ICS 35.240.50
CCS L 67

T/STIC

团　　体　　标　　准

T/STIC 120076—2023

桌面及外围设备运维服务规范

Operation and maintenance Service specification for desktop teminal and peripheral

2023－08－10 发布　　2023－08－20 实施

上海市检验检测认证协会　　发 布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由上海市检验检测认证协会提出并归口。

本文件起草单位：上海蓝盟网络技术有限公司、上海蓝盟信息技术有限公司、上海市计算机行业协会、上海微恺信息技术有限公司、上海欧测认证服务有限公司、上海添唯认证技术有限公司。

本文件主要起草人：夏立成、吴威巍、裘维东、佘灏程、陆凌云、谢柯、王栋、孙学刚、蒋文骏、王统、欧阳树生、黄惠杰。

首批承诺执行单位：上海蓝盟网络技术有限公司、上海蓝盟信息技术有限公司、上海市计算机行业协会、上海微恺信息技术有限公司、上海欧测认证服务有限公司。

桌面及外围设备运维服务规范

1 范围

本文件规定了桌面及外围设备运行维护服务在服务设施，服务人员，服务要求等方面的要求。
本文件适用于桌面及外围设备运行维护服务的设计、建设与管理工作。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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/T 28827.1-2022 信息技术服务 运行维护 第1部分：通用要求
SJ/T 11564.5-2017 信息技术服务 运行维护 第5部分：桌面及外围设备规范

3 术语和定义

GB/T 28827.1-2022界定的以及下列术语和定义适用于本文件。

3.1
桌面及外围设备 desktop termainal and peripheral
直接面向用户，具备计算、输入输出、数据通信、数据存储中一项或多项功能，用于使用或管理信息系统应用的终端设备。
[来源：SJ/T 11564.5-2017，3.1]

3.2
服务级别协议 service level agreement：SLA
运行维护服务组织与需求方之间定义服务和服务指标所形成的文件。
[来源：GB/T 28827.1-2022，2.8]

3.3
定期检查 routine check
根据既定的运行维护计划，以固定的频率对设备进行状态检查或信息记录。
[来源：SJ/T 11564.5-2017，3.8]

3.4
日常维护 daily maintenance
为了提高设备的使用效能和使用寿命，降低安全风险和成本浪费，供方对设备进行的主动服务操作。
[来源：SJ/T 11564.5-2017，3.9]

3.5
组织 organization
提供桌面及外围设备运行维护服务的实体或虚拟团队。

4 缩略语

下列缩略语适用于本文件。
AP：（网络）接入点（Access Point）
BIOS：（计算机）基本输入输出系统（Basic Input Output System）
DHCP： 动态主机设置协议（Dynamic Host Configuration Protocol）
DMZ： 隔离区CDeMilitarized Zone）
DNS： 网域名称系统（Domain Name System）
IIS应用： 联网信息服务(Internet Information Services)

IP： 互联网协议（Internet Protocol）
LPT：并行打印口（Line Print Terminal）
UPS： 不间断电源（Uninterruptible Power System）
USB： 通用串行总线（Universal Serial BUS）
WAN：广域网（Wide Area Network）

5 服务设施

5.1 信息化管理

组织应制定信息化建设发展规划，基于信息化管理体系，建立信息化管理平台，确保组织管理与项目运行管理协同，应包括以下功能：

a） 集成相关信息系统，实现组织管理与主营业务的信息化，推进组织管理信息系统中项目业务管理和财务管理的信息系统深度集成；
b） 集成知识库，实现知识的共享，充分挖掘和利用知识的价值，支撑智慧组织建设；
c） 集成监控工具，具备 IT 系统运行状况实时监视、故障预警告知以及远程支持的服务能力；
d） 集成服务台，包括服务请求的接收、记录、跟踪和反馈等流程，实现服务流程在线化；
e） 网络安全自查、巡检、风险评估及安全整改，并持续优化网络安全；
f） 容灾备份，具有灾难恢复系统、防病毒、防篡改、防泄漏系统。

5.2 备件管理

组织应具备并有效管理运行维护服务活动所需的备件资源的能力，包括但不限于：

a） 建立供应商选择和评价管理，规范备件的采购过程；
b） 建立备件出入库管理制度，规范入库备件的标识、使用、核销和账务管理；
c） 采用信息化工具对备件库管理，确保备件库信息真实有效；
d） 管理备件状态，以确保其功能满足运行维护需求。

5.3 智能运维工具

组织应根据运行维护服务的不同场景需求，规划和建设智能运维能力，结合人工智能、大数据、云计算等技术，开发或集成相应的运维工具，提高服务效率和质量。

a） 识别智能运维场景，分析运维场景的需求，目标，特征，可行性，形成设计方案；
b） 选择适宜的技术手段，构建实现能力，满足实时性，有效性，可靠性，安全性等技术需求；
c） 明确场景数据需求，对实现过程进行评审，优化和变更管控；
d） 使用数据建模工具，完成数据模型的定义、设计和开发；
e） 在数据存储，数据加密，数据压缩，队列调度等关键处理中采用相适宜的算法，满足元数据管理的需要；
f） 配置适当的资源满足智能运维工具的运行要求，包括计算，网络，存储等。
g） 建立评估机制，定期进行效果评估，制定改进措施，持续改进，快速迭代。
h） 覆盖服务的主要场景，包括并不限于软件分发，终端漏洞检测，终端日常巡检自动化，终端威胁 IP 检测，运维知识库智能应用，访问控制审核等，能力要求参考附录 D。

5.4 资产管理

组织应具备对软硬件资产进行管理的能力，包括但不限于服务器、工作站、虚拟桌面、网络设备、存储设备，以及各种操作系统、数据库、应用软件等。

a） 应识别和记录所有资产的状态和位置，以便于进行有效的管理和维护，满足资产管理的实时性和准确性需求；
b） 建立有效的通知机制，对未纳入管理的设备进行实时通知，提高设备管理的全面性；
c） 管理软件许可证，类别和合规性；
d） 统计特定软件的使用情况详细信息，例如使用次数，总使用时间，具有特定软件的系统等；
e） 在网络中检测，阻止和自动卸载禁止的软件；

f) 具有设备锁定功能，以保证设备的安全性和数据的完整性；
g) 按使用期限，磁盘使用情况，类型进行资产排序。；
h) 针对许可证数量及终端安装数量进行统计，当许可不足或过多时报警。
i) 支持将报告导出为 PDF 或 CSV 格式；
j) 资产管理统计效率达到 100 台/人天。

6 服务人员

6.1 基本要求

组织应对服务人员进行管理，包括但不限于：
a) 识别运行维护服务有关人员的分类，明确其职责、权限以及与岗位相适应的能力要求，如教育程度、专业技能、工作经验等。
b) 根据服务要求配备适合的管理和作业人员，特殊岗位按规定要求持证上岗。
c) 识别培训需求，制定并实施员工培训计划，做好员工上岗前和在岗中的培训。
d) 建立员工绩效考核管理制度，规定考核内容、标准，并将考核结果作为人力资源管理评价和质量管理改进的依据。
e) 建立和实施人才梯队培育制度，并定期评价培育规划的充分性、适宜性和有效性。

6.2 团队建设

组织应确定并配置满足服务所需的人员，包括：
a) 满足一线提供运维服务所需的人员，即在保持高绩效的同时具备良好的服务意识、职业素养以及运行维护基本知识和技能的人员；
b) 满足二线提供支持服务和服务管理所需的高潜人才，即在保持高绩效的同时具备领导意愿、取得成功的能力以及对组织有着更高敬业度的人才；
c) 在相应的行业领域和专业范围内配置满足战略发展需求的战略性人才；
d) 考虑行业未来发展趋势配置满足组织技术创新需要的研发人才。

6.3 行为监督

a) 组织应制定、实施能够体现组织文化并被全体员工认同和遵守的服务人员基本行为准则和日常行为规范；
b) 组织应依据基本行为准则和日常行为规范建立服务人员行为监督管理机制，监督、评价、分析、改进服务人员行为及其后续的工作内容与工作方式。

6.4 人员培训

组织应建立培训管理体系，包括：
a) 组织应依据理论、实训与实践相结合的培训组织体系以及相应的管理和激励；
b) 组织应有专门的部门进行培训的实施和管理，培训教育过程和结果应保留记录；
c) 组织应针对运行维护服务常见问题的描述、分析和解决方法建立相关的知识库，并利用信息化工具进行知识的收集、共享以及生命周期管理；
d) 组织应建立技能培训平台，并配置至少包括防火墙、无线网络、sd-wan 、网上行为管理设备在内的 IT 网络相关的主流厂商设备，以及虚拟化服务器平台和虚拟桌面平台部署环境；
e) 组织应至少每半年开展一次技能更新培训，培训内容至少应包括：windows 系统、exchange 邮件系统、文件系统、域环境、vsphere 虚拟化环境部署、主流虚拟桌面部署、交换机、路由器、防火墙、VPN 设备常规操作技能等；
f) 组织应设置专业技术人员和技术管理人员技术分级标准、培训及考核方案，定期评价培育规划的充分性、适宜性和有效性，相关人员应经培训并通过考核才能上岗。

7 服务要求

7.1 基本要求

7.1.1 服务要求

7.1.1.1 组织应根据客户需求提供包括但不限于电话支持，远程协助，应急服务，驻场服务，AI 服务，定期巡检等多种服务模式。

7.1.1.2 提供服务时服务人员应遵守以下共同要求：

a) 提供相应的服务前应征得客户同意，遇到需方提出额外要求时，服务人员应得到上级授权后再做处理；
b) 服务人员应确保个人联系方式畅通，表达准确，注意仪表和礼仪，在客户现场应遵守客户管理制度；
c) 运维工程师若不能按要求到场则需要在第一时间向组织说明，由组织安排其他运维工程师提供应急服务；
d) 对客户交代的每件事情要有始有终，跟进过程要及时汇报；
e) 事件完成时限应符合附录 A 的要求，处理及时率 ≥ 95%，服务可用性 ≥ 99.6%。
f) 应根据客户需求，制定数据灾备管理方案，参照附录 B。
g) 服务过程中应注重 IT 系统故障处理的规范性，尽量减低因操作不慎带来的风险，操作流程可参照附录 C。

注：服务可用性 =（ 1 - 故障时间/服务时间）×100%，故障时间和服务时间按年度平均值计算。

7.1.2 跨平台支持

组织应具备跨平台技术服务能力，支持管理多种主流操作系统，包括Windows，Mac，Linux，iOS,Android，tvOS，ChromesOS。

a) 开发统一的管理平台或接口，用以监控和管理多种操作系统上的资产，确保无论资产处于何种操作系统，均能够被有效地管理；
b) 提供自动化配置和部署工具，支持在多种操作系统上快速部署和配置软件及服务；
c) 实施跨平台的监控系统，用于实时收集多种操作系统的性能数据，并生成统一的报告，以便于运维人员分析和决策；
d) 定期进行兼容性测试，确保运维工具和应用在多种操作系统上都能够稳定工作，且具备良好的用户体验；
e) 建立灵活的访问控制策略，确保用户能够根据权限在多种操作系统上访问相应的资源和服务；
f) 制定统一的安全策略，确保在多种操作系统上都能执行相同的安全标准和措施；
g) 实现数据的跨平台同步与备份，保证数据的一致性和可恢复性；
h) 管理多种操作系统间的兼容性和依赖性问题，确保跨平台应用的连续性和稳定性；
i) 提供全面的技术支持，确保在多种操作系统上，用户都能获得及时有效的帮助；
j) 应覆盖主流操作系统 80%以上。

