应具备的云平台层安全保障能力,用户无需另行购买即可享受服务。

3.云服务商应基于云平台加快发展 PaaS 及 SaaS 生态能力。

3.1.3基础服务目录

编号	服务类别	服务子类	服务项	计价单位	报价单位	备注说明	各服务项最高限制单价	权值
1001	计算服务	平台云主机服务（包含 X86、ARM、C86）	vCPU（vCPU ARM 架构主频不低于 2.4GHz，C86 和 x86 主频不低于 2.2GHz，平均虚拟化率，即物理 CPU/虚拟 CPU ≥1/4，虚拟 CPU 利用率不低于物理 CPU 的 25% ）	1 CPU	元 / 月	提供云主机备份服务,数据备份空间需单独计费	14.02	10%
1002			内存	1 GB	元 / 月		41.15	16%
1003		物理服务器租用服务（包含 X86、ARM、C86）	配置 1：双路每 CPU 核数≥32 核，主频≥2.0GHz，128G 内存，2 块 600GSAS 硕盘，2 个 HBA 卡，2 个万兆端口	1 台	元 / 月	原则上适用于云主机无法支撑应用系统正常运行的情况	354.23	2%
1004			物理服务器配置2：四路每 CPU核数≥48 核，主频≥ 2.6Ghz，256G内存，2块 600SAS硬盘，2个HBA卡，2 个万兆端口	1 台	元 / 月		374.52	2%
100		物理服务器增配服务（包含 X86、ARM、C86）	内存-32GB 内存	1 条	元 / 月		200.60	1%

5								
1006			硬盘配置 1-480GB SSD	1 块	元 / 月		122.68	1%
1007			硬盘配置 2-600GB SAS	1 块	元 / 月		102.83	1%
1008			硬盘配置 3-4TBSATA	1 块	元 / 月		191.73	1%
1009		GPU 卡算力服务（适配 X86、ARM、C86）	GPU 显存（需同时租用算力资源、云主机或物理服务器资源，联合使用）	1 GB	元 / 月		45.00	3%
1010			半精度浮点运算能力（需同时租用 GPU 显存、云主机或物理服务器资源，联合使用）	1 TFLOPS	元 / 月		8.00	6%
1011	存储服务（兼容 X86、ARM、C86）	普通性能存储	普通存储（单盘技术指标：单盘 IOPS 2000-5000）	100 GB	元 / 月	提供普通性能存储服务，IOPS 随磁盘容量增加而增加。	28.60	8%
1012		高性能存储	高性能存储（单盘技术指标：单盘 IOPS 10000-25000）	100 GB	元 / 月	提供高性能存储服务，IOPS 随磁盘容量增加而增加。	64.25	10%
1013		静态存储	提供大容量、高可靠的数据存储服务，具备 PB 级线性扩展能力	1 TB	元 / 月	提供静态数据存储	72.75	8%
1014		本地备份服务	本地备份服务	100 GB	元 / 月	通过备份策略实现文件、操作系统、数据库的本地备份（不包含备份存储空间费用）	88.45	3%
10		异地备份服务	异地备份服务	100 GB	元 / 月	通过备份策略实现文件、	138.90	3%

15						操作系统、数据库的异地备份(不包含备份存储空间费用)		
1016	网络服务（兼容X86、ARM、C86）	互联网链路服务	互联网链路带宽	1 Mb	元 / 月	须提供多线运营商接入服务,保证稳定可靠。	49.55	8%
1017			互联网 IP 地址租用服务、并提供备案服务	1 IP	元 / 月	提供互联网地址租用,并且提供网站域名备案服务。	76.05	2%
1018		主机负载均衡服务	主机负载均衡服务	1 IP（内网）	元 / 月	提供主机应用集群负载均衡服务	66.47	6%
1019		远程接入服务	远程接入服务	1 账号	元 / 月	每个账号结合身份验证通过 VPN 远程接入堡垒机进行维护（免费提供1个账号）	356.37	1%
1020		VPN 服务	SSL VPN 接入	1 套	元 / 月	用户通过 SSL VPN 访问业务系统。每套 10 个并发用户。所需带宽参照“互联网链路带宽”购买。	257.72	1%
1021			IPSec VPN 接入	1Mb 带宽	元 / 月	提供 IPSec 隧道接入服务,隧道带宽按需灵活调整,用户可利用 VPN 隧道进行大量数据传输。	127.78	1%
102		SSL 证书服务	提供 SSL 证书服务	1 域名	元 / 月	为网站提供 https 保护，对流量进行	313.69	2%

2						加密，防止数据被窃取。		
1023		Web 应用防火墙（WAF）	针对网站及 Web 应用系统提供应用层安全防护，支持各类 SQL 注入、XSS 攻击、网页木马、WEBSHELL 等 Web 威胁防护 （200Mbps）	1 套	元 / 月	在网站前端架设 WAF 防护服务，保证用户网站对已知安全隐患进行防护，实时升级漏洞补丁，配置防护策略，可起到前端防护作用。	98.86	4%
	采购项目最高限价：79.0430 元/月 **注：23 个分项服务报价可以精确到分位，即小数点后可以保留两位有效数字，若保留有效数字超出两位，作无效响应处理。**							

3.1.4基础安全保障服务目录

基础安全保障服务目录（适用于云服务商提供的所有政务云平台）			
编号	**服务类别**	**服务目录**	**项目**
2001	安全管理服务	运维人员管理	7x24 小时运维人员管理、安全登记
2002		机房运维管理	机房设备管理、安全控制
2003		应急演练	协助使用单位进行安全应急演练
2004	安全技术服务	物理访问控制	机房进出控制、监控等
2005		机房三防服务	机房防火、防盗、防雷电
2006		设备访问审计	设备访问记录、日志统计、安全事件
2007		出口流量监测	出口流量控制、检测，并且可观测数据，互联网网络行为审计
2008		本地抗 DDoS 防护	云平台整体提供总带宽为 20Gb 的抗 DDoS 防护
2009		防火墙安全防护	出口安全
2010		防入侵监测 IPS	防入侵监测
2011		远程接入服务	免费提供 1 个远程登录堡垒机的运维账号
2012		租户隔离	租户虚拟化层隔离
2013		租户内部访问控制	租户内部访问权限控制，用户可以自由分配
2014		云主机监控	提供云上资源的基本监控，包括 CPU、内存使用率等
2015		角色权限管理	提供通过代入角色实现获取操作权限
2016		监控平台接入服务	可提供租户管辖内的云资源监控数据接口调用
2017		云主机深度监控服务	7*24 小时深度监测云主机资源、硬件设备监控、云平台层应急处置等内容

3.1.5扩展服务目录

除服务目录规定的服务能力外，云平台应具备一定扩展服务能力，具体见下表。

服务类别	服务子类	服务项	备注说明
基础软件支撑服务	商用操作系统套餐	Windows Server 套餐：Windows Server 租用、安装及维护。	由云服务商提供租用、安装、调优，排错，技术支持服务。
		国产 Linux 套餐：国产 Linux 操作系统服务租用、安装及维护。	
	开源操作系统套餐	提供开源操作系统安装和维护服务。	由云服务商提供安装、调优，排错，技术支持服务。
	商用应用中间件套餐	国产商用应用中间件租用、安装及维护	由云服务商提供租用、安装、调优、排错、技术支持服务。
	开源应用中间件套餐	主流开源应用中间件安装及维护服务（3 种以上开源中间件）	由云服务商提供调优，排错，技术支持服务。（1 套包括 1 种开源中间件软件）
	商用数据库套餐	国产商用数据库租用、安装及维护（至少支持 3 种国产数据库）	由云服务商提供商用数据库的租用、安装、调优、排错、技术支持服务。
	开源数据库套餐	开源数据库安装及维护服务	由云服务商提供开源数据库的租用、安装、调优、排错、技术支持服务。（1 套包括 1 种开源数据库软件）
平台即服务（PaaS 服务）	云原生数据库（集中式）服务	云原生数据库（集中式）服务	提供云原生关系型数据库，支持高可用架构。
	云原生数据库（分布式）服务	云原生数据库（分布式）服务	提供云原生关系型数据库，采用分布式架构，支持分库分表、全局索引等能力。
	内存型数据库（分布式缓存 redis）服务	内存型数据库（分布式缓存 redis)服务	兼容开源 Redis 协议标准，支持多版本存储引擎，拥有数据可持久化存储、可用性高、弹性扩展和智能运维等特性
	容器服务	容器服务	提供容器服务，支持 Docker 镜像，支持多个 Kubernetes 版本，提供集群管理、容器生命周期管理能力。
	微服务框架	微服务框架	支持应用托管和微服务管理，支持应用托管和微服务管理，支持基于原生 SpringCloud、Dubbo 等应用托管。
	消息队列服务	消息队列(RocketMQ)服务	分布式消息中间件，提供消息订阅和发布、消息轨迹查询、定时（延时）消息、资源统计等能力，提供 TCP 协议和 HTTP 协议层面的接入方式，支持

