ICS

T/

团　　体　　标　　准

信息技术应用创新项目运行维护服务标准

（征求意见稿）

xxxx - xx - xx 发布　　xxxx - xx - xx 实施

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。

本文件起草单位：XXX。

本文件主要起草人：XXX、XXX、……。

本文件首次修订。

引　言

随着信息技术应用创新项目（以下简称“信创项目”）的开展实施，项目由实施交付阶段逐步进入长期的运维服务保障。在此背景下，信创项目的建设和运行维护同等重要，信创项目持续高效应用更依赖于高质量的运行维护，目前，GB/T 28827《信息技术服务 运行维护》规定了信息技术服务的通用要求与规范，缺乏针对国产化软硬件设备的运行维护服务标准规范。因此，急需一种有效的标准，提供运行维护服务需方选择和评价供方以及运行维护服务供方改进和提升自身的运行维护服务能力。制定《信息技术应用创新项目运行维护服务标准》，按照标准要求实施信创项目运行维护服务，客观公正地评价服务机构的服务能力，既可作为服务机构开展自我评价的规范和标准，为信创行业规范业务行为、提升管理水平、加强行业监督、强化行业宏观管理和决策水平等方面提供有力的技术保障。

信息技术应用创新项目运行维护服务标准

1 范围

本标准规定了信息技术应用创新项目运行维护服务的总体要求、服务内容、组织架构及保障措施。

本标准适用于信创项目涵盖的终端、外设、服务器、基础软件和应用系统等的运维服务。适用于用户单位信创项目系统运行维护服务能力的建设、管理和评估。

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 信息技术服务 运行维护

3 术语和定义

下列术语和定义适用于本标准。

3.1

人员

组织中从事运行维护服务的人。

3.2

过程

组织中利用输入实现预期结果的相互关联或相互作用的一组活动。

3.3

技术

组织中为交付运行维护服务研究和转化的知识、经验、手段、方法的总和。

3.4

关键指标

在评估、衡量运行维护服务能力过程中起决定性作用的指数、规格、标准，一般用数据表示。

3.5

服务台

面向用户的、完成大部分支持工作的支持组。

3.6

服务级别协议

运行维护服务组织与需方之间约定的用以识别服务及其绩效的协议。

3.7

信创业务系统

在约定的信创项目业务环境下，用于实现用户特定需求的应用软件及其运行的软环境和承载业务直接关联的数据。信创项目业务系统的应用软件运行软环境，包括信创操作系统、信创中间件、信创数据库等。

3.8

信创应用软件

设计用于实现信创用户的特定需要而非计算机本身问题的软件。例如：信创项目国产化运行环境的人力资源管理软件、客户关系管理软件、办公自动化软件等。

3.9

信息系统

由计算机硬件（物理和虚拟资源）、网络和通讯设备、计算机软件、信息资源、信息用户和规章制度组成的以收集（或获取）、处理、存储、分配信息为目的的人机一体化系统。

3.10

安全性

对业务系统进行的保护，以防止其受到意外的或蓄意的存取、使用、修改、毁坏或泄密。

3.11

易用性

业务系统在指定的使用环境中，为指定的目标，在有效性、效率和满意度特性方面可为指定用户使用的程度。

3.12

可维护性

业务系统能修改以排除故障、改进性能或其他属性或适应变更了的环境的容易程度。

3.13

故障

指业务系统在没有预先安排的情况下出现的对用户提供服务的中断。

3.14

事件

指导致或可能导致服务中断或服务质量下降的任一事态，事件包括用户的故障、申告、咨询以及监控系统自动产生的告警。

3.15

缺陷

指业务系统发生的异常或存在的隐患（包括信息安全漏洞），这些异常或隐患将影响业务系统安全可靠运行、性能、寿命或服务质量。缺陷按照其严重程度分为紧急缺陷（致命缺陷）、重大缺陷（严重缺陷）、一般缺陷。