7.1.3 操作系统及应用补丁更新

组织应监控其所管理的所有系统和应用运行状态，及时发现并修复安全漏洞，缩短更新周期，保障IT环境的稳定和安全。

a) 建立实时监控机制，对所有管理的操作系统和应用的运行状态进行监控，以便及时发现异常或潜在的安全漏洞，并通过警报系统快速通知运维团队；
b) 对发现的安全漏洞进行评估，根据漏洞的严重性和对业务的影响程度，为补丁更新制定优先级，确保关键系统的安全性最先得到加强；
c) 采用自动化工具来管理补丁的下载、测试和部署过程，减少人为操作的错误，提高补丁管理的效率和准确性；
d) 对补丁部署后的系统和应用进行验证，确保补丁正确应用且不影响系统的正常运行；
e) 在进行补丁更新前，确保有完整的备份，以便在更新出现问题时能够快速回滚到稳定状态；
f) 更新周期应在补丁发布后的 45 天内完成。

7.1.4 终端软件自动部署

组织应采取自动化和批量化的方式对终端软件进行部署，包括新软件部署，软件更新与补丁应用，配置变更，软件许可证管理，应急响应，硬件更换或升级，遵从性和审计，远程办公支持等场景，提高准确性和部署效率，提升运维效率。

a) 明确组织的需求，包括需要部署的软件类型、目标终端的数量和类型、预期的部署时间等；
b) 根据需求分析的结果，选择合适的自动化部署工具。工具的选择应考虑其是否支持跨平台部署、是否具有丰富的功能、是否易于使用和管理等因素；
c) 对工具进行合理配置。包括设置部署策略、定义部署流程、配置软件仓库等；
d) 在少量终端上进行测试部署，验证配置的正确性和部署的效果，测试部署的结果将为实际部署提供参考；
e) 测试部署成功后，在所有目标终端上进行实施部署。在部署过程中，需要密切监控部署的进度和结果，及时发现并解决问题；
f) 部署完成后，需要进行后续的管理，包括监控软件的运行状态、更新软件和补丁、管理软件许可证等，根据实际运行情况，调整部署策略和流程，以提高部署的效果；
g) 自动化和批量化应覆盖 90%以上的部署场景。

7.1.5 终端自动运维操作

组织应采取自动化和批量化的方式执行常规运维操作，包括系统监控，日志管理，用户账户管理，安全管理，备份与恢复，网络配置，资产管理，故障响应等场景，降低出错率，提升运维效率。

a) 对运维流程进行彻底的审查和评估，确定可自动化的操作。制定全面的自动化策略，包括目标、时间表、预算和资源分配；
b) 根据自动化需求选择合适的工具和平台，包括监控工具、日志分析器、配置管理系统、安全扫描工具、备份软件等，确保工具可集成并协同工作，提供统一的自动化解决方案；
c) 准备必要的基础设施，包括服务器、存储和网络资源，以支持自动化工具的部署和运行，确保有足够的容量来处理监控数据、日志文件、备份集等；
d) 开发自动化脚本和流程，以执行常规任务，如监控性能指标、收集和分析日志、管理用户账户、安装和更新软件、维护系统配置、执行安全扫描、管理网络设置、跟踪资产和故障响应；
e) 在控制环境中对自动化脚本和流程进行测试，应确保按预期工作，不会干扰现有的业务流程，验证自动化操作是否符合安全标准和合规要求；
f) 测试完成后，逐步部署自动化解决方案到生产环境。监控部署过程，确保自动化操作不会导致服务中断或其他问题；
g) 应持续监督性能和效率，收集反馈，根据实际运行情况不断改进自动化流程，确保覆盖率达到目标，对于无法自动化的特殊情况，应制定手动处理策略；
h) 应为运维团队编制完整的操作文档，说明自动化系统的工作原理和操作方法。对团队成员进行培训，确保能够有效地使用自动化工具和处理异常情况；
i) 定期进行安全审计和合规性检查，以确保自动化操作不会引入新的安全风险，并且符合行业标准和法规要求；
j) 应进行持续的监控和维护，以应对基础设施变化、新的安全威胁、软件更新和其他可能影响自动化效率的因素；
k) 自动化和批量化应覆盖 90%以上的运维操作场景。

7.2 电话支持

7.2.1 电话支持是指通过电话指导客户快速解决问题，适用于简单易操作，可在 10 min 内排除的故障类故障，采用电话支持前应与客户进行沟通，判断客户针对相关问题的操作能力是否适合采用电话支持。

7.2.2 电话支持服务应至少符合以下要求：

a) 操作过程描述清晰，并和客户确认每一步操作显示的窗口和现象；
b) 如果某些步骤等待时间比较长，提前向客户说明；
c) 如果尝试过一两种方法，故障仍不能解决，向顾客建议改由运维工程师上门服务。

7.3 远程协助

7.3.1 远程协助是指通过远程控制软件登陆客户桌面协助客户解决问题，仅适用于网络正常情况下的

桌面类的故障。

7.3.2 远程协助服务应至少符合以下要求：

a) 远程报修需要记录客户名称、联系人、联系方式、报修问题；
b) 远程连接后，先让客户操作确认故障现象，并提醒客户自行保存文档，再按照常流程处理；
c) 结束服务时由客户先断开远程后，服务人员才能断远程；
d) 如果尝试过两种或以上方法，故障仍不能解决，向顾客建议改由运维工程师上门服务。

7.4 应急服务

7.4.1 应急服务是指接到客户报修后，派遣运维工程师进行上门服务，适用于比较复杂，需要全面地排查，预估处理比较长的故障。应急服务的范围包含所有在 SLA 范围内的故障内容。

7.4.2 应急服务应至少符合以下要求：

a) 组织应根据服务规模配置相应的运维工程师，密度比应至少达到 1:18（运维工程师 ： 客户数量）；
b) 应及时响应客户需求，并初步确认故障原因及处理方式，响应时间 ≤ 5 min；
c) 应急事件需要记录客户信息、联系人信息、处理事务、预约到场时间、服务地址；
d) 运维工程师出发前应检查确认所携带的工具、服务单、系统盘，人员到场时间 ≤ 2 h；
e) 运维工程师现场进行的所操作都应在工单上进行记录，内容至少包括工作内容，服务标签、耗时、处理过程、是否解决；
f) 对复杂或存在风险的工作做好预案，经审核后实施，如现场碰到 30min 内无法处理问题直接进行问题升级；
g) 工单完成后客户签字确认，该项目服务经理审核工单关闭服务事件。

7.5 驻场服务

7.5.1 驻场服务是指派出运维工程师驻扎在客户现场进行服务，适用于对可用性和连续性要求比较高的项目，可及时响应客户需求，服务的范围应包含所有在 SLA 范围内的故障内容。

7.5.2 驻场服务应至少符合以下要求：

a) 应自备工具、服务单、系统盘；
b) 应按客户方上班时间准时上下班并按组织要求做考勤记录；
c) 按标准的工作清单提供服务并填写工单，内容包括工作内容，服务标签、耗时、处理过程、是否解决；
d) 工单完成后客户签字确认，该项目服务经理审核工单关闭服务事件
e) 服务中如果碰到无法解决的技术问题，应提交问题升级；
f) 应主动询问客户负责人是否有其他工作安排，主动帮助客户员工。

注：驻场人员如需请假或调休，应按组织人事管理制度执行，并提前至少一天告知客户，同时组织应为客户提供临时代班的驻场人员。

7.6 AI 服务

7.6.1 AI 服务是指在服务过程中利用人工智能技术，为客户提供交互式服务的智能服务系统，替代人工进行客户服务，实现信息的智能化处理。

7.6.2 AI 服务应至少符合以下要求：

a) 宜实现对声音的实时采集和识别，自动将语音处理成自然文本；
b) 宜集成人工智能技术驱动的自然语言处理工具，具有语言理解和文本生成能力；
c) 宜集成组织知识库，并训练运维工程师模型，根据客户输入的关键词，进行检索查询，可回复或处理技术问题；
d) 宜利用大数据建模和算法实现，处理客户日常运维数据，用于加速服务报告生成和服务需求预测。

7.7 定期巡检

7.7.1 定期巡检是指对电脑（硬件或者虚拟桌面）、服务器、网络设备、打印机等设备在运行一定时限后进行定期检查，提前建议客户进行备件更换或者设备扩容，有助于预防问题的发生，服务的范围应

包含所有在 SLA 范围内的巡检内容。

7.7.2 定期巡检应至少符合以下要求：

a) 按照 SLA 约定制定巡检计划，内容包括巡检项目，巡检周期，巡检要求；
b) 执行巡检任务前应提前征得客户同意，运维工程师按时抵达现场根据巡检工单进行巡检；
c) 巡检完成后客户签字确认，一周内提交巡检报告；
d) 针对巡检中发现的问题，按照 SLA 约定的方案进行处理。

8 信息安全

应符合GB/T 28827.1-2022 中7.12 的要求，无因组织管理不当导致的泄密事故发生。

9 持续改进

应符合GB/T 28827.1-2022 中5.3.4的要求。

10 评价要求

10.1 评价准则

10.1.1 第 5，6，7，8，9 章给出了桌面及外围设备运维的服务要求，其评价应依据附录 E 表 E.1 给出的评价工具实施。

10.1.2 评价人员基于表 E.1 实施桌面及外围设备运维的服务要求评价：

a) 表 E.1 是根据第 5，6，7，8，9 章的要求，赋权量化构建的服务要求评价表，设定满分值为 100 分;
b) 给出基于李克特 5 点式量表的评价内容体验系数 α ,如下：
c) 远低于预期：0≤ α ≤0.2;
d) 低于预期：0.2＜ α ≤0.4;
e) 符合预期：0.4＜ α ≤0.6;
f) 高于预期：0.6＜ α ≤0.8;
g) 远高于预期：0.8＜ α ≤1.0。
h) 用表 E.1 中给定的每一项评价内容的分值乘以该项的体验系数 α 后求和，得出服务要求评价得分。

10.2 评价结果

桌面及外围设备运维服务评价结果分为通过、不通过。其中：

a) 通过是指服务要求评价达到 80 分（含）以上；
b) 当桌面及外围设备运维服务评价发生下列任一情况时，评价结果为不通过：
c) 服务要求评价低于 80 分；
d) 评价期间组织因重大违法违规行为而受到行政处罚；
e) 评价期间组织提供的服务发生重大安全或舆情事故，社会影响恶劣。