			Java、C++、.NET 等多种编程语言。
	消息队列服务	消息队列(kafka)服务	兼容开源 Apache Kafka,可直接使用开源 Apache Kafka 客户端与消息队列 Kafka 版通讯
	API 网关服务	API 服务网关服务	支持 API 服务总线、API 组织管理和 API 运维监控等功能
	应用监控服务	应用监控服务	能够对应用进行全方位监控，支持自动生成应用拓扑，快速定位出错误接口和慢接口（慢 SQL）、重现调用参数、发现系统瓶颈。
迁移服务	云主机迁移（包含 X86、ARM、C86）	每个 VM 业务迁移	由云服务商提供使用单位现有虚拟化业务迁移上云，包括迁移前调研、迁移、测试、上线、技术支持服务。（不包括迁移到托管区）
	物理主机迁移（包含 X86、ARM、C86）	每台 X86 物理主机迁移	由云服务商提供使用单位现有物理主机业务迁移上云，包括迁移前调研、迁移、测试、上线、技术支持服务。（不包括迁移到托管区）
	单机数据库迁移	数据迁移服务（包括商用数据库和开源数据库）	由云服务商提供使用单位现有单机数据库业务迁移上云，只限于同构数据库架构迁移，包括迁移前调研、迁移、测试、上线、技术支持服务。（1 套为 1 个数据库实例）
	高可用数据库迁移	数据迁移服务（包括商用数据库和开源数据库）	由云服务商提供使用单位现有高可用（例如 HA、ORACLE RAC)数据库业务迁移上云，只限于同构数据库架构迁移，包括迁移前调研、迁移、测试、上线、技术支持服务。（1 套为 1 个数据库实例）
安全服务	云端抗 DDOS 服务	云端抗 DDOS 服务	根据流量提供云端抗 DDOS 服务,避免业务遭受拒绝服务攻击（攻击流量在 20G 以内）
	云端 APT 防护服务	云端 APT 防护服务	对未知攻击威胁进行检测和防护，发现隐蔽威胁、木马后门等异常威胁。
	主机杀毒服务	主机杀毒服务	对云主机进行定期的病毒查杀，杀毒软件集中控制，对网络性能无影响。
	主机防护	主机防护	主机防护：提供符合等保三级要求的主机权限管理及安全防护。

	主机安全加固	主机安全加固	针对漏扫或等级测评结果对操作系统进行安全加固，用以解决等级测评结果中所显示的漏洞。
	网页防篡改服务	网页防篡改服务	提供网页防篡改服务。通过防篡改软件对用户页面进行实时防护，减少用户页面被恶意篡改的可能性。
安全检测监测、审计服务	主机漏洞扫描	主机漏洞扫描	为用户提供针对主机层面的安全扫描服务，并反馈相关结果。
	主机日志审计服务	主机日志分析	针对操作系统进行日志收集，用于了解主机安全情况及资源使用情况
	数据库审计服务	数据库审计服务	支持 Oracle、SQL-Server、DB2、MySQL 等数据库审计。（1 套为 1 个数据库实例）。
其他服务	CDN 加速	提供内容加速及视频加速服务	将源站内容分发至最接近用户的节点，使用户可就近取得所需内容，提高用户访问的响应速度和成功率。
	密码应用安全支撑服务	提供身份认证、数据加解密、数据安全传输 、签名验签、密钥管理等密码应用安全支撑服务	用于支持云服务用户采用符合国家密码管理部门要求的密码技术保障云上系统安全。
	短信服务	提供短信服务	提供短信验证，通知等服务

3.2云平台服务能力要求

3.2.1计算服务

3.2.1.1 通用算力

须按照“一云多芯”模式建设，按需提供鲲鹏、飞腾、海光等各技术路线的计算资源。

指标项	规格要求
性能限制	按内存不复用方式分配资源，要求ARM架构CPU主频≥2.4GHz，C86和x86架构CPU主频≥2.2GHz
性能范围	CPU核数可选范围1-16核，内存可选范围1-64G
操作系统兼容性	支持主流操作系统，如windows server系列、Linux发行版、国产Linux等，需正版授权
扩展性	用户可以灵活调整云主机CPU、内存、硬盘规格
云主机隔离	对不同用户的虚拟主机提供安全组和VLAN级别的隔离，确保不同用户之间数据互不可见；云主机之间可以做到隔离保护，其中每一个云主机发生故障都不会影响同一个物理机上的其它云主机运行，每个云主

	机上的用户权限只限于本云主机之内，以保障系统平台的安全性。
管理权限	用户对云主机有完全的控制权，具有管理员权限，使用方式与传统物理主机完全一致。
HA功能	虚拟化管理节点须支持双机热备
	虚拟化管理系统支持虚拟机的HA功能
	硬件设备出现故障时，云主机会自动进行HA切换
备份功能	支持云主机备份功能，可以实现云主机的全量备份、增量备份，支持备份周期、备份策略的设定
可操作性	支持通过云管理平台，实现申请部署与使用
安全防护	提供防ARP欺骗、自定义防火墙功能，支持防DDos攻击；
弹性网络	支持虚拟路由、虚拟交换机和弹性IP，用户可自定义虚拟主机的网络拓扑和IP地址；
镜像快照	创建虚拟主机时，可指定用户预先配置好的镜像文件作为模板。虚拟主机支持增量快照备份功能，提高备份效率，减小备份占用空间，并支持公共镜像、私有镜像以及共享镜像等多种方式。
数据存储	虚拟主机底层采用分布式块存储，每个虚拟主机的镜像存储达到多副本可靠性，数据可靠性不低于99.9999%；
高可用性	虚拟主机服务采用全冗余架构，无单点故障，平均可用性不低于99.99%；
扩展性	支持计算能力的垂直伸缩，支持对CPU和内存的升级与降级操作，支持增加、减少磁盘和带宽； 支持计算能力的水平伸缩，通过与负载均衡配合实现水平伸缩；

3.2.1.2 物理服务器租用服务

提供裸金属主机服务，云服务商根据用户单位需求可提供不同配置参数的裸金属物理主机（包含 X86、ARM、C86）。

指标项	规格要求
服务器（包含X86、ARM、C86）	提供（包含X86、ARM、C86）裸机服务
性能要求	至少提供以下几种规格物理机以及配件规格供用户租用 物理服务器配置1：双路每CPU核数≥32核，主频 ≥2.0GHz，128G内存，2块600GSAS硕盘，2个HBA卡，2个万兆端口。 物理服务器配置2：四路每CPU核数≥48 核，主频≥2.6Ghz，256G内存，2块600SAS硬盘，2个HBA卡，2个万兆端口 物理服务器增配服务（包含X86、ARM、C86） 内存：32GB内存 硬盘1：480GB SSD硬盘 硬盘2：512GB SSD硬盘

	硬盘3：600GB SAS硬盘 硬盘4：900GB SAS硬盘 硬盘5：4TB SATA硬盘
管理权限	用户对云主机有完全的控制权，具有管理员权限
扩展性	可支持扩展GPU卡
可操作性	支持通过云管理平台，实现申请部署与使用

3.2.1.3 GPU 卡算力服务

云服务商能提供支持 GPU 卡服务包括但不限于 GPU、NPU 等（需适配 X86、ARM、C86 等架构）。

指标项	规格要求
部署要求	基于X86、ARM、C86等架构计算平台提供图形计算服务
性能要求	根据用户需求提供国产算力服务，提供半精度浮点运算能力，支持按照1TFLOPS和1GB显存为单位提供算力服务（需同时租用GPU显存、云主机或物理服务器资源，联合使用）
可操作性	提供的 GPU 卡算力服务，支持查看算力卡使用率等信息。 配合云主机使用的 GPU 卡需支持将一个或多个 GPU 采用直通虚拟化技术透传给云服务器。

3.2.1.4 普通性能存储

指标项	规格要求
可靠性要求	提供普通存储服务，要求稳定可靠，确保数据可靠性 99.9999%
性能要求	单盘技术指标满足 IOPS2000-5000
使用要求	用户可以以 1G 为最小单位进行容量申请，并可以申请直接挂载给云主机使用，同时用户可以将申请到的磁盘空间分配给一台或者多台虚拟机/物理机使用
架构要求	系统整体架构无单点故障
可操作性	支持通过云管理平台，实现申请部署与使用

3.2.1.5 高性能存储

指标项	规格要求
可靠性要求	要求稳定可靠，不会因单一部件故障、单一路径故障等原因导致业务停用、数据丢失，系统可靠性 99.9999%
性能要求	单盘技术指标满足 IOPS 10000-25000
使用要求	用户可以以 1G 为最小单位进行容量申请，并可以申请直接挂载给云主机使用，同时用户可以将申请到的磁盘空间分配给一台或者多台虚拟机/物理机使用
架构要求	系统整体架构无单点故障
可操作性	支持通过云管理平台，实现申请部署与使用

3.2.1.6 静态存储

指标项	规格要求
可靠性要求	提供静态存储服务，要求稳定可靠，结合其他技术，确保数据可靠性 99.999%
架构要求	采用分布式部署架构，具备 PB 级以上容量扩展能力，支持存储容量和性能的线性扩展，可根据需求迅速完成空间扩展

可操作性	支持通过云管理平台，实现存储服务的部署与挂载使用
可操作性	支持通过云管理平台，实现申请部署与使用

3.2.1.8 备份服务

通过备份策略实现对用户数据（文件、操作系统、数据库）的本地备份/异地备份（不包含备份存储空间费用），默认提供非结构化数据保护、Windows/Linux/Unix 操作系统备份保护及对应平台的数据库、文件备份保护。备份服务应满足如下要求:

（1）备份介质本身具备高可用性和冗余性。

（2）备份方式包括完整备份、差异备份和增量备份。

（3）支持 Windows 系列操作系统、Linux 主流系统操作系统、主流数据库软件、主流中间件软件、结构化数据以及非结构化数据等备份对象。

（4）支持建立统一的备份管理系统，用来管理本地备份和异地备份。

云服务商应提供对备份过程状态、备份结果提供运维监控保障服务，确保备份任务执行成功以及备份的数据完整性。

3.2.1.9 互联网链路服务

指标项	规格要求
带宽租用服务	提供互联网带宽租用服务，带宽提供方应为一级运营商
可靠性要求	须提供多线运营商接入服务，保证服务稳定可靠。
可操作性	支持通过云管理平台，实现申请部署与使用
互联网 IP 地址租用服务	可提供 IPV4/IPV6 互联网 IP 地址租用服务
网站域名备案服务	配合使用单位完成网站域名备案
可操作性	支持通过云管理平台，实现申请部署与使用

3.2.1.10 主机负载均衡服务

指标项	规格要求
服务能力	通过云管理平台实现针每租户按需自动分配负载均衡服务的能力。总体峰值可支持每秒新建链接数不少于40万
均衡策略	支持加权轮询(Weighted Round Robin)、加权最小连接数调度(Weighted Least-Connection Scheduling)等流量分发策略
健康检查	可以按照指定规则对配置的虚拟主机进行健康检查，自动隔离异常状态虚拟主机，确保可用性
会话（Session）保持	可对虚拟主机提供TCP/HTTP协议的负载均衡服务，并提供会话保持功能，在会话生命周期内，将同一会话请求转发到同一台后端虚拟主机
高可用性	采用全冗余或集群架构，无单点故障；平均可用性不低于99.99%

转发规则	提供多种转发规则，满足不同业务场景的要求
扩展性	支持在线平滑升级，承载能力和网络总带宽同步线性扩容；可与虚拟主机配合提供三层架构系统的弹性扩展
可操作性	支持通过云管理平台，实现申请部署与使用
协议支持	提供 4 层（TCP 协议）和 7 层（HTTP 和 HTTPS 协议）的负载均衡服务

3.2.1.11 远程接入服务

指标项	规格要求
功能要求	提供堡垒机远程接入服务
运维审计	字符操作审计、图形操作审计、文件操作审计
访问控制	支持基于IP/IP段、用户/用户组、资产/资产组、协议、危险级别等组合策略进行访问控制，对于不合法的行为予以阻断；
	可基于运维账号的登陆时间和资产登陆时间进行访问控制；
	可基于运维操作命令进行访问控制；
	可基于主机、用户、IP地址控制审计日志的访问权限；

3.2.1.12 VPN 服务

1. SSL VPN接入

指标项	规格要求
接入方式	实现Web接入，TCP接入，IP接入等多种方式，记录完整的用户访问日志
身份管理	支持基于用户身份的管理，实现不同身份的用户拥有不同的命令执行权限，并且支持用户视图分级，对于不同级别的用户赋予不同的管理配置权限
访问控制策略	可以根据请求报文的目的IP地址和目的端口号、源IP地址和源端口号进行过滤
密码要求	采用通过商用密码产品认证的SSL VPN产品

2. IPSec VPN接入

指标项	规格要求
配置方式	通过手工配置或自动配置的方式实现IPSecVPN隧道的建立，支持对IKE策略、IPSec策略配置及对VPN服务、IPSec站点连接的申请并提供状态监控，记录完整的用户访问日志
基本功能	实现IPsec抗重放检测功能、反向路由注入功能，支持IPv6协议

密码要求	采用通过商用密码产品认证的IPSEC VPN产品

3.2.1.13 SSL 证书服务

提供域名 SSL 证书服务，可支持服务器、负载均衡等设备部署配置，实现数据信息在客户端和服务器之间的加密传输，可以防止数据信息的泄露，保证信息传递的安全性。

3.2.1.14 WAF 防护

指标项	规格要求
检测算法	可精确识别包括注入、XSS等OWASP Top 10 WEB通用攻击，有效应对盗链、跨站请求伪造等WEB特殊攻击
部署方式	可以通过透明串接或反向代理、路由模式等方式接入网络中，即可对应用层HTTP流量进行安全防护
黑名单	通过预定义策略及自定义规则，进行规则匹配，阻断异常流量
可操作性	支持通过云管理平台，实现申请部署与使用

3.2.2基础安全保障服务要求

云服务商须具备下列云基础安全保障服务能力并免费向使用单位提供。

3.2.2.1 安全管理服务：运维人员管理

指标项	规格要求
岗位设置	设立系统管理员、网络管理员、安全管理员等岗位，并定义各个工作岗位的职责
人员配备	至少配备的系统管理员、网络管理员、安全管理员各一名
授权和审批	根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人
离岗管理	及时终止离岗员工的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备

3.2.2.2 安全管理服务：机房运维管理

指标项	规格要求
机房运维管理	指定专门的部门或人员负责机房安全，对机房出入进行管理，定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理
	建立机房安全管理制度，对有关机房物理访问，物品带进、带出机房和机房环境安全等方面的管理做出规定
	机房应设置温、湿度自动调节设施，使机房温、湿度的变化在设备运行所允许的范围之内
	不允许在重要区域接待来访人员、公开区域上没有包含敏感信息的纸档文件、移动介质等

3.2.2.3 安全管理服务：应急演练

指标项	规格要求
应急演练	制定云平台重要事件的应急预案，包括应急处理流程、系统恢复流程等内容；提出上云业务系统应急演练的指导方案，配合完成业务系统应急演练。
	从人力、设备、技术和财务等方面确保应急预案的执行有足够的资源保障
	定期对系统相关的人员进行应急预案培训，并进行应急预案的演练；每年至少开展1次云平台应急演练。

3.2.2.4 安全技术服务：物理访问控制

指标项	规格要求
物理访问控制	机房出入口安排专人值守，控制、鉴别和记录进入的人员
	需进入机房的来访人员须经过申请和审批流程，并限制和监控其活动范围
	对机房划分区域进行管理，区域和区域之间设置物理隔离装置，在重要区域前设置交付或安装等过渡区域
	重要区域应配置电子门禁系统，控制、鉴别和记录进入的人员，采用符合国家密码管理部门要求的密码技术保证电子门禁系统进出记录的完整性

3.2.2.5 安全技术服务：机房三防服务

指标项	规格要求
机房环境	机房具有防震、防风和防雨
	机房安装防雷和接地线，设置防雷保安器，防止感应雷，要求防雷接地和机房接地分别安装，且相隔一定的距离
	机房应采取区域隔离防火措施，将重要设备与其他设备隔离开
	机房利用光、电等技术设置机房防盗报警系统，并采用符合国家密码管理部门要求的密码技术保证视频监控音像记录的完整性

3.2.2.6 安全技术服务：设备访问审计

指标项	规格要求
运维审计	字符操作审计、图形操作审计、文件操作审计
访问控制	支持基于IP/IP段、用户/用户组、资产/资产组、协议、危险级别等组合策略进行访问控制，对于不合法的行为予以阻断；
	可基于运维账号的登陆时间和资产登陆时间进行访问控制；
	可基于运维操作命令进行访问控制;对特定命令的执行需要更高级管理员授权才能执行。

	可基于主机、用户、IP地址控制审计日志的访问权限；
	对运维设备的账号密码强度进行自动核查，及时发现设备弱口令。

3.2.2.7 安全技术服务：出口流量监测

指标项	规格要求
用户行为审计	支持基于IP、端口等自定义协议服务；
	内置URL分类库，支持约100个URL分类，URL库可在线升级
	支持自定义URL过滤，并支持URL的模糊匹配，提供web界面配置截图
	支持自定义关键字对象，在应用控制的时候可选择“包含”、“不包含”、“等于”、“不等于”四种匹配模式，匹配类型包含关键字和数字，提供web界面配置截图
	支持应用、用户流量统计，应用流量支持趋势图、饼状图呈现，可查看某一应用的流量趋势图和其Top流量用户

3.2.2.8 安全技术服务：本地 DDoS 防护

指标项	规格要求
引流方式	支持旁路（Offline）工作模式。当发生DDoS攻击时，清洗设备通过BGP路由宣告的方式将去往被保护目标的流量牵引导入到设备处理
流量清洗	实现对Syn flood、ICMP flood、Ack flood、Syn+Ack Flood 、DNS query request flood、TCP连接耗尽、HTTP Get Flood（含CC）、UDP FLOOD攻击、TCP FIN攻击、TCP UDP混合攻击等攻击流量的清洗；支持导入SSL证书对HTTPS流量进行防护
基本功能	支持流量过滤、反欺骗、异常流量识别、协议分析和速率限制功能，支持用户黑白名单功能，支持恶意流量识别和分离，保障正常访问流量的正常通过不受影响
流量回注	设备支持干净流量回注到业务系统中去 支持配合云清洗平台形成混合清洗解决方案，解决出口带宽拥塞情况下的攻击防护； 支持对CDN、云清洗等使用代理源IP的流量进行防护，并对代理前真实源IP进行告警记录和黑名单过滤。

3.2.2.9 安全技术服务：防火墙安全防护

指标项	规格要求
攻击防范	ARP欺骗攻击、TCP报文标志位不合法攻击、Large ICMP报文攻击、地址扫描攻击和端口扫描攻击等多种恶意攻击，同时支持黑名单、MAC绑定、内容过滤等功能
NAT支持	提供多对一、多对多、静态网段、双向转换 、Easy IP和DNS映射等NAT应用方式；支持多种应用协议正确穿越NAT，提供DNS、FTP、H.323、NBT等NAT ALG功能