3.16

改正性维护

改正性维护是指改正在系统开发阶段已发生而系统测试阶段尚未发现的错误。通常所发现的错误有的不太重要，不影响系统的正常运行，其维护工作可随时进行。

3.17

适应性维护

适应性维护是指使用软件适应信息技术变化和管理需求变化而进行的修改。

3.18

完善性维护

完善性维护是为扩充功能和改善性能而进行的修改，主要是指对已有的软件系统增加一些在系统分析和设计阶段中没有规定的功能与性能特征。

3.19

预防性维护

预防性维护为了改进应用软件的可靠性和可维护性，为了适应未来的软硬件环境的变化，应主动增加预防性的新的功能，以使应用系统适应各类变化而不被淘汰。

3.20

块设备

块设备是 I/O 设备中的一类，当我们的应用层对该设备读写时,是按扇区大小来读写数据的，若读写的数据小于扇区的大小,就会需要缓存区，可以随机读写设备的任意位置处的数据，例如普通文件(*.txt 等)、硬盘、U 盘、SD 卡等。

3.21

MD5 值

MD5 的全称是 Message-Digest Algorithm 5，它一种被广泛使用的密码散列函数，可以产生出一个 128 位（16 字节）的散列值（hash value），用于确保信息传输完整一致。MD5 值等同于文件的 ID，它的值是唯一的。如果文件已被修改（例如嵌入式病毒，特洛伊木马等），其 MD5 值将发生变化。

3.22

JVM

JVM 是 Java Virtual Machine（Java 虚拟机）的缩写，JVM 是一种用于计算设备的规范，它是一个虚构出来的计算机，是通过在实际的计算机上仿真模拟各种计算机功能来实现的。引入 Java 语言虚拟机后，Java 语言在不同平台上运行时不需要重新编译。Java 语言使用 Java 虚拟机屏蔽了与具体平台相关的信息，使得 Java 语言编译程序只需生成在 Java 虚拟机上运行的目标代码（字节码），就可以在多种平台上不加修改地运行。

3.23

内存泄漏

内存泄漏（Memory Leak）是指程序中已动态分配的堆内存由于某种原因程序未释放或无法释放，造成系统内存的浪费，导致程序运行速度减慢甚至系统崩溃等严重后果。

3.24

SQL

结构化查询语言（Structured Query Language）简称 SQL，是一种特殊目的的编程语言，是一种数据库查询和程序设计语言，用于存取数据以及查询、更新和管理关系数据库系统。结构化查询语言是高级的非过程化编程语言，允许用户在高层数据结构上工作。它不要求用户指定对数据的存放方法，也不需要用户了解具体的数据存放方式,所以具有完全不同底层结构的不同数据库系统,可以使用相同的结构化查询语言作为数据输入与管理的接口。结构化查询语言语句可以嵌套，这使它具有极大的灵活性和强大的功能。

3.25

I/O

输入/输出（Input/Output，简写为 I/O）是信息处理系统（例如计算器）与外部世界（可能是人类或另一信息处理系统）之间的通信。输入是系统接收的信号或数据，输出则是从其发送的信号或数据。该术语也可以用作行动的一部分；到“运行 I/O”是运行输入或输出的操作。

3.26

IP

IP 地址（Internet Protocol Address）是指互联网协议地址，又译为网际协议地址。IP 地址是 IP 协议提供的一种统一的地址格式，它为互联网上的每一个网络和每一台主机分配一个逻辑地址，以此来屏蔽物理地址的差异。

3.27

MAC

MAC 地址（Media Access Control Address），直译为媒体存取控制位址，也称为局域网地址（LAN Address），MAC 位址，以太网地址（Ethernet Address）或物理地址（Physical Address），它是一个用来确认网络设备位置的位址。在 OSI 模型中，第三层网络层负责 IP 地址，第二层数据链路层则负责 MAC 位址。MAC 地址用于在网络中唯一标示一个网卡，一台设备若有一或多个网卡，则每个网卡都需要并会有一个唯一的 MAC 地址。

3.28

VLAN

VLAN（Virtual Local Area Network）的中文名为"虚拟局域网"。虚拟局域网（VLAN）是一组逻辑上的设备和用户，这些设备和用户并不受物理位置的限制，可以根据功能、部门及应用等因素将它们组织起来，相互之间的通信就好像它们在同一个网段中一样，由此得名虚拟局域网。

3.29

TCP/IP 协议

TCP/IP（Transmission Control Protocol/Internet Protocol，传输控制协议/网际协议）是指能够在多个不同网络间实现信息传输的协议簇。TCP/IP 协议不仅仅指的是 TCP 和 IP 两个协议，而是指一个由 FTP、SMTP、TCP、UDP、IP 等协议构成的协议簇，只是因为在 TCP/IP 协议中 TCP 协议和 IP 协议最具代表性，所以被称为 TCP/IP 协议。