附 录 A
（规范性）
运维服务级别及完成时限

A.1 驻场运维服务级别及完成时限

驻场运维服务分类，服务项，服务可用时段，服务响应时限，服务完成时限，以及服务优先级要求应符合表A.1。

表A.1 驻场运维服务级别及完成时限

服务大类	服务小类	服务项	服务可用时段	服务响应时限	服务完成时限	服务优先级
桌面终端维护	PC硬件	PC端内存、硬盘等配置升级	工作日	1 d	3 d	4
		PC电脑硬件安装或更换（不含采购时间）		20 min	1 h	4
	虚拟桌面终端硬件	终端硬件固件更新		1 h	2 h	4
		终端硬件部署和安装（不含采购时间）		20 min	40 min	4
	办公软件	新电脑操作系统或非标软件安装、操作系统修复或优化		20 min	1 h	4
		办公标准软件安装		10 min	30 min	3
		办公软件应用维护、软件使用咨询		20 min	2 h	3
	数据备份	移动存储数据备份		1 h	4 h	4
		备份软件备份数据		30 min	2 d	4
	电话服务	电话安装、功能变更		20 min	1 h	3
		话机移动		20 min	1 h	4
	电子邮件服务	员工邮箱或公共邮箱或邮箱组建改删		20 min	1 h	3
		邮件客户端设置（设置OUTLOOK邮箱配置）		30 min	1 h	3
		邮件客户端排错		30 min	2 h	3
		邮箱数据恢复，容量扩容		20 min	2 h	4
	互联网服务	访问权限设置、使用权限开通、无法访问排错		30 min	1 h	4
	打印/传真服务	打印机安装、共享打印机设置		20 min	30 min	3
		传真、电子传真号码申请，传真移机		20 min	2 h	4
	文件共享	共享目录设置、共享目录历史文件恢复		20 min	2 h	4
		共享目录权限更改、共享目录扩容		20 min	1 h	3
		部门文件发布		30 min	2 h	4
	特殊办公支持	电话会议申请、无限卡申请及交付		20 min	1 h	4
		专用网连接、移动网卡安装		1 h	4 h	4
		会议室网络环境支持		10 min	30 min	3
	域账号	员工域账号建改删（密码重置）		20 min	1 h	3
		VPN权限建改删		20 min	4 h	3
	员工桌面配置（PC硬件）	包括：安装桌面电脑、安装标准办公软件、分配并配置个人邮箱、安装或连接相应的打印机。		30 min	3 h	5
	员工桌面配置（虚拟桌面终端硬件）	包括：安装桌面电脑、安装标准办公软件、分配并配置个人邮箱、安装或连接相应的打印机。		30 min	2 h	5

表 A.1 驻场运维服务级别及完成时限（续）

服务大类	服务小类	服务项	服务可用时段	服务响应时限	服务完成时限	服务优先级
	员工异动权限改删	包括：域账号、邮箱、应用系统、上网权限的改动或清除		20 min	1 h	3
	工位变动支持服务	办公桌面移动，包括：重要数据备份、设备拆除、搬移、安装、打印机服务配置变更、电话服务变更等。		1 h	1 d	5
	特殊环境服务	用户培训环境、特殊安全环境构建与拆除		1 h	2 d	5
	电脑巡检服务	PC电脑及虚拟桌面运行状态的巡检工作		20 min	1 d	5
业务支持	应用支持	业务系统全局性服务完全中断故障	所有日期	即时	1 h	1
		业务系统片区域部分线上或线下订单处理关键业务服务中断故障		即时	2 h	2
		业务系统单点部分线上或线下订单处理等关键业务服务中断故障		20 min	4 h	3
		业务系统部分线上或线下订单处理等非关键业务服务中断故障	工作日	20 min	8 h	4
		业务系统使用咨询		5 min	30 min	4
		业务数据提取、差错数据修改		1 h	2 d	4
	IT资源	应用系统账户建改删、呼叫中心话务配置、配置发放回收、密码重置		1 h	8 h	4
		配置账单提供		2 h	2 d	5
	通报	重大故障通报、内外部维护通报、最新业务通报	所有日期	即时	20 min	1
信息安全管理	安全支持	特殊环境数据导入/导出	工作日	1 h	8 h	2
		访问控制权限管理	所有日期	1 h	5 d	4
	安全服务	技术环境安全评估、应急预案及应急演练	-	-	1 次 /2 月	3
		病毒防护系统维护	所有日期	-	1次/天	3
		安全设备性能巡检		-	3次/天	4
		电脑病毒查杀	工作日	3 0min	2 h	4
基础环境维护	机房物理环境维护	空调制冷设备、消费系统、环境监控系统、安防系统、防雷接地、温湿度、UPS设备、柴油发电机设备、线缆的标识和标签巡检	所有日期	-	3次/天	4
	IT基础环境日常维护	网络设备性能、网络线路带宽流量、服务器设备性能、操作系统运行环境、虚拟化环境监控		-	实时	3
		客户端月度例行巡检		-	10台电脑/h	4
技术支持	办公室自动化支持	AD域、企业邮箱、ITSM应用、电话系统维护		20 min	4 h	3
		财务、人力、审计专用系统技术支持	工作日	20 min	4 h	3
	业务类技术支持	研发相关系统环境需求分析		1 h	3 d	3
		研发相关系统环境搭建		1 h	-	3
		硬件设备选型与测试、容量规划管理	-	-	-	3
	其他	用户培训	工作日	5 d	7 d	4
		IT行政事务		2 h	3 d	4

表 A.1 驻场运维服务级别及完成时限（续）

服务大类	服务小类	服务项	服务可用时段	服务响应时限	服务完成时限	服务优先级
事件处理	安全事件支持	安全事件处理	所有日期	即时	8 h	1
	办公环境故障支持	旧电脑操作系统重装、业务办公软件故障处理	工作日	20 min	2 h	3
		PC电脑硬件故障送修		20 min	-	4
		互联网线路、电话线路、传真机、公告打印机故障处理		20 min	4 h	3
	基础环境故障支持	基础环境故障处理		即时	2 h	1
运维报表	服务报告	服务台关键KPI、客户服务月报		-	次月第一个工作日	2
	基础环境报告	基础环境运行分析月报		-		2
	运维报告（客户自行选择，可单选或多选）	运维月报		-		2
		运维周报		-	次周首日	2
		运维日报		-	次日上午10点	2

注1：服务优先级共分1级-5级，优先服务等级依次递减。
注2：所列运维服务级别内容不包括以下自然灾害、外因或规划性事情。
——地震、台风、洪水等自然灾害；
——战争、罢工、停电、政府行为等；
——政府电力部门或电信部门的行为；
——电信线路被人为破坏或骨干网线路、设备因调试、扩容所引起的中断；
——互联网公网阻塞或其他通路（如访问目的地的服务器响应速度）问题；
——外部人为破坏因素引起的， 超过设备的承载能力；
——第三方服务提供商因素引起的；
——业务操作人员在没有技术人员的指导下或私自操作造成服务中断的；
——因业务发展的需要在正常上班时期进行服务维护的；
——因规划需要，计划内的维护。

A.2 远程运维服务级别及完成时限

远程运维服务分类，服务项，服务可用时段，服务响应时限，服务完成时限，以及服务优先级要求应符合表A.12。

表A.2 远程运维服务级别及完成时限

服务大类	服务小类	服务项	服务可用时间段	服务响应时限	服务完成时限	服务优先级
桌面类远程	办公软件	办公标准软件安装	工作时间	10 min	30 min	3
		非标准软件安装	工作时间	10 min	1 h	4
		办公软件应用维护	工作时间	10 min	30 min	3
		办公软件使用咨询	工作时间	10 min	30 min	3
	电子邮件服务	员工邮箱新建修改删除	工作时间	10 min	20 min	3
		公共邮箱新建修改删除	工作时间	10 min	20 min	3
		邮箱组新建修改删除	工作时间	10 min	20 min	3
		邮箱归档，收发软件设置&排错	工作时间	10 min	30 min	3

表 A.2 远程运维服务级别及完成时限（续）

服务大类	服务小类	服务项	服务可用时间段	服务响应时限	服务完成时限	服务优先级
	互联网服务	互联网访问权限设置	工作时间	10 min	30 min	4
		网络使用权限开通	工作时间	10 min	30 min	4
	打印机服务	打印机安装	工作时间	10 min	15 min	3
		共享打印机设置	工作时间	10 min	30 min	3
		打印机排错	工作时间	10 min	30 min	3
	共享盘问题处理	共享目录设置（局域网共享）	工作时间	10 min	1 h	4
		共享目录权限修改	工作时间	10 min	1 h	3
		共享目录历史文件恢复	工作时间	10 min	2 h	4
	域环境	员工域账号新建修改删除（密码重置）	工作时间	10 min	15 min	3
		客户端加域退域	工作时间	10 min	30 min	3
注：服务优先级共分1级-5级，优先服务等级依次递减。						

附 录 B
（资料性）
数据灾备管理

B.1 数据丢失和应用中断因素

组织应根据客户需求，制定数据备份与恢复的机制、策略、规范、流程和应急保障措施，满足客户不同级别数据的存储安全保护要求。数据备份和恢复应保障数据存储过程的保密性、完整性、可用性和可追溯性。数据丢失和应用中断因素见表B.1。

表B.1 数据丢失和应用中断因素

序号	类别	内容
1	自然因素	地震、火灾、雷电、 洪水、 腮风、 工业事故等。
2	人为因素	盗窃、蓄意破坏、 病毒、缺乏经验造成的误操作、 压力和恐慌造成的误操作等。
3	硬件故障	硬盘损伤、 服务器岩机、 电源故障、 存储器故障等。
4	软件故障	数据库设计缺陷、 应用软件故障、 操作系统故障等。
5	网络故障	络连接问题、 网卡和驱动程序故障等。

B.2 数据安全风险

B.2.1 单服务器运行风险

若不对单机架构的应用服务器数据采取有效的数据安全保护措施，应用系统面对人为误操作、病毒、网络攻击、软硬件故障、自然灾害等意外事件时缺少必要的安全保护，极易造成数据丢失，甚至将严重影响到业务的正常开展，带来巨大的经济损失以及负面影响。另外，操作系统也需要进行保护，否则重大故障发生时，需要先重新安装操作系统、重装所有应用程序，然后才能恢复数据，耗费相当长的时间才能够重新恢复应用。

B.2.2 手工备份弊端

采用手工方式进行备份将无法避免会出现漏备、 误备等情况， 备份的数据也难以管理。

B.2.3 本地数据中心损毁风险

本地信息化安全措施无法防范水灾、地震等重大灾难对本地机房的整体性摧毁，因此需要建设更高安全保护等级的灾备系统，如异地数据灾备系统。异地数据灾备要求在异地保存与本地一致的备份数据，灾难发生后， 当无法从本地恢复时，可以从异地恢复系统和数据，确保用户原有的数据不会丢失或遭到破坏。