增强状态安全过滤	实现基础、扩展和基于接口的状态检测包过滤技术；支持对每一个连接状态信息的维护监测并动态地过滤数据包，支持对应用层协议的状态监控

3.2.2.10 安全技术服务：防入侵监测 IPS

指标项	规格要求
入侵防御能力	具有流量模型自学习能力，当短时间内大规模爆发的病毒导致网络流量激增时，能自动发现并阻断攻击和异常流量，以保护路由器、交换机、VoIP系统、DNS服务器等网络基础设施免遭各种恶意攻击
零时差防护	同步全球知名安全组织和厂商发布的安全公告，能够及时更新特征库，以定期（每周）和紧急（当重大安全漏洞被发现）两种方式发布，并自动或手动地分发到IPS设备中 应具备攻击快照功能，详细记录触发告警的数据特征，以便做进一步的事件分析

3.2.2.11 安全技术服务：远程接入服务

指标项	规格要求
操作审计	多面记录运维人员的操作行为，作为事件追溯的保障和事故分析的依据。
职权管控	通过账号管控和权限组管理，实现分职权进行人员和资产的管理。
安全认证	引入双因子认证机制，防止运维人员身份冒用和复用。

3.2.2.12 安全技术服务：租户隔离

指标项	规格要求
实现方式	应实现云计算环境业务网络的有效隔离，包括云服务客户使用的基础设施、云服务方的管理网络以及内部局域网。应制定各应用系统的访问控制策略并实时监控策略的有效性
VPC资源池	部门业务区中，云服务方应为不同的云服务客户分配不同的VPC，每个VPC之间不能直接进行通信，同时解决不同云服务客户间可能产生的地址重叠问题
安全防护	云服务方应具备为每个云服务客户提供独立安全服务的能力，其安全防护设备的安全策略应与云服务客户共享，应对安全策略实施的有效性进行监测和控制
权限	云服务客户拥有VPC内部信息系统和数据完整的使用权和管理权
部署模式	具备将VPC内部流量通过隧道等技术导出到物理或虚拟安全防护设备的能力

3.2.2.13 安全技术服务：租户内部访问控制

指标项	规格要求

租户内安全	以虚拟机为单位，为不同用户提供2～7层的安全防护
访问路径可定义	根据云租户的业务要求定义安全访问路径，实现租户内业务系统间的访问安全

3.2.2.14 安全技术服务：云主机监控

指标项	规格要求
监控内容	管理员可以监控云主机的运行状况，包括CPU、内存、磁盘利用率以及网络流量等。
统计报表	支持输出云主机监控统计报表
监控告警	云主机资源告警项支持主机CPU利用率、内存利用率、磁盘分区利用率、网络流量告警设置

3.2.2.15 安全技术服务：角色权限管理

指标项	规格要求
权限分类	可以划分系统管理员、租户管理员、用户等多种用户权限类别
权限管理	上级管理员可以创建下级管理员以及下级用户，并可以对其权限进行设置
权限调整	上级管理员可以对下级管理员以及下级用户的权限进行调整
权限监督	系统管理员无权获取租户内的云主机操作系统管理权限，无权读取用户的业务数据
	管理员对于角色权限的操作要求能够被记录、监督

3.2.2.16 安全技术服务：监控平台接入服务

指标项	规格要求
接入内容	租户管辖内的云资源监控数据
接入方式	接口调用

3.2.2.17 安全技术服务：云主机深度监控服务

指标项	规格要求
云主机深度监控	提供云主机7*24小时深度监控服务，并提供相应报告
集中告警监控	支持多维度告警/事件展现
Top性能监控	提供常用指标的 TopN 性能视图，包括： 1） 服务器、虚拟机的CPU、内存TopN视图； 2） 网络接口流量； 3） 存储读写带宽、读写IOPS、读写IO大小。

安全事件服务	提供主机安全事件的验证、分析，并提供事件报告
应急处置服务	提供特定云主机的应急问题协助排查，协助处理应用故障等服务，并提供相应报告
值守保障服务	提供7x24小时的机房内或远程运维值守工作，不仅限于机房巡检、云平台和硬件监控，同时提供问题排查协助、协助处理应用故障等服务，并提供相应报告

为了实现政务云高效运维管理，云服务提供商需将上述监控数据对接至政务云监管平台。

3.2.3扩展服务能力要求

3.2.3.1 商用操作系统套餐

提供主流商业操作系统服务，应支持 Windows Server、国产 Linux 操作系统（银河麒麟/中标麒麟/统信等）的各种主流版本，并提供操作系统的安装部署和各种故障处理。

3.2.3.2 开源操作系统套餐

提供主流开源操作系统服务，应支持 Ubuntu 等主流 Linux 操作系统的各种版本，并提供操作系统的安装部署和各种故障处理。

3.2.3.3 国产商用应用中间件套餐

提供主流国产商用中间件服务，应支持金蝶、东方通、普元等 3 种以上国产中间件的主流版本，并提供中间件的安装部署以及各种故障处理和日常维护。

3.2.3.4 开源应用中间件套餐

提供主流开源中间件服务，应支持 Tomcat 等中间件的各种版本，并提供中间件的安装部署和各种故障处理和日常维护。

3.2.3.5 商用数据库套餐

提供主流国产商用数据库服务，应支持 3 种以上国产数据库单机、集群的主流版本，提供数据库的安装部署和各种故障处理及日常维护。

3.2.3.6 开源数据库套餐

提供主流开源数据库服务，应支持 MYSQL 数据库的主流版本，提供数据库的安装部署和各种故障处理及配置优化，提供数据库日常维护。

3.2.3.7 云原生数据库（集中式）服务

提供云原生关系型数据库，支持高可用架构。

3.2.3.8 云原生数据库（分布式）服务

提供云原生关系型数据库，采用分布式架构，支持分库分表、全局索引等能力。

3.2.3.9 内存型数据库（分布式缓存 redis)服务

提供内存型数据库（分布式缓存 redis)服务，兼容开源 Redis 协议标准，支持多版本存储引擎，拥有数据可持久化存储、可用性高、弹性扩展和智能运维等特性。

3.2.3.10容器服务

提供容器服务，支持 Docker 镜像，支持多个 Kubernetes 版本，提供集群管理、容器生命周期管理能力。

3.2.3.11微服务框架

提供微服务框架，支持应用托管和微服务管理，支持应用托管和微服务管理，支持基于原生 SpringCloud、Dubbo 等应用托管。

3.2.3.12消息队列服务

提供消息队列服务，消息队列支持 RocketMQ 和 kafka。消息队列（RocketMQ）提供消息订阅和发布、消息轨迹查询、定时（延时）消息、资源统计等能力，提供 TCP 协议和 HTTP 协议层面的接入方式，支持 Java、C++、.NET 等多种编程语言。消息队列(kafka)兼容开源 Apache Kafka,可直接使用开源 Apache Kafka 客户端与消息队列 Kafka 版通讯。

3.2.3.13API网关服务

提供 API 网关服务，支持 API 服务总线、API 组织管理和 API 运维监控等功能。

3.2.3.14应用监控服务

提供应用监控服务，能够对应用进行全方位监控，支持自动生成应用拓扑，快速定位出错误接口和慢接口（慢 SQL）、重现调用参数、发现系统瓶颈。

3.2.3.15 迁移服务

提供整体的业务上云迁移服务，应支持（包含 X86、ARM、C86）云主机迁移、（包含 X86、ARM、C86）物理主机迁移、单机数据库迁移、高可用数据库迁移等迁移场景。负责需求调研、架构规划设计、应用迁移部署等工作。

3.2.3.16 云端抗 DDOS 服务

利用云端海量带宽资源，提供 DDoS 防护服务，为云内应用系统抵御大流量分布式拒绝服务攻击。

3.2.3.17 云端 APT 防护服务

通过 APT 防护服务，实现恶意代码检测、恶意软件检测及攻击溯源。

3.2.3.18 网页防篡改

通过防篡改软件对网站页面进行实时防护，减少用户页面被恶意篡改的可能性。

3.2.3.19 数据库审计服务

对数据库操作行为进行细粒度审计的合规性管理,对数据库遭受到的风险行为进行告警,对攻击行为进行阻断。对用户访问数据库行为的记录、分析和汇报，生成合规报告以及事故追根溯源。

3.2.3.20 主机杀毒服务

通过杀毒软件，对云主机进行定期的病毒查杀，杀毒软件集中控制。

3.2.3.21 主机防护服务

提供符合等保三级要求的主机权限管理及安全防护。可对主机系统安全涉及的控制点形

成立体防护。

3.2.3.22 主机日志审计服务

对主机系统日志进行采集分析处理，用于发现各种安全威胁、异常行为事件。主机系统日志应集中存储，且日志存储时间不低于 6 个月。

3.2.3.23 主机漏洞扫描

基于漏洞数据库，通过扫描等手段对主机安全脆弱性进行检测。

3.2.3.24 主机安全加固

根据主机漏洞扫描结果对操作系统暴露的安全问题进行系统加固。

3.2.3.25 CDN 加速

支持对静态页面、静态图片、流媒体点播直播、动态内容等内容资源，CDN 核心节点从源站获取分发资源，分级分发到响应的边缘节点，保证用户能到最近及响应最好的节点中访问响应的资源。提供按流量和按带宽两种计费方式。

3.2.3.26 密码应用安全支撑服务

基于符合国家密码要求的密码产品或服务，提供弹性、高可用、高性能的身份认证、数据加解密、数据安全传输、签名验签、密钥管理等密码应用安全支撑服务，以支持云上系统采用符合国家密码管理部门要求的密码技术保障系统安全。