3.30

JMX 协议

JMX（Java Management Extensions，即 Java 管理扩展）是一个为应用程序、设备、系统等植入管理功能的框架。JMX 可以跨越一系列异构操作系统平台、系统体系结构和网络传输协议，灵活的开发无缝集成的系统、网络和服务管理应用。

3.31

JDBC 协议

Java 数据库连接，（Java Database Connectivity，简称 JDBC）是 Java 语言中用来规范客户端程序如何来访问数据库的应用程序接口，提供了诸如查询和更新数据库中数据的方法。我们通常说的 JDBC 是面向关系型数据库的。

3.32

SNMP 协议

简单网络管理协议（SNMP）是专门设计用于在 IP 网络管理网络节点（服务器、工作站、路由器、交换机及 HUBS 等）的一种标准协议，它是一种应用层协议。

3.33

B/S

B/S 结构（Browser/Server，浏览器/服务器模式），是 WEB 兴起后的一种网络结构模式，WEB 浏览器是客户端最主要的应用软件。这种模式统一了客户端，将系统功能实现的核心部分集中到服务器上，简化了系统的开发、维护和使用。客户机上只要安装一个浏览器。

3.34

用户

通过桌面及外围设备管理和使用信息系统应用的人员。

3.35

服务级别协议

服务供方与需方之间签署的描述符合和约定服务级别的协议。

3.36

功能置换

当服务对象整体功能丧失或部分性能下降时，在满足服务协议规定的前提下，服务供方临时性提供的能满足需方应用最低需求的设备、软件或者人工服务。

3.37

监督控制

是指制定标准、统一的使用、管理制度或指导手册，并且以制定的设备运行维护服务行为规范或作业指导为标准监督运行维护完成情况。

3.38

定期检查

指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。

3.39

日常维护

指供方对设备进行的主动服务操作，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。

3.40

宣传指引

指供方为提高用户使用水平，改善用户使用习惯所采取的一系列主动服务行为，引导用户利用各种自助服务方法或工具解决桌面及外围设备的故障。

4 信创项目运维服务等级

4.1 等级划分原则

信创项目运维服务等级划分应在项目立项阶段，由业务管理部门、技术承办单位共同确定。信创运维服务涉及到信息系统分为核心系统和非核心系统，核心系统就是对该单位业务有重大影响的系统。信创项目运维服务等级的划分需要根据信创项目所涵盖信息系统和影响程度进行运维服务等级确定。

信创项目中涉及多个信息系统运行的，运维服务等级应以信创项目中信息系统运行维护服务最高保障要求为基准确定。

信创项目运维服务划分为三个等级，一级为最低级别，三级为最高级别。

4.2 服务等级定义

4.2.1 一级运维服务

一级运维的是非核心系统，影响是局部的，信息系统中断后对业务工作开展基本没有影响或只是轻微影响。此类信息系统的运行维护服务可以定义为一级运维服务。

4.2.2 二级运维服务

二级运维的是主要系统，影响单位业务部门，但没有社会影响。此类信息系统的运行维护服务可以定义为二级运维服务。

4.2.3 三级运维服务

三级运维的是核心业务，影响是全单位的，且有社会影响。中断后对业务工作有重大影响，社会影响大，政治影响大。此类信息系统的运行维护服务可以定义为三级运维服务。

4.3 运维服务内容

信创运维不同服务等级的具体内容见表1。

表 1 信创运维服务表

服务等级	服务内容
一	提供信创基础软硬件及业务系统运维保障，包括终端、服务器、操作系统、外设等设备硬件及运行环境检查、系统故障检测及排除、系统或相关软件终端重部署及调试；数据库系统维护、配置变更、部署及调试、故障检测及排除；中间件运行维护、软件补丁升级、故障检测及排除、相关软件重部署及配置；网络故障检测及排除、主机固件软件版本升级更新、网络系统重部署及调试；机房硬件维护、系统账号维护服务、数据备份服务、通知等基础服务。实行“5 天×8 小时”基础环境层面的技术支持和热线服务，系统运维需求响应及恢复在 3 个工作日以内完成。无需运维人员驻场，但需提供负责运维服务人员能力等级为初级。
二	在一级运维服务的基础上，提供信创软硬件维护，系统监控备份以及性能优化服务。提供运信创维工具的使用管理，提供非工作时段故障调度和热线服务，实行“5 天×24 小时”基础环境层面的技