B.3 数据备份方案

数据备份方案见表B.2。

表B.2 数据备份方案

方式	描述	优点	缺点
普通双机热备	两台服务器通过磁盘阵列实现双机热备，在一台服务器出现问题的时候，可以马上切换到另外一台服务器继续运行。但如果磁盘阵列出现问题，整个系统将不能正常运行。	在主机出现故障，比如电源、内存、硬盘等硬件设备出现故障，另外一台服务器可以马上代替工作。	磁盘阵列是整个系统的瓶颈，磁盘阵列出现故障后，需要专业人员进行数据恢复，并且存在数据丢失与完全无法恢复的可能。

表 B.2 数据备份方案（续）

方式	描述	优点	缺点
全冗余双机热备	由两台服务器、两套磁盘阵列再加上专用磁盘阵列同步软件以及相关连接设备构成。	服务器或磁盘阵列任何单个设备出现问题，备份设备可以及时代替工作。	系统复杂程度高，除了双套设备之外，还有许多连接设备及软件，导致系统维护成本高。由于存在着数据同步的过程，因此整体运行性能较低且造假高。
NBS备份	在局域网内设置一个专用存储服务器，通过FTP等通知协议继续定期数据备份。	备份机制独立，系统维护起来简单。 支持异地备份， 可 以避免机房发生火灾等严重损害时，可以保证数据不丢失，数据恢复容易，成本低。	不能实现实时备份，一般备份周期为一h或者一天。

B.4 数据备份策略

B.4.1 数据库备份策略

数据库备份策略见表B.3。

表B.3 数据库备份策略

实时策略	关键应用的数据库采用实时备份： 设置数据库为在线 CDP 持续监控备份， 保留 3 个月的连续性各份数据，保证数据趋于 0 丢失。
定时策略	非关键应用数据库：建议每周至少做 1次欠完全备份，周末进行；每天做 1 次增量备份，每 4 h做 1 次归档日志备份（勾选 “删除已备份的本地归档日志 ” ）。保留三个月的完全备份版本数目。
	数据库访问非常频繁：若只能容忍半h或 10 min的数据丢失，则应加大各种各份的频率。应每周备份 2次～3 次全备份，每天至少备份 2次增量备份、每半h进行 1 次归档日志备份。
	用户数据库非常大：则备份需要消耗更长时间，应按照最佳备份策略进行备份。
	用户数据库数据非常重要，需要经常恢复到某个时间点，则应加大归档日志备份频率， 应每0.5 h进行一次归档日志备份。保留更多完全备份版本。

B.4.2 文件备份策略

文件备份策略见表B.4。

表B.4 文件备份策略

实时策略	重要文件资料设置为对全盘所有文件进行实时监控，默认排除类型：tmp、 temp、exe、rmvb、rar、 MP3。同一个文件的实时备份间隔为连续，每个文件保留500个版本。对超过200M前文件，实时各份间隔为1h，每个文件保留10个版本。
定时策略	非关键性资料采用定时备份：初始为完全备份，每天做1次差异备份；保留 1个月的备份版本数目（即备份保留版本数为30个）。
LAN-Free备份策略	大数据LAN-Free备份：针对服务器数据量大的文件数据，采用LAN-Free方式备份，晚间进行。

B.4.3 操作系统备份策略

操作系统备份策略见表B.5。

表B.5 操作系统备份策略

在线热备策略（定时）	操作系统（含应用程序）设置在线热备份：操作系统盘采取镜像文件备份，每月初做备份，晚间进行：保留3个月的备份版本数目（即备份保留版本数为3 个）。

B.5 灾难恢复

系统出现故障，导致不能运行的时候，应有排除故障的预案，以便于及时解决故障并迅速使系统正常运行，表B.6对可能出现的故障进行列举，并列出故障排除方案。

表B.6 常见故障排除方案

故障类型	故障点	故障排除方案
硬件故障	电源、内存等非存储相关设备故障	确定故障点，更换故障配件，如故障配件没有备份配件，联系相关配件生产厂家进行采购；如配件发货周期较长，可考虑把同类型服务器的配件暂用替换下，先拷贝数据出来，然后在其他备用服务器上安装程序，以及恢复数据，使系统尽快地先恢复起来。
	硬盘或者磁盘阵列 故障	如出现一块坏硬盘,可通过替换相同类型的硬件,服务器自带Raid5功能，将自动修复。如多块硬盘出现故障，数据无法读取的时候，首先查找备份文件，如备份文件较新，如是一天内的备份数据，此时应评估丢失的数据是否重要或者可以通过其他方式恢复。如不重要或者可以通过重新录入恢复，则用备份服务器上的数据进行数据恢复；否则应请专业磁盘数据恢复公司进行数据恢复。
软件故障	操作系统故障	首先确保数据没有丢失的情况，备份数据，然后重新安装系统以及数据库，并重新安装相关应用程序，最后进行数据恢复。
	应用程序故障	联系应用程序开发厂家，要求进行售后支持，或者根据厂家提供的安装程序，进行重新安装部署。

附 录 C
（资料性）
操作流程

C.1 计算机重新安装系统操作流程

计算机重新安装系统操作步骤及注意事项与说明应符合表C.1的要求。

表C.1 计算机重新安装系统操作流程

操作步骤	注意事项与说明
确认重装系统	a）根据计算机重新安装系统条件判定为重新安装系统； b）系统盘由客户提供。如客户不能提供，则运维服务人员安装官方版系统，版权由客户负责，并向客户确认。
数据备份	a）虚拟桌面系统资料，进行整机备份。 b）备份系统盘资料。 如需运维服务人员操作， 应该提前声明运维服务人员不对资料的损坏、丢失负责； c）备份储存介质由客户提供。 如客户不能提供， 则使用运维服务人员备份储存介质前须经过客户同意，并在资料还原后经客户检查恢复完成后， 将客户备份在运维服务人员储存介质上的全部资料完全删除； d）记录 IP、 DNS、打印机等网络配置； e）和客户确认其他需要保存的资料，并妥善保存，并由客户签字确认资料已经保存。
检测安装	a）检测硬盘是否有坏道、 内存条是否报错和其他硬件是否有报错或异常， 如有坏道或报错 等异常应主动及时向客户提出，并提出合理的建议； b）检测硬件配置， 根据计算机系统安装标准确定电脑可以安装的系统版本。 如客户需要安装更高版本的系统， 则须给客户说明情况， 表明此硬件安装高版本系统可能会导致运行异常或不畅； c)所安装系统如果是运维服务人员自备的，系统文件应是官方的、安全的且经过验证的，系统版权由客户负责。
软件安装	a）安装软件时， 如果软件是运维服务人员自备的， 则软件应是官方的、 安全的且经过验证的， 也可参照平台计算机软件安装标准进行； b）安装软件时，安装顺序为： 杀毒软件→驱动→压缩软件→OFFICE→专业软件→邮箱及配 置导入邮件→导入其他备份资料→测试； c）让客户确认是否还需安装其他软件。
验收确认	a）首先自己检查设备是否恢复正常； b）经检查无误后交给客户检验， 由客户检验完成后签字确认。
注：符合以下情形之一，计算机应重新安装系统： a）客户请求服务； b）系统宕机，且无法恢复状态时； c）为确保系统满足用户使用需求。必要时，经客户确认批准。	

C.2 软件安装操作流程

软件安装操作步骤及注意事项与说明应符合表C.2的要求。

表C.2 软件安装操作流程

操作步骤	注意事项与说明
软件获取	a）安装和卸载软件需经过客户同意； b）软件由客户提供或者为官方下载版本； c）软件版权由客户负责。
安装准备	a）备份软件的资料、记录软件的配置； b）若客户提供安装流程则按照客户流程安装，若客户未提供安装流程，则了解官网注意事项。
安装	a）安装时需要注意客户对安装盘符是否有要求； b）若无，则按照默认安装位置安装，安装过程注意去除推送广告、捆绑软件等。
设置	a）设置软件配置时，如果客户有配置，则按照客户提供配置进行设置； b）若客户没有配置，则根据客户需求设置，达成客户所需效果； c）注意去除广告弹窗、推广弹窗，并根据客户需求是否开启开机自启。
测试	a）安装、设置完成后，应进行测试，测试软件是否可以正常运行； b）检测是否可以满足客户需求，若不能满足，则进行检查，修改配置以达到客户需求。
验收确认	测试完成后，由客户检验完成后签字确认。
注：应确定应用软件安装权限，在未得到客户批准前，不提供服务。	

C.3 计算机拆机操作流程

计算机拆机操作步骤及注意事项与说明应符合表C.3的要求。

表C.3 计算机拆机操作流程

操作步骤	注意事项与说明
确认拆机	a）根据计算机拆机条件判定计算机是否需要拆机； b）拆机前应经过客户确认。
准备及检查	a）拆机前检查计算机外观、接口、外设是否完好，无损伤，电脑是否可以开机； b）拆笔记本计算机前，应先了解拆机教程或拆机手册； c）洗手、佩戴防静电手环、防静电毯等。
拆机	a）首先拔掉电源，再按电源键几次进行放电； b）拆掉机箱螺丝并妥善保管； c）打开机箱后先拍照记录机箱内布局； d）清理机箱里面的灰尘，清洁时不可在办公区操作； e）拆机顺序为：外设→线缆→配件（电源、驱、硬盘等）→显卡、内存→主板→风扇、CPU； f）插拔相关配件时注意防呆口，不可强插强拔； g）拆下来的配件应妥善放置、注意防静电、注意防水。
安装	a）安装前对所有配件须进行清洁，保证机箱内整洁干净； b）安装时注意防呆口，避免损坏设备； c）安装顺序为 CPU、风扇、内存→主板→显卡→电源、硬盘、光驱→插线→安装外设→通电源→ 开机测试→正常→安装机箱盖螺丝； d）安装完成后注意核对拆机时的拍照记录，检查所有配件、线缆是否安装正确，避免安装问题导致设备不能正常运行。
检查与测试	检查外设、螺丝等全部安装完成无遗漏，开机运行情况是否正常，检查设备运行温度是否正常，并重启 3-5 次确保设备无异常。
验收确认	将线缆梳理整齐，外设摆放整齐，由客户检验完成后签字确认。

表 C.3 计算机拆机操作流程(续)

注1：符合以下情形之一，计算机可进行拆机操作： a）客户请求服务； b）为确保计算机硬件的新增、故障处理、问题检测服务符合要求。 注2：符合以下情形之一，可提供计算机配件更换服务： a）客户请求服务； b）经过检测和替换确认配件损坏且无法修复，并经客户同意； c）因配件原因导致设备运行效率严重下降，严重影响客户工作，并经客户同意。