3.2.3.27 短信服务

提供短信平台服务，支持各种操作系统和开发语言，支持二次开发，并可将短信接口嵌入到业务系统中，满足短信发送、验证、管理等功能。

四、云服务商服务要求

4.1服务要求

4.1.1云服务管理体系建设

云服务商可参考以下管理制度要求，在响应文件中制定云服务商管理制度体系，并按照云管理单位要求，调整完善相关制度规范。

4.1.1.1 云服务商服务水平规范

云服务商服务水平规范应全面体现云服务商所提供的云服务能力，云服务商在与使用单位签订服务协议时应遵守规范要求，如用户需求与规范不一致，应在服务协议中明确差异。云平台投入运行后，规范将在相关网站发布公示。规范可参考如下要求：

（1）云平台整体服务能力

云服务介绍；各方权利义务、责任边界、服务规则（服务开通、费用、中止或终止）、第三方产品或服务、服务费抵扣索赔、服务级别协议排除项等。

（2）云服务目录交付质量

应根据采购文件要求及服务目录内容给出量化指标，具体内容要求应包括但不限于：服务内容说明、服务水平级别目标（如可用性、响应能力、故障恢复能力、可审查性等）、服

务交付物、服务变更流程、各方职责义务、补偿方式等。

4.1.1.2 云服务申请规范

本规范适用使用单位申请云服务使用，云服务商应根据本次采购服务目录输出申请规范，实现对用户信息、入云系统信息、云资源分配信息、配套服务信息等用户及需求信息的严格管理。

4.1.1.3 运维管理规范

为了保障平台的服务质量，云服务商应基于 ITSS 运维管理最佳实践编制运维管理流程，规范包括但不限于：事件/故障管理流程、变更管理流程、资源管理流程、监控与告警管理流程、备份与恢复管理流程等。

4.1.1.4 服务退出规范

规范包括但不限于：退出时间计划、业务迁移方案、数据处理流程、硬件设备处理方案、保密方案等。

4.1.1.5 安全管理规范

云服务商需根据等保三级要求、密码应用基本要求、中央网信办要求进行编制。

4.1.1.6 业务迁移规范

规范包括但不限于：现在业务调研内容、迁移流程、迁移风险评估、迁移验证方法、迁移效果跟踪等。

4.1.1.7 应急响应规范

提出云平台应急预案、应急流程规范和云平台应急演练要求，并指导用户开展业务系统应急演练。

4.1.1.8 数据安全管理规范

提出云平台的数据安全管理要求。

云服务标准化要求	系统迁移	配合使用单位方完成入云迁移，并免费开展不同云节点间的系统迁移。
	测试要求	在业务系统入云前云服务商应至少开展适应性测试，并与使用单位共同开展入云系统的安全检测。
	基于数据的服务要求	云服务商应具备对云平台运行数据的安全管理能力，能向使用单位提供其所需的入云系统及云资源运行数据。
	服务响应要求	为最终用户提供技术服务热线(7*24 小时)， 负责解答用户在云平台使用中遇到的问题，并及时提出解决问题的建议和操作方法，方式应包括邮件、电话、即时通讯工具等；在服务期内，提供 7*24 小时的现场和技术支持服务，对故障 15 分钟内响应；2 小时内到达云机房。如果逾期未作出响应，承担由于故障所造成的全部损失。
	运维管理制度及规范要求	云服务商应遵循政务云或行业云相关管理办法及运维相关管理制度和流程开展工作，并具备清晰的内部管理框架和完善的管理方案。云服务商需制订满足自身业务需要的云服务相关制度、标准、规范和办法，定期为项目成员和使用单位提供相关培训服务。

4.1.2云平台运行维护要求

4.1.2.1 运维管理系统和数据分析要求

运维系统可以同时满足云服务商和使用单位各自运维需求，不应仅限于云 IaaS 层资源的监控和管理，应结合使用单位需求和云管理单位的管理要求，建立起较为全面、及时的监控和预警体系，实现对使用单位、业务系统、云资源及各类资产的统一管理、统计和展示，并能够向云管理单位提供各类基础信息。在此基础上，不断发展基于云平台各类基础信息的数据分析和展示能力。基础信息不包括任何用户业务数据。

（1）基本能力：运维管理系统需要对物理服务器、网络设备、存储设备、网络带宽资源，以及虚拟化平台、云主机、操作系统、数据库、中间件/应用服务器等资源进行统一的资源监控，全面覆盖数据中心的监控和管理需求。快速发现和展示网络、主机、存储、应用、虚拟化等资源间的连接关系，并从网络、应用等不用视角进行展示和查看；告警和与资源关联，动态展示全局告警情况，将整个数据中心运行状态直观呈现。具备对云内运行的业务系统可用性监控等能力，结合云主机、云资源监控为用户提供较为全面的监控和及时通知服务。支持对各业务系统相关的软硬件设备进行监控，并能对各类监控状态提供方便的展示方式。能够提供灵活的配置，使不同应用系统的管理员能够方便的看到各自所管理的应用系统相关软硬件设备的监控状态，并支持分层和分子系统的横纵向切分，横向为各个业务系统的各个子系统，纵向包括网络层、硬件层、操作系统、中间件、数据库、存储、业务等。

（2）能力提升：在基本能力基础上，定制实现的辅助管理和展示功能，包括但不限于：用户信息、业务系统信息、云主机信息等基础信息的管理，各类型资产管理和虚拟资产管理，工单管理，巡检管理，按用户需求定制的各类统计报告模板，面向云管理单位和使用单位的及时通知工具（如自动短信或电话）等。运维管理系统应对使用单位业务系统所申请的云服务内容和数量、云服务使用情况、云资源使用情况、服务申请工单、安全策略申请工单等进行统计和展示。具备支撑对使用单位使用云资源的绩效情况统计能力。

（3）数据分析和展示：云服务商应发展基于云平台各类基础信息的数据分析和展示能力，通过应用数据分析云平台底层各类数据，对内发现和解决云平台技术隐患，不断提高运维能力；对外为使用单位提供使用指导，提高服务水平和服务价值。包括但不限于：对云平台各类硬件和虚拟化资产的运行和使用效率情况、流量日志、监控预警等云平台底层数据的分析，为云平台运维和使用单位提供发现问题和咨询服务的能力，如发现云平台隐患和故障，向使用单位提供合理云资源配置建议，发现云内业务系统的安全和系统功能、性能方面可能存在的不足等。

4.1.2.2 资源管理要求

（1）云服务商应对自身云资源池容量进行管理，对资源总量（计算、存储、带宽）及已分配资源、未分配资源进行监控，当平台某资源的已分配量超过该资源总量 80%时，须承诺实现 7 个自然日快速扩容。

（2）云服务商需要保障基础设施资源可扩展性，满足所有用户需求，能够在多租户网络流量条件下，对用户网络流量进行识别并进行精细化管理。

（3）云服务商应具备资源动态调整机制，根据业务系统运行情况进行资源的动态调整，并承诺短期内提供免费的云资源扩展服务（不超过原有资源的 20%）。

（4）云服务商应按内存不复用方式分配云资源。

4.1.2.3 云平台监控要求

（1）云服务商应结合使用单位需求和云管理单位的管理要求，建立起较为全面、及时的监控和预警体系，实现对使用单位业务系统、云资源的统一管理和统计，并能够向云管理单位提供各类基础信息。

（2）云服务商需要对物理服务器、网络设备、存储设备、网络带宽资源，以及虚拟化平台、云主机、操作系统、数据库、中间件/应用服务器等资源进行统一的资源监控，全面覆盖数据中心的监控和管理需求。快速发现和展示网络、主机、存储、应用、虚拟化等资源间的连接关系，告警和与资源关联，动态展示全局告警情况，将整个数据中心运行状态直观呈现。具备对云内运行的业务系统可用性监控等能力，结合云主机、云资源监控为用户提供较为全面的监控和及时通知服务。

（3）云服务商应提供 7x24 小时的运维值守工作，不仅限于机房巡检、云平台和硬件监控，同时提供问题排查协助、协助处理应用故障等服务，并提供相应报告。

（4）云服务商制定严格的日常巡检计划，定期对云平台的服务器、操作系统、云平台软件、存储、网络 设备、数据库、机房环境、传输专线和其他相关设备进行巡检，巡检周期不可超过一周时间，巡检记录需要保存 2 年。

4.1.2.4 云平台运维管理要求

（1）云服务商应服从云管理单位的管理，协助建立服务云运维管理体系、管理制度并切实执行。

（2）云服务商应遵循市级政务云相关管理办法及运维相关管理制度和流程开展工作，并具备清晰的内部管理框架和完善的管理方案。云服务商需制订满足自身业务需要的服务相关制度、标准、规范和办法。

（3）云服务商需要能够对云基础设施、平台软件提供集中运维管理、监控，包括虚拟化、服务器、存储、网络、安全等，可以实现资源利用率可视化，为使用单位提供单个用户内的业务可视化，定位事件、问题和故障，实现事前预测及告警、事中及时处理和事后可审计。

（4）为了保障平台的服务质量，云服务商应基于 ITSS 运维管理最佳实践编制运维管理流程，规范包括 但不限于：事件/故障管理流程、变更管理流程、资源管理流程、监控与告警管理流程、备份与恢复管理流程等。

（5）云服务商应配置独立的运维团队，提供 7x24 小时的运维值守工作，不仅限于机

房巡检、云平台和硬件监控，同时提供问题排查协助、协助处理应用故障等服务，并提供相应报告。承诺运维需求平均响应时间小于等于15分钟，平均故障恢复时间小于等于30分钟，为本项目设置合理的运维团队。