	术支持和热线服务，系统运维需求响应及恢复在 1 个工作日以内完成。运维人员实行工作日驻场，提供运维服务人员能力等级为中级。
三	在二级运维服务的基础上，提供信创基础软硬件及业务系统运维保障，包括主机、机房、网络、外设等基础软硬件；提供应用系统兼容性测试，提供安全漏洞扫描、安全风险评估、安全加固服务。实行“7 天×24 小时”基础环境层面的技术支持和热线服务，系统运维需求响应及恢复在 8 小时以内完成。运维人员全天驻场，提供运维服务人员能力等级为高级。

5 运维服务流程规范

5.1 概述

信创运维服务流程以服务台为核心，将五个主流程相互关联，形成一整套相辅相成运维服务的处理机制，同时将相关经验知识记录并沉淀下来，以支撑信创运维的持续改进优化。运维流程框架见图1。

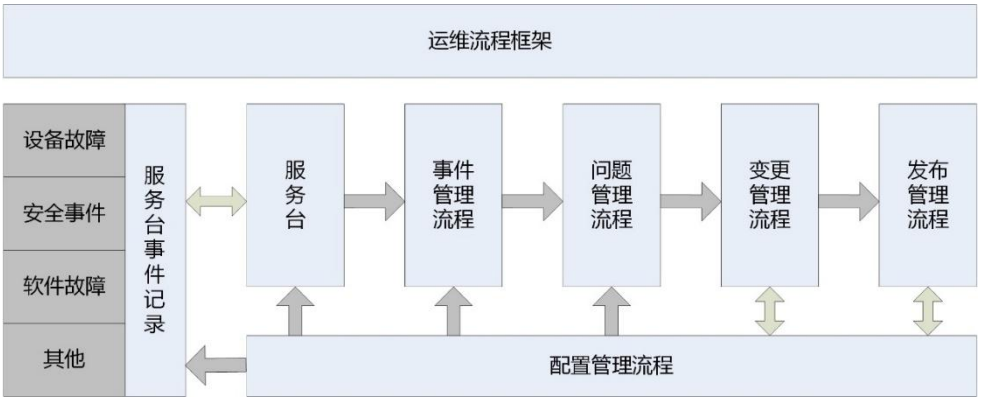

图 1 运维流程框架

5.2 服务台

信创项目运维服务流程中服务台是支持运维服务的核心功能，它与各个管理流程联系密切。所有管理流程都要通过服务台为用户提供联系，解答用户的相关问题和需求，或为用户寻求相应的支撑及资源。

信创项目运维服务应针对服务场景的特点建立服务台，服务台应具备服务接入、信息交互、资源调度、服务过程管控等职能，并结合自身业务特点进行管理。考虑到信创产品的持续改进需要，服务台接收的服务请求与事件需要记录用户使用的软硬件产品运行环境（产品厂家与型号、软件版本），方便进行运维分析与产品改进。服务台需要对服务请求与事件等信息进行记录、跟踪、反馈及统计分析。

服务台应该建立信创硬件设备厂家、基础软件厂家的售后技术支撑联系人与联系方式。

5.3 事件管理流程

信创项目事件管理流程的主要目标是尽可能在最短时间内解决问题，恢复相关服务并减少事件对业务的不利影响，尽可能保证最好的服务质量。

信创项目运维组织为确保具有及时解决事件的能力，应建立事件服务请求响应和事件服务处置过程。服务请求与事件需要记录用户的信创软硬件运行环境、软硬件版本信息，在完成事件处理后需要反馈处理措施，需要时进行知识沉淀，服务台对事件进行分类统计，并定时反馈给服务商或厂家，完成产品的持续改善。服务台需要对服务请求与事件处理过程进行监控与跟踪。必要时，需要进行事件升级。事件管理流程见图2。