C.4 打印机安装操作流程

打印机安装操作步骤及注意事项应符合表C.4的要求。

表C.4 打印机安装操作流程

操作步骤	注意事项与说明
准备	a）了解打印机品牌、型号，获取官方打印机驱动； b）了解现场连接环境，确认是直连共享还是网络打印机； c）如果是网络打印机，需了解网络环境，确认网段，分配固定IP地址； d）如果是直连打印机，需确保所有用户在同一工作组中。
安装	a）根据连接方式，将打印机连接到设备上。直连打印机连接到计算机上，USB接口插在USB上，LPT接口接在串行接口上：网络打印机连接到交换机上，并在打印机上配备分配到的固定IP地址； b）若安装共享打印机，则应在共享主机上设置打印机的共享权限，并在高级共享设置里开启网络发现、文件夹打印机共享等功能； c）在计算机上可以通过IP地址、计算机名连接到打印机上，并安装官方驱动、扫描驱动、扫描软件等。
测试	a）电脑重启后进行测试，保证重启后可以正常运行； b）打印测试页确保打印机正常连接； c）让客户打印办公文件测试； d）使用扫描功能进行测试。
验收确认	a）让客户再次检查是确认正常； b）检查完成后， 由客户确认完成后签字确认。
注1：符合以下情形之一，可提供打印机运维服务： a）客户请求服务； b）经过检测确认打印机耗材无法继续使用，得到客户同意可替换耗。 注2：运维服务人员不应擅自拆机，如需拆机需经过客户同意方可拆机，对于硬件故障部分应联系打印机服务商予以支持。	

C.5 程控交换机配置操作流程

程控交换机配置操作步骤及注意事项应符合表C.5的要求。

表C.5 程控交换机配置操作流程

操作步骤	注意事项与说明
准备	a）了解设备是数字程控或IT程控； b）根据现场环境和客户需求设计分机号分布、策略设置、IP电话地址； c）了解话机点位，确保程控交换机有足够端口使用。
连接	a）连接内线、外线，安装部门或工位将内线插入相应的内线板卡端口，以便配置是方便配置分机号码； b）插接外线时先检查外线是否畅通，确保外线正常；

表 C.5 程控交换机配置操作流程(续)

操作步骤	注意事项与说明
	c）IP 程控确保程控接入内网交换机，且模块端所有话机接入网络模块。
配置	a）根据设计方案配置分机号， 设置相关策； b）IP 电话还需在电话端设置设计好的 IP 地址、 以及分机号； c）配置完成后做好配置备份。
检查	a）检查所有话机拨打外线、 内线是否正常； b）检查配置的策略是否正常； c）让客户检查所有需求是否满足。
验收确认	a）检查所有功能正常后， 清洁现场； b）检查完成后， 由客户确认完成后签字确认。

C.6 网络设备故障诊断和处理

网络设备故障诊断和处理应符合表C.6的要求。

表C.6 网络设备故障诊断和处理

设备	故障诊断和处理
路由器	a）若电脑接到路由器后获取不到IP地址，可先登录到路由器查看路由器的DHCP功能是否开启。如果没有开启，则开启DHCP功能即可。如果路由器是命令行配置的路由器，且已配置了DHCP但是客户端仍然获取不到IP地址，则可将原来的DHCP配置删除掉，然后再重新进行配置； b）若客户端可以正常获取到IP地址但是上不了网，可先测试外线。如果外线正常的话，可能是路由器的WAN口配置不正确，应根据相对应的外网参数配置路由器的WAN口。
交换机	a）若交换机转发性能不足（例如若一台24口交换机全部接的是摄像头，则会导致监控画面卡顿）， 则主要原因是背板带宽不够导致交换机无法同时处理这么大的流量； b）若一台电脑网络连接时断时续，但模块和网线测试都正常，应判断为交换机的接口问题，可通过更换端口解决此问题。
无线路由器	a）对于不同的客户端，有的客户端能连接上，有的则连接不上的问题，此时应将无线路由器的加密方式设置为wpa2-psk。 b）100M 的带宽若经过一台路由器后网络带宽降到了50M，其性能不足以支撑百兆带宽，此时应更换高性能路由器即可解决带宽下降问题。
AP	a）当连接的无线客户端数超过了AP所能承载的最大限度时，限定AP的最大可连接的无线客户端数； b）当存在信道干扰，工作环境内AP数量多而且所有AP的信道并没有统一规划时，对AP的信道统一进行规划，以可避免干扰，并提升AP性能。
程控交换机	a）分机没拨号音:先确认是单独一个分机没有拨号音，还是所有分机都没有拨号音。若所有分机都没有拨号音，检查电话交换机电源是否正常，或重启交换机测试。若是单独一个分机没有拨号音，需先排除话机问题，可以交换话机测试。若不是话机问题，再检查线路(配线架、跳线、面板模块等)； b）外线打不出去:若是模拟外线，可直接使用模拟话机接到外线线路上进行测试，若依旧无法呼出则是运营商线路问题。若可以，则检查交换机外线端口是否有松动，交换外线的端口测试； c）外线呼入总机不振铃:若有语音话务员，检查话务员配置，并检查总机的话机是否正常； d）无法打省际或国际电话:检查运营商外线是否开通了省际或国际通话功能，再检查电话交换机的配置是否给分机赋予了省际或国际通话权限。如有经济路由，需检查经济路由业务及设备是否正常。

表 C.6 网络设备故障诊断和处理(续)

设备	故障诊断和处理
防火墙	a）若无法连通防火墙接口和外网，例如：以华为防火墙为例，华为防火墙默认是禁止所有流量，如需要连通相连接的内外网接口，则须在接口底下开启连通服务： b）若将服务器的端口映射出去，依旧无法从外网访问，则放行非授信区到 DMZ 端口的流量。
注1：网络故障处理要求包括： a）计划性断网，应得到客户的确认批准； b）设备配置完成后须及时保存配置，并及时备份新的配置； c）设备调试好后应得到客户确认已符合使用要求； d）在需要短暂中断全网（如重启路由或交换设备）前，应告知客户可能带来的影响，并征得客户同意，方可进行重启设备等工作。 注2：网络设备巡检要求包括： a）电源、UPS：检查机房供电状况，UPS工作情况、指示状态； b）服务器：检查服务器是否当机，服务器（磁盘阵列）硬盘灯指示是否正常； c）机房环境：检查机房空调工作状态，机房温度、湿度是否正常； d）网络设备： 1）检查网络设备，包括交换机、路由器、防火墙等及其附属设备； 2）检查设备工作状态，CPU使用率，内存使用率和冗余状态； e）网络通道：检查内外网络通道状态，上行效率应≥80%，下行效率应≥80%。	

C.7 服务器系统常见故障处理流程

服务器系统常见故障处理步骤及注意事项应符合表C.7的要求。

表C.7 服务器系统常见故障处理流程

操作步骤	注意事项与说明
观察判断	初步判断是硬件还是软件故障，不应随意切断服务器的电源，或在未判明故障类型时就操作服务器，服务器的关机应进行正常的本地或远程关机，不允许直接切断服务器电源，如果无法进行本地或远程关机，需要手动长按开关键5s以上，但操作前应该明确告知客户这样关机的风险，得到可记录的同意回复后方可操作。
数据备份	a）向客户提出完全、 增量 或差异备份方案后， 按客户要求进行Backup操作； b）按照服务器操作系统数据和系统备份操作指南进行数据备份操作。
故障排查与处理	a）硬件故障：查看故障指示灯，依照故障诊断指示灯的指导手册来判断问题所在，并将确定的故障情况与解决方案告知客户，得到客户同意后方可进行下一步操作。如需更换硬件，应另行预约更换时间； b）启动故障：根据报错信息对故障进行判断，如果无法判断，则记录错误提升，以便支持人员诊断、解决问题，并进行技术升级； c）软件故障：应记录软件或系统的报错提示，按照提示进行故障诊断。如果不能判断问题原因， 应进行二线支持升级。不应在未经客户同意的情况下，随意删除或卸载软件。也不应覆盖安装， 以免造成数据丢失； d）系统故障：涉及到重装系统的情况，请先与客户确认原服务的所有应用程序，包括但不限于：IIS应用、数据库应用、域策略、邮件服务应用、财务软件等。将服务器的所有应用及应用数据、策略进行备份后，请客户签字确认，再进行系统安装。如需第三方软件供应商支持，请客户联系原供应商进行备份后，再预约时间进行服务。
测试	进行一段时间的压力测试，来进一步确认故障是否已经完全修复。
验收确认	a）首先自己检查设备是否恢复正常； b）经检查无误后交给客户检验， 由客户检验完成后签字确认。

C.7 服务器系统常见故障处理流程（续）

注1：服务器运维应满足：
a）服务器维护前，先检查所有应该备份的数据是否完成备份；
b）关闭设备时应：
1）进行正常的本地或远程关机，不允许直接切断服务器电源，如果无法进行本地或远程关机，需要手动长按开关键5s以上；
2）操作前应该明确告知客户这样关机的风险，得到可记录的同意回复后方可操作；
3）进行正常的本地或远程关机，不允许直接切断服务器电源，如果无法进行本地或远程关机，需要手动长按开关键5s以上，但操作前应该明确告知客户这样关机的风险，得到可记录的同意回复后方可操作；
c）更换部件之前带上防静电手腕释放自身的静电；
d）更换部件时要按照服务器服务指南手册给出的步骤进行；
e）更换部件后，拔掉电源的要仔细插好电源；
f）启动设备后，需要恢复操作系统、应用系统或客户数据的要及时恢复；
g）最后需要测试的进行测试，包括更换的部件、操作系统和应用系统等。
注2：服务器巡检要求包括：
a）系统运行环境检查；
b）系统硬件运行情况检查、供电情况、硬件温度情况；
c）检查服务器电源指示灯、内存指示灯、硬盘指示灯、网络指示灯是否正常；
d）检查如发现有隐患的部件应及时反馈并督促客户及时更换；
e）服务器磁盘空间使用情况检查；
f）系统运行状态、性能检查，包括：
1）CPU；
2）内存和交换区使用情况；
3）硬盘和网络的IO情况检查。
g）检查服务器应用软件运行情况；
h）系统日志查看；
i）给客户提供巡检报告。