（6）云服务商应根据事件可能的影响范围和时间对事件定级，并根据管理单位的相关规定对各等级事件制定事件处理和上报流程，将事件的影响范围和影响时间最小化。

（7）云服务商需保证所提供文档、数据的真实性和有效性。

（8）云服务商需提供知识库工具作为日常运维管理工作中经验累积沉淀工具，运维人员可以通过知识库 功能很方便地实现对于知识的新建、审批、分类、查询、统计、管理等操作。

（9）云服务商应根据用户需要提供备份/快照功能，防止存储故障导致数据丢失，并可以实现云主机的全量备份、增量备份，支持备份周期、备份策略的设定。

（10）云服务商应根据需要对平台相关设备、业务配置数据、数据库等制订备份作业计划，并指定专人定期进行数据备份，同时按照备份方案中数据管理的要求进行备份数据的管理，确保备份数据可恢复。

4.1.2.5 日常安全管理要求

（1）制定严格的云机房出入管理制度；需要对人员的出入进行记录，记录保存期限最短为 1 年，并接受出入记录审计；

（2）云服务商需要做好云机房内的用电安全、防火安全和防水安全等基础设施安全；

（3）云服务商需要制定完善的云机房内部物理设备安全操作流程及安全操作步骤，需要能够对操作流程及操作过程进行记录；记录保存最短保存期限为 1 年；并接受出入记录审计；

（4）为了保证云平台的安全、稳定运营，云服务商需要制定完善的安全运维管理体系，制定完善的安全管理制度规范，对不同的安全区域、安全保护对象明确安全责任人；

（5）云服务商需要提供符合网络安全等级保护第三级要求的云平台基础安全和应用系统安全的服务内容，从而为使用单位提供安全服务支撑；

（6）云服务商的安全服务包括不限于如下服务：VPC、安全组、云用户业务隔离、安全漏扫、安全审计系统、虚拟化安全等；

（7）云服务商要做好各自的信息安全监控，安全监控内容包含但不限于网络流量监控、各个安全设备的日志记录监控、安全设备运维操作监控和云资源运行状态监控等，可以无条件供云管理单位查看调取；

（8）云服务商提供基于用户的不同等级安全服务，并提供安全事态分析，满足用户不同安全级别业务系统的安全需求。

4.1.2.6 应急保障要求

（1）云服务商应在市级政务云整体应急预案框架下，结合自身情况编写各自应急预案，

规范管理应急过程中的信息报送。

（2）云服务商应急预案应包含综合应急预案、专项应急预案、现场处置方案等。应急预案内容应包含总则、组织机构与职责、监测与预警、应急处置、调查与评估、预防工作、保障措施等方面内容。

（3）云服务商每 2 个月开展一次应急响应培训，每年开展不少于一次应急演练工作。

（4）按照云管理单位预警通知，云服商应组织开展预警响应工作，做好风险评估、应急准备和风险控制工作。各云服务商须及时报告事态发展情况，有关重大事项应及时通报市应急处置中心。

4.1.2.7 运维知识库体系建设要求

云服务商需提供知识库工具作为日常运维管理工作中经验累积沉淀工具，运维人员可以通过知识库功能很方便地实现对于知识的新建、审批、分类、查询、统计、管理等操作。

4.1.2.8 PaaS 和 SaaS 服务扩展要求

云服务商需具备 PaaS 及 SaaS 服务扩展能力，能够基于自身云平台适配多样化服务，包括但不限于：容器服务、微服务框架、大数据服务、数据仓库服务、人脸识别服务等。

4.1.2.9 PaaS 和 SaaS 服务部署备案要求

允许以云服务商为主发展云生态圈，但应就服务内容和价格、服务水平、监测手段等向管理单位备案。

4.1.3 业务迁移服务要求

4.1.3.1 业务系统迁移入云要求

云服务商在业务迁移入云阶段应提供上云咨询服务、迁移实施方案、迁移测试服务、迁移实施服务等服务。业务系统在向云平台迁移的过程中要做到无缝迁移，提供成熟的 P2V、V2V 迁移工具，并确保系统的完整性、兼容性以及数据安全。迁移流程包括：业务环境调研、迁移方案论证、云服务商环境兼容性测试、业务迁移开展及结束等阶段。

（1）应用迁移由云服务商提供的，云服务商主要负责具体应用系统、操作系统、中间件及数据库的迁移等工作；使用单位应组织完成系统联调和业务验证。

云服务商完成迁移前调研并与使用单位制定迁移方案后，3 个工作日内完成云基础资源发放及迁移相关的网络、存储等云资源配置（含测试环境），由云服务商提供针对 X86 云主机或 X86 物理主机迁移的，迁移主机数量少于 20 台，5 个工作日内完成迁移工作；迁移主机数量在 20 台以上的，或数据量超过 10TB 的业务系统，原则上每个业务系统的迁移效率不低于每天 4 台主机。

（2）应用迁移由第三方服务商提供的，云服务商应免费配合完成系统迁移工作，搭建系统入云所需的测试环境，并在测试期内免费配合迁移测试；第三方服务商负责整体迁移工作。

云服务商与使用单位制定迁移方案，并接到使用单位提出的云资源需求后，3 个工作日

内完成云基础资源发放及迁移相关的网络、存储等云资源配置（含测试环境）。

在迁移测试过程中，云服务商需协助搭建测试环境，与云平台业务区域隔离。在业务系统入云前云服务商应至少开展适应性测试，并与使用单位共同开展入云系统的安全检测。

云服务商应提供原厂迁移工具及工具迁移方案，支撑 P2V、V2V 等，提供物理机到虚拟机迁移服务、虚拟机到虚拟机迁移服务及主流数据库的迁移服务；提供原厂数据库迁移工具将异构关系型数据库迁移到云平台的数据库。

4.1.3.2 多业务集中迁移要求

云服务商应具备同时应对多使用单位、多信息系统同时迁移入云的服务支撑能力、资源快速扩容能力、快速迁移工具支持能力，具备成熟的迁移工具，对多系统集中迁移可能出现的难点、风险有较为充分的预判并提出解决对策。云服务商应在响应文件中阐述的对该场景下集中迁移工作的理解、服务方案、支撑能力及可行的应急预案，并保证不低于“业务系统迁移入云要求”中提出的迁移进度要求。

4.1.3.3 跨云平台的业务迁移要求

云服务商之间需互相配合，提供跨云平台业务迁移所需的配合和技术支持。

（1）通过迁移工具进行云主机导入导出

迁入云服务商负责提供迁移工具、存储设备、服务器等相关工具，并在迁移工作开始前负责迁移可行性的评估、迁移方案制定、回退方案制定等工作；迁出云服务商在迁移周期过程中，配合迁入云服务商开展相关工作；使用单位应组织系统开发单位配合完成系统联调和业务验证等工作。

（2）通过迁移平台对云主机进行在线迁移

在线迁移应按照业务系统需求，原则上不允许业务系统中断。迁入云服务商负责实施迁移平台及相关配套资源的提供及整体迁移工作;迁出云服务商应提供必要的专线接入支持、带宽、远程接入等业务系统迁移相关资源和人力支持；使用单位应组织系统开发单位配合完成系统联调和业务验证等工作。

云服务商应在响应文件中阐述的对该场景下迁移工作的理解、服务方案、支撑能力及可行的应急预案，并保证不低于文件中提出的迁移进度要求。

云服务商应在响应文件中针对上述四种场景的业务迁移服务制定面向用户的“业务系统迁移技术指导方案”。

4.2服务团队要求

4.2.1服务团队要求

云服务商须根据项目要求安排具备相应资质和经验的专业人员从事本项目工作，确保项目实施队伍的稳定，提供本地化服务，保证担任重要岗位的人员具备相应专业资质。任命 1 名项目经理作为云平台售前和售后的总接口人，常驻现场工作，定期向管理单位汇报工作。

项目实施过程中，云服务商应保证关键岗位人员不能随意变更，如因正当理由需要调整

项目主要人员的，应当提前 1 个月通知云管理单位，获得书面同意后方可更换。

云服务商应配置独立运维团队，为最终用户提供技术服务热线(7*24 小时)，负责解答用户在云平台使用中遇到的问题，并及时提出解决问题的建议和操作方法。

在服务期内，云服务商 7*24 小时运行值班监控，配备具备两年以上云平台维护经验的运维人员，支持电话、网上值班等响应方式，所有运维人员需在半年内获取原厂认证证书。

日常运维：每个节点服务团队不少于 20 人，云计算平台应保证核心服务人员不少于 10 人，客户响应及运维人员不少于 6 人。应设有安全审计员岗位，负责云平台核心设备日志记录审查及运维人员操作记录审查等，定期提出安全审计报告。运维服务人员需具备网络、安全、虚拟化、数据库、操作系统等专业知识和技能，具备两年以上云平台维护经验。

重大活动保障期间：每个节点运维团队不少于 30 人，云计算平台应保证核心服务人员不少于 10 人，云原厂服务人员不少于 4 人，客户响应及运营人员不少于 10 人。

4.2.2保密要求

为确保电子政务系统和信息的安全保密，云服务商需分别与使用单位以及相关运维人员签署保密协议。

4.2.3培训要求

培训工作是云服务商提高运维能力和云服务水平的重要工作之一。云服务商应至少提供以下培训：

1.内部培训

内部培训旨在提高云平台运维能力，规范运维管理。内容包括但不限于：

（1）面向项目管理人员、系统管理人员的培训，确保此类人员能清晰地了解云平台的设计理念和设计方法，掌握云平台的整体结构，以及各类云资源的申请、审核、开通、回收等管理流程。