附 录 D
（资料性）
智能运维工具能力要求

D.1 智能运维工具能力要求

部分智能运维工具的能力要求，见表D.1。

表D.1

场景	目标	技术	过程	数据	算法	资源
桌面软件分发	通过自动化方式对客户端批量下发安装包、动态库文件等，执行安装部署，检查日志，完成软件分发部署。	日志采集技术：Logstash、Filebeat、Flume、Fluentd等工具用于收集和处理来自各种来源的日志。这些工具既可以主动采集数据，也可以被动接收远程主机的日志。 分布式消息中间件：Kafka、Pulsar等分布式消息中间件处理高吞吐量的日志数据。这些中间件能对采集流量进行削峰填谷，支持线性扩容，满足日志采集的实时性、有效性、可靠性和安全性等需求。 日志数据监控技术：Prometheus、Grafana等监控工具用于监控日志数据采集节点的延误和丢失情况。这些工具提供实时监控和告警，帮助及时发现和处理问题。 软件打包和部署技术：Docker、RPM、DPKG、Puppet、Chef、Ansible、SaltStack等工具用于将软件和其依赖项打包并部署到客户端。这些工具帮助自动化部署过程，确保软件在各个客户端的一致性。 网络传输技术：FTP、HTTP、BitTorrent等网络传输协议用于将软件包从服务器传输到客户端。 安全和认证技术：数字签名、SSL/TLS等安全技术用于在软件分发过程中确保软件包的完整性和安全性。	桌面软件分发的过程首先是识别需要分发的软件以及用户需求，然后选择合适的工具进行日志采集、消息传递和软件打包。接着，执行分发过程，包括软件打包、部署和日志数据的收集处理。在分发过程中，需要进行审查以确保软件的完整性和安全性，同时监控日志数据的采集状态。完成分发后，对结果进行回顾和评估，如部署成功率和日志准确性等，然后根据评估结果进行必要的优化和调整，最后实施软件分发。	软件包数据：这是分发过程中最主要的数据，包括软件本身以及其依赖的库和配置文件等。 元数据：关于软件包的信息，如版本号、发布日期、开发者信息、软件包大小、依赖关系等。 配置数据：用于控制软件部署的配置信息，如目标系统的地址、部署路径、运行参数等。 日志数据：在软件分发过程中产生的日志信息，如操作日志、错误日志、性能日志等。这些日志可以用于监控和优化分发过程。 状态数据：关于软件分发状态的信息，如分发进度、成功/失败状态、错误信息等。 安全数据：为了确保软件分发的安全，可能会涉及到一些安全相关的数据，如数字签名、加密密钥、证书等。 用户数据：关于用户的信息，如用户ID、权限信息、设备信息等。这些信息可能会影响到软件分发的策略和结果。	哈希算法：在软件分发过程中，哈希算法通常用于验证软件包的完整性。例如，可以计算软件包的哈希值，并与源服务器提供的哈希值进行比较，以确认软件包在传输过程中没有被修改。 加密算法：为了保护软件包的安全，可能会使用到一些加密算法。例如，可以使用公钥加密算法对软件包进行加密，以保护其内容不被未授权的用户访问。 压缩算法：为了减少软件包的大小，提高传输效率，可能会使用到一些压缩算法。例如，可以使用gzip或bz2等压缩算法对软件包进行压缩。 差异算法：在进行软件更新时，可能会使用到一些差异算法。例如，可以使用bsdiff等算法计算出新版本和旧版本之间的差异，然后只分发这些差异，以减少传输的数据量。 调度算法：在进行大规模的软件分发时，可能会使用到一些调度算法。例如，可以使用一些负载均衡算法来分配软件分发的任务，以确保各个服务器的负载均衡。	根据桌面终端的数量，操作系统版本，需要部署的软件类型及数量，配置适当的算力和网络资源，并完成相应的网络架构建设。

表 D.1(续)

场景	目标	技术	过程	数据	算法	资源
桌面终端漏洞检测	通过自动化的方式对桌面终端设备进行漏洞检测扫描,批量下发漏洞补丁更新,同时记录日志,由终端用户选择重启更新时间。	网络扫描：扫描开放的网络端口和服务。 指纹识别：通过收集的信息确定操作系统和应用程序的版本。这通常涉及到网络协议的特征分析和应用程序行为的分析。 数据库查询：查询漏洞数据库，如CVE(Common Vulnerabilities and Exposures)数据库，找出可能影响目标系统的已知漏洞。 自动补丁应用和配置修改：这涉及到与操作系统的更新服务（如Windows Update）或第三方软件的更新服务进行交互，自动下载并应用相关的补丁。对于可以通过修改配置来修复的漏洞，需要有能力自动修改系统或软件的配置。这可能涉及到文件操作、注册表操作（对于Windows系统）以及对特定软件配置格式的理解等技术。 测试和验证：在自动应用补丁或修改配置后，需要能够验证修复是否成功，以及是否对系统的正常运行产生了影响。这可能涉及到系统监控、日志分析、性能测试等技术。 报告生成：生成报告通常需要数据处理和可视化技术，以便以易于理解的方式呈现扫描结果。 加密和身份验证：为了保护扫描过程的安全，可能需要使用到一些加密和身份验证技术，如SSL/TLS加密，SSH身份验证等。 并行和分布式扫描：在扫描大规模网络时，可能需要使用到一些并行和分布式处理技术，以提高扫描效率。	信息收集：首先，漏洞扫描工具需要收集目标系统的基本信息，如操作系统版本、已安装的软件及其版本等。这通常通过发送探测请求或读取系统信息来完成。 漏洞数据库比对：扫描工具将收集到的信息与已知的漏洞数据库进行比对。这个数据库包含了各种已知的操作系统和软件漏洞，通常由漏洞扫描工具的供应商维护并定期更新。 漏洞验证：对于可能存在的漏洞，扫描工具可能会进行进一步的验证。这通常通过模拟攻击或发送特定的请求来实现。需要注意的是，这个步骤可能会对系统性能或稳定性产生影响，因此在实际操作中需要谨慎进行。 自动修复：对于一些已知的并且有可用补丁的漏洞，扫描工具可以自动应用这些补丁进行修复。 报告生成：最后，扫描工具会生成一份报告，列出发现的所有漏洞以及相关的修复建议。	系统信息:包括操作系统版本、已安装的软件及其版本、开放的网络端口和服务等。 漏洞数据库:包含了各种已知的操作系统和软件漏洞的信息，如CVE（Common Vulnerabilities and Exposures）数据库。 漏洞验证结果:包括验证过程中的请求和响应、模拟攻击的结果等。 补丁信息:包括补丁的来源、适用的软件和版本、补丁的内容(如修复的漏洞、改变的配置等）。 修复结果:包括是否成功应用了补丁、是否成功修改了配置、修复后的系统状态等。 报告数据:包括发现的漏洞、应用的补丁、修改的配置、修复的结果等，用于生成报告。 加密和身份验证数据:包括用于加密和解密的密钥、用于身份验证的证书和密钥等。	网络扫描算法：如SYN扫描、ACK扫描等。 指纹识别算法:这些算法通过分析收集的数据，如网络协议的特征、应用程序的行为等,来确定操作系统和应用程序的版本。 数据库查询算法:这些算法用于在漏洞数据库中搜索与目标系统相关的漏洞。 漏洞验证算法:这些算法通过模拟攻击或发送特定的请求,来验证可能存在的漏洞。例如，缓冲区溢出攻击、SQL注入等。 补丁应用和配置修改算法:这些算法用于自动下载并应用补丁,或者修改系统或软件的配置。例如,补丁的二进制差分和合并算法,配置文件的解析和修改算法等。 测试和验证算法:这些算法用于验证修复是否成功,以及是否对系统的正常运行产生了影响。例如,系统状态的监控算法、日志的分析算法、性能的测试算法等。 加密和身份验证算法:例如，SSL/TLS使用的公钥加密和数字签名算法，SSH使用的密码学哈希和公钥加密算法等。 并行和分布式算法:这些算法用于在多个处理器或计算机之间分配任务,以提高扫描效率。例如,任务调度算法、数据分片算法等。	相关资源主要包括硬件资源（如计算机、网络设备等）、软件资源(如漏洞扫描工具、补丁管理工具、网络扫描工具等）、漏洞数据库、补丁资源、网络资源以及人力资源(如信息安全专家、系统管理员等）。

表 D.1(续)

场景	目标	技术	过程	数据	算法	资源
桌面终端日常巡检自动化	效率提升:有效提高各运维行为的时效性和准确性。	脚本编程:PowerShell脚本语言来编写自动化脚本。 监控工具：通过wmi接口定期收集系统的各种性能数据,然后通过图形化的界面显示出来,方便管理员查看和分析。 配置管理工具:像Ansible、Puppet、Chef等工具可以用来自动化的管理和配置大量的系统,包括执行日常的巡检任务。 日志管理和分析：工具如Logstash、Elasticsearch、Kibana（通常被称为ELK Stack）可以用来收集、存储、搜索和分析大量的系统日志。 容器和虚拟化技术：使用Docker、Kubernetes等容器技术,可以方便地部署和管理自动化的巡检工具和应用。 APIs：通过各种windows shell接口实现windows各种管理操作动作。	定义巡检内容：首先，需要明确巡检的内容和目标。这可能包括检查硬件状态（如CPU使用率、内存使用、硬盘空间等）、软件状态(如操作系统和应用程序的版本、安全更新的安装情况等）、网络连接状态等。 编写巡检脚本：使用选定的工具或语言编写自动化巡检脚本。。 部署和执行脚本：将巡检脚本部署到所有需要巡检的桌面终端上，并设置为定期自动执行。 收集和分析结果：收集所有桌面终端的巡检结果，进行统一的存储和分析。 报告和响应：根据巡检结果生成报告，并对任何发现的问题进行响应。响应可能包括发送警告、自动修复问题、或者通知管理员进行手动处理。 持续优化：根据实际运行情况和需求变化，持续优化巡检内容和工具，以提高巡检的效率和效果。	硬件性能数据：这包括CPU使用率、内存使用、硬盘空间、网络带宽使用等。 软件状态数据:这包括操作系统和应用程序的版本、安全更新的安装情况、服务运行状态等。 网络连接数据:这包括网络连接状态、网络延迟、数据包丢失率等。 日志数据:这包括系统日志、应用程序日志、安全日志等。 巡检结果数据:这是巡检脚本执行后生成的数据，包括每项巡检任务的执行状态、发现的问题、执行时间等。	阈值检测：对于硬件性能数据（如CPU使用率、内存使用、硬盘空间等），设置一些阈值，当数据超过这些阈值时，触发警告或者其他相应的动作。 时间序列分析：对于随时间变化的数据，如网络带宽使用、服务运行状态等，使用时间序列分析的方法，比如滑动平均、指数平滑等,来预测未来的趋势，或者检测异常的变化。 模式匹配：在日志分析中，使用模式匹配的算法,如正则表达式等,来搜索特定的模式或者信息。 聚类分析：在大量的巡检结果中，使用聚类分析的方法，将相似的结果或问题归类在一起，以便于分析和处理。 关联规则学习：从大量的巡检数据中，可能可以发现一些关联规则，比如某些问题总是同时出现，或者某些问题总是在某些条件下出现。这可以使用关联规则学习的方法，如Apriori算法、FP-Growth算法等。	硬件设备，服务器资源；包括脚本编程环境、监控工具、配置管理工具、日志管理和分析工具等软件平台资源；网络带宽资源；服务器网络运维团队资源。

表 D.1(续)

场景	目标	技术	过程	数据	算法	资源
桌面终端威胁IP检测	安全控：提高运维服务和运维对象的安全性和合规性	防火墙和入侵防御系统（IDS/IPS）：实时监控网络流量，检测和防止来自恶意IP的攻击。 网络流量监控和分析工具：实时监控和分析网络流量，发现异常模式或行为。 安全信息和事件管理（SIEM）系统：收集和整合来自各种源的安全事件数据，更全面和深入地检测和分析威胁。 威胁情报平台：提供最新的威胁情报提前防范和应对威胁。 自动化工具和脚本：自动化工具和脚本自动执行一些常规任务，如更新IP黑名单和白名单，发送威胁警报等。 数据分析和机器学习算法：从大量的数据中发现威胁的模式和趋势，提高威胁检测的精度和效率。	数据收集:收集桌面终端的网络流量数据，包括源IP、目标IP、端口号、协议类型等信息。 预处理:对收集的数据进行清洗和格式化,以便于后续的分析和处理。 威胁检测:使用防火墙、入侵检测系统（IDS）和入侵防御系统（IPS）等工具，检测和阻止来自恶意IP的威胁。同时，使用网络流量分析工具,检测可能的恶意IP活动。 威胁分析:使用安全信息和事件管理（SIEM）系统，对收集到的安全事件数据进行分析,发现威胁的模式和趋势。 响应和处理:根据威胁分析的结果,采取相应的措施,如阻止恶意IP的连接请求、修复被恶意IP攻击的系统漏洞等。 后续监控和改进:持续监控桌面终端的网络流量,发现新的威胁IP。同时，根据威胁检测和处理的结果,改进威胁检测的策略和方法。	网络流量数据：这包括源IP地址、目标IP地址、端口号、协议类型、数据包大小、数据包数量等信息。 系统日志数据：这包括操作系统日志、应用程序日志、防火墙日志、入侵检测系统（IDS）日志等，这些日志包含有关潜在威胁的重要信息。 威胁情报数据：这包括已知的恶意IP地址、已知的攻击模式、已知的恶意软件签名等信息，这些信息可以提前防范和应对威胁。 安全事件数据：这包括由防火墙、IDS/IPS、网络流量分析工具等生成的安全事件数据，这些数据可以检测和分析威胁。 响应和处理数据：这包括响应和处理威胁的记录，如阻止恶意IP的操作、修复系统漏洞的操作等，这些数据用来改进威胁检测和处理的策略和方法。	统计学算法：分析网络流量数据的统计特性，如平均值、方差、峰度、偏度等，以发现异常的网络行为。 聚类算法：网络流量数据分成几个类别，以发现异常的网络行为。 分类算法：根据已知的正常和异常网络行为，训练一个模型来预测未知的网络行为。 异常检测算法：检测出不符合正常网络行为模式的异常网络行为。 深度学习算法：从大量的网络流量数据中学习和提取有用的特征，以提高威胁检测的精度和效率。	硬件资源（如服务器和网络设备）进行数据收集和处理，软件资源（如网络监控工具和数据处理软件）支持任务执行，数据资源（如网络流量数据和系统日志数据）进行威胁分析。人力资源，如网络安全工程师和数据分析师，负责系统运维和数据分析。此外，持续的时间投入是必要的，包括数据收集、处理、模型训练和优化等各个环节。

表 D.1(续)

场景	目标	技术	过程	数据	算法	资源
桌面运维知识库智能应用	效率提升：有效提高各运维行为的时效性和准确性	自然语言处理（NLP）：NLP技术可以帮助计算机理解和处理人类语言，使得知识库能够理解用户的查询，提供相关的答案。 机器学习和深度学习：机器学习和深度学习可以用于从大量的运维数据中学习和提取有用的特征，以提高知识库的检索和推荐能力。 transformer：通过自注意力机制增强远距离文本语句理解能力。 用户交互界面：用户交互界面可以使得用户更方便地查询和使用知识库，提高知识库的使用体验。 数据分析：数据分析帮助理解用户的需求和行为，以优化知识库的功能和性能。 云计算和分布式系统：云计算和分布式系统提供计算和存储能力，以支持知识库的大规模运行。	数据收集：收集所有相关的桌面运维知识和信息，这可能包括文档、教程、论坛帖子、问题与答案等。 数据预处理：对收集的数据进行预处理，包括清洗、格式化、标注等，以便后续的处理和分析。 知识库构建：使用NLP、机器学习等技术，将预处理后的数据转化为知识图谱或其他形式的知识库。 查询处理：当用户提出查询时，系统会使用NLP技术理解查询的意图，并使用知识库检索相关的信息。 结果返回：系统将检索到的信息返回给用户，可能以列表、图形或其他形式展示。 用户交互：用户可以对返回的结果进行反馈，系统根据反馈进行学习和优化。 持续更新和优化：系统需要不断收集新的数据，更新知识库，并根据用户的反馈和行为数据进行优化。	知识数据：包括各种桌面运维相关的文档、教程、论坛帖子、问题与答案等。 用户查询数据：用户在使用知识库时输入的查询，这些数据可以用于理解用户的需求，优化知识库的检索和推荐算法。 用户反馈数据：用户对知识库返回结果的反馈，这些数据可以用于评估知识库的性能，优化知识库的检索和推荐算法。 用户行为数据：用户在使用知识库时的行为数据，如查询次数、停留时间、点击率等，这些数据可以用于理解用户的行为，优化知识库的设计和服务。 运维事件数据：运维过程中产生的事件数据，如故障报告、解决方案等，这些数据可以用于更新和丰富知识库。	自然语言处理(NLP)算法：这些算法用于理解和处理用户的查询，包括词语的分词、词性标注、命名实体识别、依存句法分析、情感分析等。这些算法还可以用于处理和组织知识库的内容。 信息检索算法：这些算法用于根据用户的查询从知识库中检索相关的信息，包括布尔检索、向量空间模型、概率检索模型、语言模型等。 机器学习和深度学习算法：这些算法用于从大量的运维数据中学习和提取有用的特征，以提高知识库的检索和推荐能力，包括分类算法、聚类算法、回归算法、神经网络、卷积神经网络（CNN）、循环神经网络（RNN）、长短期记忆网络(LSTM)、Transformer等。 推荐系统算法：这些算法用于根据用户的历史行为和偏好，推荐他们可能感兴趣的信息，包括协同过滤、基于内容的推荐、混合推荐等。	硬件资源如服务器和存储设备支持数据处理和模型训练。软件资源，如数据库管理系统和机器学习库，提供数据处理和模型训练的平台。数据资源，包括运维知识和用户行为数据，用于构建知识库和优化系统。人力资源包括数据科学家和工程师，负责系统的开发和运维。同时，还需要时间资源进行各阶段的工作，包括数据收集、处理、系统开发和优化。

附 录 E
（规范性）
服务要求评价工具

E.1 桌面及外围设备运维服务要求评价内容

桌面及外围设备运维服务要求评价内容，由评测人员实施。

表E.1 桌面及外围设备运维服务规范评价工具

评价项目	评价要求	分值	体验系数α	体验描述	评价得分
5.1 信息化管理（10）	a）集成相关信息系统，实现组织管理与主营业务的信息化，推进组织管理信息系统中项目业务管理和财务管理的信息系统深度集成； b）集成知识库，实现知识的共享，充分挖掘和利用知识的价值，支撑智慧组织建设； c）集成监控工具，具备IT系统运行状况实时监视、故障预警告知以及远程支持的服务能力； d）集成服务台，包括服务请求的接收、记录、跟踪和反馈等流程，实现服务流程在线化； e）网络安全自查、巡检、风险评估及安全整改，并持续优化网络安全； f）容灾备份，具有灾难恢复系统、防病毒、防篡改、防泄漏系统；	10			
5.2 备件管理（5）	a）建立供应商选择和评价管理，规范备件的采购过程； b）建立备件出入库管理制度，规范入库备件的标识、使用、核销和账务管理； c）采用信息化工具对备件库管理，确保备件库信息真实有效； d）管理备件状态，以确保其功能满足运行维护需求。	5			
5.3 智能运维工具（5）	a）识别智能运维场景，分析运维场景的需求，目标，特征，可行性，形成设计方案； b）选择适宜的技术手段，构建实现能力，满足实时性，有效性，可靠性，安全性等技术需求； c）明确场景数据需求，对实现过程进行评审，优化和变更管控； d）使用数据建模工具，完成数据模型的定义、设计和开发； e）在数据存储，数据加密，数据压缩，队列调度等关键处理中采用相适宜的算法，满足元数据管理的需要； f）配置适当的资源满足智能运维工具的运行要求，包括计算，网络，存储等。 g）建立评估机制，定期进行效果评估，制定改进措施，持续改进，快速迭代。 h）覆盖服务的主要场景，包括并不限于软件分发，终端漏洞检测，终端日常巡检自动化，终端威胁IP检测，运维知识库智能应用，访问控制审核等。	5			
5.4 资产管理（10）	a）应识别和记录所有资产的状态和位置，以便于进行有效的管理和维护，满足资产管理的实时性和准确性需求； b）建立有效的通知机制，对未纳入管理的设备进行实时通知，提高设备管理的全面性； c）管理软件许可证，类别和合规性； d）统计特定软件的使用情况详细信息，例如使用次数，总使用时间，	10			

表 E.1 桌面及外围设备运维服务规范评价工具（续）

评价项目	评价要求	分值	体验系数α	体验描述	评价得分
	具有特定软件的系统等； e）在网络中检测，阻止和自动卸载禁止的软件； f）具有设备锁定功能，以保证设备的安全性和数据的完整性； g）按使用期限，磁盘使用情况，类型进行资产排序。； h）针对许可证数量及终端安装数量进行统计，当许可不足或过多时报警； i）支持将报告导出为PDF或CSV格式； j）资产管理统计效率达到100台/人天。				
6.1 基本要求（6）	a）识别运行维护服务有关人员的分类，明确其职责、权限以及与岗位相适应的能力要求，如教育程度、专业技能、工作经验等。 b）根据服务要求配备适合的管理和作业人员，特殊岗位按规定要求持证上岗。 c）识别培训需求，制定并实施员工培训计划，做好员工上岗前和在岗中的培训。 d）建立员工绩效考核管理制度，规定考核内容、标准，并将考核结果作为人力资源管理评价和质量管理改进的依据。 e）建立和实施人才梯队培育制度，并定期评价培育规划的充分性、适宜性和有效性。	6			
6.2 团队建设（3）	a）满足一线提供运维服务所需的人员，即在保持高绩效的同时具备良好的服务意识、职业素养以及运行维护基本知识和技能的人员； b）满足二线提供支持服务和服务管理所需的高潜人才，即在保持高绩效的同时具备领导意愿、取得成功的能力以及对组织有着更高敬业度的人才； c）在相应的行业领域和专业范围内配置满足战略发展需求的战略性人才； d）考虑行业未来发展趋势配置满足组织技术创新需要的研发人才。	3			
6.3 行为监督（3）	a）组织应制定、实施能够体现组织文化并被全体员工认同和遵守的服务人员基本行为准则和日常行为规范。 b）组织应依据基本行为准则和日常行为规范建立服务人员行为监督管理机制，监督、评价、分析、改进服务人员行为及其后续的工作内容与工作方式。	3			
6.4 人员培训（3）	a）组织应依据理论、实训与实践相结合的培训组织体系以及相应的管理和激励； b）组织应有专门的部门进行培训的实施和管理，培训教育过程和结果应保留记录； c）组织应针对运行维护服务常见问题的描述、分析和解决方法建立相关的知识库，并利用信息化工具进行知识的收集、共享以及生命周期管理。 d）组织应建立技能培训平台，并配置至少包括防火墙、无线网络、sd-wan 、网上行为管理设备在内的IT网络相关的主流厂商设备，以及虚拟化平台部署环境。 e）组织应至少每半年开展一次技能更新培训，培训内容至少应包括：windows系统、exchange邮件系统、文件系统、域环境、vsphere 虚拟化环境部署、交换机、路由器、防火墙、VPN设备常规操作技能等。 f）组织应设置专业技术人员和技术管理人员技术分级标准、培训及考核方案，定期评价培育规划的充分性、适宜性和有效性，相关人员应经培训并通过考核才能上岗。	3			