（2）面向系统维护人员的培训，确保此类人员能理解和掌握云平台的相关技术知识，能够熟练地维护云平台，快速定位和解决系统出现的问题，保证云平台服务期间正常运转，并持续提高运维服务质量。

（3）本单位人员的安全培训教育，确保工作人员符合岗位要求。

（4）云平台维护人员的定期业务培训和保密培训，重保前的业务培训和应急保障培训等。

（5）面向管理单位的培训，确保此类人员充分了解云平台的技术架构、服务水平等。

2.外部培训

云服务商应根据本项目的特点制定培训方案并提供培训，负责安排专业培训讲师授课，并提供全套培训教材和培训课程计划表，培训课程涵盖云平台使用和管理培训，使使用单位在培训后能够独立使用相关服务功能，而不必依赖云服务商现场指导。云服务商每年应组织安排至少一次针对使用单位的系统入云及用户培训，培训规模应至少 100 人次。云服务商应

将所有培训费用（含培训教材费）及各项支出计入资源租赁费用中，不单独报价。内容包括但不限于：

（1）面向使用单位和开发人员的技术交流，包括云架构规划咨询、应用系统部署、迁移，云平台运维及其他技术服务。

（2）面向使用单位的培训，确保云平台最终用户能理解和掌握各类云服务的使用方法和操作技巧，能够高效、熟练地基于云平台部署上层业务应用，最终使使用单位在培训后能够独立使用相关服务功能，而不必依赖云服务商现场指导。

（3）面向开发人员的培训，确保其能理解和掌握基于云平台的开发规范，针对具体的业务应用场景能够充分发挥云平台的技术优势，合理地设计上层业务应用的技术架构，制订部署、迁移方案，评估云资源的容量需求。

（4）定期对系统相关的人员进行应急预案培训，并进行应急预案的演练；每年至少开展 1 次云平台应急演练。

云服务商应在此基础上制定具有本单位特色的培训方案。

4.3云服务商管理机制

4.3.1云服务商管理机制概述

响应人入围后，政务云（服务云）、行业云（健康云）、行业云（教育云）分别由行业主管部门按照相关管理规定，从入围云服务商中选择云服务商建设。具体选择条件，由行业主管部门拟定，原则上不低于本采购需求的相关要求。

入围云服务商的选择、评估、评级、退出等相关管理要求由行业主管部门拟定，所有入围云服务商应承诺遵守行业主管部门发布的相关管理规定，否则将视为违约。

4.3.2服务资格评估机制

以下是政务云（服务云）的评估机制，行业云参照执行。

4.3.2.1 云服务商资质动态更新机制和定期审查机制

在服务期内，如国家、北京市政策调整，导致云服务商不再满足提供政务云服务的基本要求，云服务商应在相关政策出台后及时向云管理单位备案，云管理单位应在政务云网站上公示，云服务商应在 3 个月内更新相关运营资质。更新运营资质前不得开展新增业务，该云平台的入云工单等相关审核流程暂停。

服务云管理单位委托云综合监管服务商每年审查云服务商运营资质情况，结果纳入评估评级。对于超过 6 个月未完成运营资质更新的云服务商，服务云管理单位按照退出机制处理。

4.3.2.2 考核机制

为加强建设和服务管理，促进各方持续提高云服务工作质量和效果，本着“争先创优、激励为主、科学评价”的原则，服务云管理单位定期对北京云服务商的云平台能力、云服务商服务能力进行评估考核，并将通过数据分析开展多维度的云服务商评估排名。

管理单位负责管理、监督和指导云服务商相关考核工作，审批和发布考核管理办法、

审核云服务商的考核结果、考核云服务商的工作绩效。云综合监管服务商受管理单位的委托具体执行云服务商考核，负责编制和修订绩效考核管理办法，开展各项考核工作，定期汇报考核结果，跟进各项整改工作，向被考核对象发布考核结果。

云服务商考核包括建设期考核和运维期考核。

4.3.2.2.1 建设期考核

建设期考核包括建设初期考核和建设中期考核。建设初期考核是在云平台初步完成建设并具备基础服务能力后开展的阶段性考核，主要检验云平台功能和性能、云服务商提供服务的基本能力；中期建设考核是在云平台运行一段时间后开展的阶段性考核，主要检验云服务商的服务水平和运维管理的能力。

1.初期建设考核

初期建设考核指在云平台初步完成建设并具备基础服务能力后开展的阶段性考核，旨在检验云平台功能和性能、云服务商提供服务的能力和云服务商持续服务的扩展能力，以确保云平台能够实现支撑基础服务、基础安全保障服务目录要求的所有功能，确保云服务商具备为用户提供标准化服务的能力。

由云管理单位组织，云综合监管服务商协助组织并具体执行对云平台初期建设成果的考核。考核内容包括：

（1）检测云平台基础功能和性能指标是否实现，包括支撑基础服务目录、基础安全保障服务目录相关服务的功能。

（2）审查业务支撑文档，包括 “云服务商服务水平规范”、“业务系统迁移技术指导方案”、“云服务使用流程及模板”、“云内业务系统应急预案及应急演练指导书”， “云运维工作方案及流程”、“云平台安全管理方案”、“云平台应急预案”、“云年度工作计划书”等。

（3）审查云管理平台二次开发计划、云平台扩展功能实现计划。

（4）其他事项。

考核通过后，在政务云网站公示考核结果并发布“云服务商服务水平规范”、“业务系统迁移技术指导方案”、“云服务使用流程及模板”、“云内业务系统应急预案及应急演练指导书”。

考核不通过的云服务商，限期 1 个月整改并做二次考核。两次考核不通过的，服务云管理单位按照退出机制处理。

2.中期建设考核

中期建设考核指在云平台运行 6-12 个月开展的阶段性考核，旨在检验云平台扩展能力的实现及相关运营和技术问题的整改情况，以确保云服务商能够实现采购文件规定的全部要求。

由云管理单位组织，云综合监管服务商协助组织并具体执行对云平台建设成果的考核。考核内容包括：

（1）检测云平台支撑扩展服务的功能和性能指标是否实现；

（2）检查云管理平台二次开发功能是否实现,是否通过等保三级测评、商用密码应用安全性评估和云中央网信办云计算服务安全评估；

（3）抽检云服务商对云管理平台的应用情况，如云主机创建和审核记录、工单记录等；

（4）审查相关整改完成情况（如有）；

（5）审查业务支撑文档的修订情况（如有）。

考核通过后，在政务云网站公示考核结果并发布相关业务支撑文档修订版。

考核不通过的云服务商，视情况在考核后限期 3-6 个月整改并做二次考核。两次考核不通过的，服务云管理单位按照退出机制处理。

4.3.2.2.2 云服务商综合评估

云服务商综合能力评估内容包括但不限于技术更新度、平台安全度、运维规范度、业务专业度、客户满意度等。

1.技术更新度指标

技术更新度指标包括但不限于各个云服务商云主机服务能力、网络质量、监控管理能力、集约化能力等。

2.平台安全度指标

平台安全度指标包括但不限于云平台安全防护能力、漏洞处理能力、应急事件处理能力、备案检查机制、口令和权限管理能力等。

3.运维规范度指标

运维规范度指标包括但不限于：各个云服务商的基础信息完整性、工作合规性（至少包括业务流程合规性、机房运维合规性、数据质量等）、事件响应度、办公及个人环境安全能力、问题解决度等。

4.业务专业度指标

业务专业度指标包括但不限于：各个云服务商的服务资质、应急演练、风险排查等几个方面的专业度指标。

5.客户满意度指标

客户满意度指标包括但不限于：各个云服务商的入云咨询满意度、运维服务满意度、信息通报满意度、服务台满意度、用户投诉、宣传度、推广活跃度、规模增长趋势等。

2021 年开始侧重云平台运维安全能力、数据质量等方面的考察。云平台运维安全能力包括云平台口令和权限管理能力、人员安全管理能力、人员办公环境管理能力、供应链风险管理能力等。数据质量指云服务商管理云平台运行数据的能力。

4.3.2.3 其他

云服务商应在服务方案中提供“云服务质量考核标准”，考核内容应包含但不限于云服务考核标准、合同执行考核标准、违约行为考核标准等，并针对云服务质量考核未达标的情

况，陈述云服务商自愿承担的责任义务和惩戒措施。

五、机房要求

云服务商应在政务云管理单位许可的机房内开展云平台建设。

5.1健康云机房规划和网络要求

1.健康云建设双数据中心，根据国家医疗保障局建设要求和技术规范，需要建设同城双数据中心（即数据中心 A 和数据中心 B），并行运行互为容灾。双数据中心间距应大于 20 公里、小于 50 公里。数据中心 A 医保域提供不少于 60 个连续机柜，连续机柜可扩展至不低于 100 个；为数据中心 B 提供不少于 60 个连续机柜，连续机柜可扩展数量不低于 100 个。承诺根据卫生行业其他需求扩容。

2. 机房应具备互联网条件。云服务商应为行业节点提供互联网双链路服务（不低于运营商一级代理），负责按需提供健康云各节点之间的专线服务。机房应具备部署政务外网的条件（提供接入设备和预留管线空间），政务外网部管理单位提供路由接入点。