表 E.1 桌面及外围设备运维服务规范评价工具（续）

评价项目	评价要求		分值	体验系数α	体验描述	评价得分
7.1 基本要求（27）	7.1.1 服务要求	a）提供相应的服务前应征得客户同意，遇到需方提出额外要求时，服务人员应得到上级授权后再做处理； b）服务人员应确保个人联系方式畅通，表达准确，注意仪表和礼仪，在客户现场应遵守客户管理制度； c）运维工程师若不能按要求到场则需要在第一时间向组织说明，由组织安排其他运维工程师提供应急服务； d）对客户交代的每件事情要有始有终，跟进过程要及时汇报； e）事件完成时限应符合附录A的要求，处理及时率 ≥ 95%，服务可用性 ≥ 99.6%。 f）应根据客户需求，制定数据灾备管理方案，参照附录B。 服务过程中应注重IT系统故障处理的规范性，尽量减低因操作不慎带来的风险，操作流程可参照附录C。	.			
	7.1.2 跨平台支持	a）开发统一的管理平台或接口，用以监控和管理多种操作系统上的资产，确保无论资产处于何种操作系统，均能够被有效地管理； b）提供自动化配置和部署工具，支持在多种操作系统上快速部署和配置软件及服务； c）实施跨平台的监控系统，用于实时收集多种操作系统的性能数据，并生成统一的报告，以便于运维人员分析和决策； d）定期进行兼容性测试，确保运维工具和应用在多种操作系统上都能够稳定工作，且具备良好的用户体验； e）建立灵活的访问控制策略，确保用户能够根据权限在多种操作系统上访问相应的资源和服务；	5			

表 E.1 桌面及外围设备运维服务规范评价工具（续）

评价项目	评价要求		分值	体验系数α	体验描述	评价得分
		f）制定统一的安全策略，确保在多种操作系统上都能执行相同的安全标准和措施； g）实现数据的跨平台同步与备份，保证数据的一致性和可恢复性； h）管理多种操作系统间的兼容性和依赖性问题，确保跨平台应用的连续性和稳定性； i）提供全面的技术支持，确保在多种操作系统上，用户都能获得及时有效的帮助； j）应覆盖主流操作系统80%以上。				
	7.1.3 操作系统及应用补丁更新	a）建立实时监控机制，对所有管理的操作系统和应用的运行状态进行监控，以便及时发现异常或潜在的安全漏洞，并通过警报系统快速通知运维团队； b）对发现的安全漏洞进行评估，根据漏洞的严重性和对业务的影响程度，为补丁更新制定优先级，确保关键系统的安全性最先得到加强； c）采用自动化工具来管理补丁的下载、测试和部署过程，减少人为操作的错误，提高补丁管理的效率和准确性； d）对补丁部署后的系统和应用进行验证，确保补丁正确应用且不影响系统的正常运行； e）在进行补丁更新前，确保有完整的备份，以便在更新出现问题时能够快速回滚到稳定状态； f）更新周期应在补丁发布后的45天内完成。	5			
	7.1.4 终端软件自动部署	a）明确组织的需求，包括需要部署的软件类型、目标终端的数量和类型、预期的部署时间等； b）根据需求分析的结果，选	5			

表 E.1 桌面及外围设备运维服务规范评价工具（续）

评价项目	评价要求		分值	体验系数α	体验描述	评价得分
		择合适的自动化部署工具。工具的选择应考虑其是否支持跨平台部署、是否具有丰富的功能、是否易于使用和管理等因素； c）对工具进行合理配置。包括设置部署策略、定义部署流程、配置软件仓库等； d）在少量终端上进行测试部署，验证配置的正确性和部署的效果，测试部署的结果将为实际部署提供参考； e）测试部署成功后，在所有目标终端上进行实施部署。在部署过程中，需要密切监控部署的进度和结果，及时发现并解决问题； f）部署完成后，需要进行后续的管理，包括监控软件的运行状态、更新软件和补丁、管理软件许可证等，根据实际运行情况，调整部署策略和流程，以提高部署的效果； g）自动化和批量化应覆盖90%以上的部署场景。				
	7.1.5 终端自动运维操作	a）对运维流程进行彻底的审查和评估，确定可自动化的操作。制定全面的自动化策略，包括目标、时间表、预算和资源分配； b）根据自动化需求选择合适的工具和平台，包括监控工具、日志分析器、配置管理系统、安全扫描工具、备份软件等，确保工具可集成并协同工作，提供统一的自动化解决方案； c）准备必要的基础设施，包括服务器、存储和网络资源，以支持自动化工具的部署和运行，确保有足够的容量来处理监控数据、日志文件、备份集等； d）开发自动化脚本和流程，以执行常规任务，如监控性能指标、收集和分析日志、管理用户账户、安装和更新软	5			

表 E.1 桌面及外围设备运维服务规范评价工具（续）

评价项目	评价要求		分值	体验系数α	体验描述	评价得分
		件、维护系统配置、执行安全扫描、管理网络设置、跟踪资产和故障响应； e）在控制环境中对自动化脚本和流程进行测试，应确保按预期工作，不会干扰现有的业务流程，验证自动化操作是否符合安全标准和合规要求； f）测试完成后，逐步部署自动化解决方案到生产环境。监控部署过程，确保自动化操作不会导致服务中断或其他问题； g）应持续监督性能和效率，收集反馈，根据实际运行情况不断改进自动化流程，确保覆盖率达到目标，对于无法自动化的特殊情况，应制定手动处理策略； h）应为运维团队编制完整的操作文档，说明自动化系统的工作原理和操作方法。对团队成员进行培训，确保能够有效地使用自动化工具和处理异常情况； i）定期进行安全审计和合规性检查，以确保自动化操作不会引入新的安全风险，并且符合行业标准和法规要求； j）应进行持续的监控和维护，以应对基础设施变化、新的安全威胁、软件更新和其他可能影响自动化效率的因素； k）自动化和批量化应覆盖90%以上的运维操作场景。				
7.2 电话支持（3）	a）操作过程描述清晰，并和客户确认每一步操作显示的窗口和现象； b）如果某些步骤等待时间比较长，提前向客户说明； c）如果尝试过一两种方法，故障仍不能解决，向顾客建议改由运维工程师上门服务。		3			
7.3 远程协助（3）	a）远程报修需要记录客户名称、联系人、联系方式、报修问题； b）远程连接后，先让客户操作确认故障现象，并提醒客户自行保存文档，再按照常流程处理； c）结束服务时由客户先断开远程后，服务人员才能断远程； d）如果尝试过两种或以上方法，故障仍不能解决，向顾客建议改由运		3			

表 E.1 桌面及外围设备运维服务规范评价工具（续）

评价项目	评价要求	分值	体验系数α	体验描述	评价得分
	维工程师上门服务。				
7.4 应急服务（3）	a）组织应根据服务规模配置相应的运维工程师，密度比应至少达到1:18（运维工程师 ： 客户数量）； b）应及时响应客户需求，并初步确认故障原因及处理方式，响应时间 ≤ 5 min； c）应急事件需要记录客户信息、联系人信息、处理事务、预约到场时间、服务地址； d）运维工程师出发前应检查确认所携带的工具、服务单、系统盘，人员到场时间 ≤ 2 h； e）运维工程师现场进行的所操作都应在工单上进行记录，内容至少包括工作内容，服务标签、耗时、处理过程、是否解决； f）对复杂或存在风险的工作做好预案，经审核后实施，如现场碰到30min内无法处理问题直接进行问题升级； g）工单完成后客户签字确认，该项目服务经理审核工单关闭服务事件。	3			
7.5 驻场服务（3）	a）应自备工具、服务单、系统盘； b）应按客户方上班时间准时上下班并按组织要求做考勤记录； c）按标准的工作清单提供服务并填写工单，内容包括工作内容，服务标签、耗时、处理过程、是否解决； d）工单完成后客户签字确认，该项目服务经理审核工单关闭服务事件 e）服务中如果碰到无法解决的技术问题，应提交问题升级； f）应主动询问客户负责人是否有其他工作安排，主动帮助客户员工。	3			
7.6 AI服务（3）	a）宜实现对声音的实时采集和识别，自动将语音处理成自然文本； b）宜集成人工智能技术驱动的自然语言处理工具，具有语言理解和文本生成能力； c）宜集成组织知识库，并训练运维工程师模型，根据客户输入的关键词，进行检索查询，可回复或处理技术问题； d）宜利用大数据建模和算法实现，处理客户日常运维数据，用于加速服务报告生成和服务需求预测。	3			
7.7 定期巡检（3）	a）按照SLA约定制定巡检计划，内容包括巡检项目，巡检周期，巡检要求； b）执行巡检任务前应提前征得客户同意，运维工程师按时抵达现场根据巡检工单进行巡检； c）巡检完成后客户签字确认，一周内提交巡检报告； d）针对巡检中发现的问题，按照SLA约定的方案进行处理。	3			
8 信息安全（5）	应符合GB/T 28827.1-2022 中7.12 的要求，无因组织管理不当导致的泄密事故发生。	5			
9 持续改进（5）	应符合GB/T 28827.1-2022 中5.3.4的要求。	5			

参 考 文 献

[1] GB/T4754—2011 国民经济行业分类
[2] GB/T 19001-2016 质量管理体系 要求
[3] GB/T 19580-2012 卓越绩效评价准则
[4] GB/T 22080-2016 信息安全管理体系要求
[5] GB/T 24405.2—2010 信息技术 服务管理 第2部分:实践规则
[6] GB/T 28827.2—2012 信息技术服务 运行维护 第2部分:交付规范
[7] GB/T 33770.6 信息技术服务 外包 第6部分:服务需求方通用要求
[8] GB/T 34960.1—2017 信息技术服务 治理 第1部分:通用要求
[9] GB/T 36074.2—2018 信息技术服务 服务管理 第2部分:实施指南
[10] GB/T 36074.3—2019 信息技术服务 服务管理 第3部分:技术要求
[11] GB/T 37696—2019 信息技术服务 从业人员能力评价要求
[12] SJ/T 11693.1-2017 信息技术服务 服务管理 第1部分:通用要求
[13] ISO/ICDIS20000-1：2018 ITServiceManagementandITGovernance
[14] InformationTechnologyInfrastructureLibrary(ITIL)Version3Foundation
[15] InformationTechnologyInfrastructureLibrary(ITIL)Version4Foundation