5.2教育云机房规划和网络要求

机房应具备互联网条件，云服务商应为各节点提供互联网双链路服务，负责按需提供教育云各节点之间的专线服务。机房应具备北京教育信息网接入，可满足链路带宽上限不低于40Gbps，实际数据带宽根据业务需要动态配置。具备中国教育和科研计算机网（CERNET）接入，物理链路带宽不低于 10Gbps，实际数据带宽根据业务需要动态配置。应具备部署政务外网的条件（提供接入设备和预留管线空间）。

5.3机房技术要求

序号	指标项	技术需求
1	机房选址要求	响应人提供的机房均应位于北京市区域。
2	机房总体要求	响应人提供的机房必须通过验收并具备使用条件。
		机房所在地应交通方便，周边500米范围内不得有下列危险：水灾、泥石流等灾害威胁、国家重点基础设施或重大军事目标、强腐蚀源、污染源、强电磁、有害气体、强震动源、容易发生群体事件场所、易燃易爆源。
		提供服务的数据中心应具有极高的安全性、可用性设计，包括建筑结构、系统冗余能力、物理安全考虑、人员设备控制、消防安全考虑、应急能力、防电磁辐射、防雷、防水、防静电等。
		响应人所提供的机房具有合法的使用权。
		响应人在服务期内提供独立的、不少于60平米的办公场所及办公条件，满足驻场运维需要。同时提供一个用以临时存放数据中心相关设备等的独立库房。
3	机房定制化要求	（1）机房区域要求为连续、独立的模块间内，根据采购人要求，对机房区域封闭隔离，确保数据中心独立、专享。 （2）机房所在区域需安装视频监控录像装置，连续视频监控记录应保

序号	指标项	技术需求
		存至少 90 天，机房实行封闭式管理，机房应设置防盗报警系统。 （3）响应人应对机房所在区域出入人员身份执行审批审核流程，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 365 天。
4	机柜要求	（1）机柜需满足标准 19 英寸机架设备安装上架要求，机柜尺寸不小于 600mm×1100mm×2000mm，可用空间不小于 40U，机柜内置走线槽及盘线器。每机柜承重不低于 800KG，机柜内托盘或托架数量可满足设备上架要求，每个托架或托盘要求承重不小于 80KG。 （2）单机柜的满配功率不低于 4KW。
5	机房综合布线要求	响应人需根据采购人需求在机柜所在机房区域内完成综合布线，线缆敷设在所在区域桥架机柜内，对强弱电进行分离，规范整齐。所在区域内的线缆按照采购人要求进行标签标识。
		缆线采用线槽或桥架敷设时，线槽或桥架的安装位置应与建筑装饰、电气、空调、消防等专业协调一致。应将通信线缆铺设在专用线槽内，强弱电缆需隔离铺设间隔不小于300mm，并进行统一标识。
		综合布线系统应满足《综合布线系统工程设计规范》(GB 50311—2016）等标准要求。
6	机房建筑要求	机房所在建筑物为机房专用的建筑，并根据信息系统机房应用的特点和特殊需要，在功能分区划分、平面布置和建筑结构上采取相应的技术措施。
		机房所在建筑物抗震等级达到规范标准。
		机房所在建筑物建筑结构安全等级不低于二级、机房耐火等级不低于二级。
		机房活荷载承重量达到规范标准。
		机房外墙体应保持封闭性，并与建筑物外墙体之间留有缓冲区。
		机房应设有专用卸货区域及货运入口，保证大型设备的运输安全。建筑的入口至主机房应设通道及专用货梯。货物、人员通道应保证24小时可以通行。
7	供配电要求	机房采用双路市电供电，两路市电来自不同的供电站。
		IT系统供电与空调等动力供电分开。
		末端配电：每台机柜配置A\B双路PDU（来自不同的UPS系统供电），按需提供不低于16A和32A电源。每台机柜的A\B两路可用电力均不低于16A。
		机房UPS及电池均应采用2N冗余方式。
		满载情况下电池后备时间不低于15分钟，采购人租赁机房区域内每个机柜要求由分别来源于两路UPS的两路电力供应。
		柴油发电机配备2N或(N+X)冗余（X=1～N）后备柴油发电机系统。如未配置柴发系统，可由不同于双路市电线路外的第三路市电供给替代。

序号	指标项	技术需求
8	制冷要求	机房精密空调应配备 2N 或 N+X 冗余（X=1～N）机房专用空调。
		保持机房温度（开机时）23℃±1℃，相对湿度（开机时）40%-60%，不结露。制冷方式：水冷或风冷。
		有漏水隐患处应安装漏水检测装置，针对空调漏水情况能够及时发现和报警。空调机组下方应设置挡水堰，并部署有漏水检测系统，漏水检测系统报警信号接入到环境监控系统，对机房漏水情况进行实时检测和处理。
9	防雷接地要求	机房建筑设置有避雷装置，能够防范直击雷的危害。
		机房应设置交流电源地线，应设置通过国家认证的防雷装置；防止感应雷，采用共用接地系统，在供电系统做好三级防雷措施。
10	消防要求	机房区域的消防系统采用极早期火灾探测报警系统，火灾探测点应采取多层部署方式并具有地址编码及电子地图，接入到火灾自动报警系统，提供集中式灭火报警系统。
		响应人提供服务的机房场地及配电室应设置感温、感烟双重报警系统。采用IG541或FM200环保洁净气体灭火系统。气体释放喷头应采取多路部署，分区灭火方式。IT设备放置的机房区域应无水管经过。
		消防中控室应配置有7×24小时专职消防监控人员，实时监控火灾自动报警系统。
		机房内应设置有独立的消防排烟系统或事故排烟系统。
		响应人提供服务的数据中心的消防设施及管理应符合消防规范要求。
11	多运营商线路接入要求	应满足全部基础运营商和主流运营商互联网、专线、裸光纤以及政务外网接入路由空间，无条件支持线路接入，满足采购人未来的网络接入需求。
		各运营商节点机房为独立空间，传输设备、管井等资源满足多条专线布设开通条件并具备后期扩展能力，传输设备应便于维护。
		机房能够无条件支持电子政务外网的接入，并提供相应的配合和联通联调服务。
12	机房运维要求	机房所在建筑物入口处应安装出入控制和安全防护装置，并对出入人员和所带物品应进行安全检查。
		机房应配备7×24小时值班保安人员，负责机房安全保卫工作。
		机房设有动环监控系统，对机房相关基础设施运行状态和故障进行7×24小时监控。
		机房应配备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。机房的基础设施日常巡检工作，每日巡检次数不少于4次。

序号	指标项	技术需求
		机房区域应为独立、封闭区域，并配置有门禁访问控制措施、视频监控、安全检查措施，并有7×24小时安保人员值班对进出机房的人员、设备进行检查、核实、放行。有多个出入口时，每个出入口都应有人员、设备进出控制措施。
		应为出入口设置门禁控制系统，划分不同人员进出不同区域的权限。未经采购人授权，包括响应人机房工作人员的所有人员随意不得进入。门禁控制系统应保存有完整的人员进出记录，人员进出记录要求至少保留365天。
		入围供应商须保证采购人及指定人员随时进入机房区域进行操作，并配合做好相关运维工作。
		应为机房区域部署高清视频监控系统，实现对所有通道、区域、设备的监控，且监控区域无死角。视频监控数据应至少保存90天且供采购人随时调阅。
		向机房区域提供包括供变配电、UPS、电池、空调及新风系统的设备系统监测服务、运行区温湿度及漏水监测服务、末端配电监测服务。
		在进行机房扩容改造、网络变更、电源改造等重要事项变更时，应提前至少20个工作日通过书面方式通知采购人。
		每季度至少向采购人提供一次服务报告，包括监控及巡检、日常维护、应急处理工作等。

六、★专项承诺

响应人应当就下列内容作出专项承诺：

1. 云平台设计和建设满足网络安全等级保护三级要求，并在建设完成后 6 个月内通过测评，未通过测评的不得投入使用；
2. 云平台设计和建设满足中央网信办云计算服务安全评估要求，并在建设完成后 6 个月内通过审查；
3. 云平台设计和建设满足商用密码应用安全性评估要求，及时组织开展密码应用安全性评估，由第三方测评机构出具《信息系统密码应用安全性评估报告》，并于密评报告出具之日起 30 日内，报市密码管理部门备案；
4. 云平台具备资源动态调整机制，短期内为用户提供免费的云资源扩展服务（不超过原有资源的 20%）；承诺支持应用系统在线迁移；未经允许不得对云平台上的业务数据进行非法截取、加工、分析处理或提供给第三方机构；
5. 提供云平台硬件、软件设备品牌型号，并承诺按此供应设备；云平台硬件设备采用节能环保产品；
6. 云服务商对云资源池容量进行科学管理和监控，平台某资源的已分配量超过该资源总量80%时，须实现 7 个自然日快速扩容；

7. 按照云管理单位和使用单位的管理要求，对云管理平台进行定制开发，不断提升云管理平台能力；
8. 承诺运维需求平均响应时间小于等于 15 分钟，平均故障恢复时间小于等于 30 分钟，为本项目设置合理的运维团队；
9. 提供服务水平协议，明确服务目录中各项服务的服务水平，承诺按此提供服务；
10. 遵守行业主管部门发布的相关管理规定，包括对外正式发布、内部发布共同参照执行的有关规定。
11. 遵循机房管理单位要求，分摊所部署 IT 设备设施的水电费用（IT 设备用电、空调用电、其他用电等费用）和日常管理费用（安保、保洁、物业服务等费用）。

七、服务期及服务地点

1. 服务期：自签订本框架协议之日起两年
2. 服务地点：北京