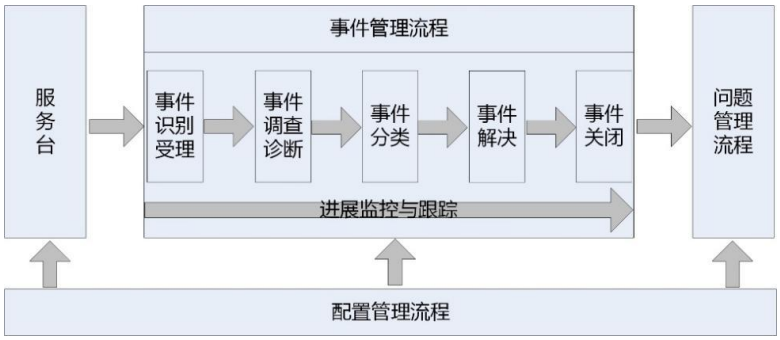

图 2　事件管理流程

5.4　问题管理流程

信创项目问题管理流程的主要目标是找出并消除引起问题的根本原因，预防问题和事件的再次发生，并将未能解决的事件的影响降低到最小。问题管理流程包括诊断事件根本原因和确定实施问题解决方案所需要的活动及资源，通过合适的控制过程，尤其是变更管理和发布管理，确保解决方案的落实。

信创项目运维组织应建立问题管理流程，分析问题根本原因，进行问题分类和确定解决方案。问题解决后，需要按问题类别对问题解决方案进行知识沉淀和知识管理，为运维组织服务优化和产品厂家持续改进提供支持帮助与建议。如果问题需要产品厂家进行技术支持的，需要与产品厂家建立服务支持通道，以有利于对信创产品的持续改进。问题管理流程见图3。

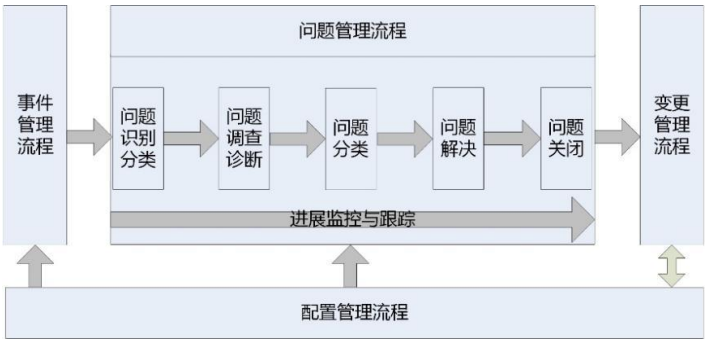

图 3　问题管理流程

5.5　变更管理流程

信创项目变更管理流程主要实现所有基础设施和应用系统的变更，变更管理应记录并对所有变更进行分类，应评估变更请求的风险、影响和业务收益。其主要目标是以对服务最小的干扰实现有益的变更。

信创项目或组织应建立变更管理流程，包括变更请求、评估、审核、实施、确认和回顾等。通过变更管理，完成用户变更需求的有效管理和控制。变更管理流程见图4。

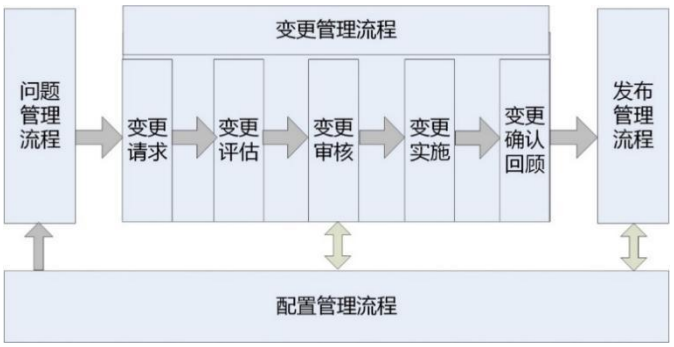

图 4　变更管理流程

5.6 发布管理流程

信创项目发布管理流程其主要目标是保证运行环境的完整性被保护以及正确的组件被发布。由发布管理制定发布方案以及计划，明确发布的内容、角色职责及资源分配、发布日期等。根据变更管理实施情况组织培训和测试，确保变更和发布的成功。

信创项目或组织应建立发布管理流程，控制部署实施活动，确保变更的成功导入，完成信创软件和硬件的规划、协调和实施（适配、测试、部署）。在变更管理的控制和配置管理的支持下，通过发布管理，确保与变更相关的硬件和软件是可追溯的和安全的，确保只有正确的、经过批准和测试的版本才能被安装。发布管理流程见图5。

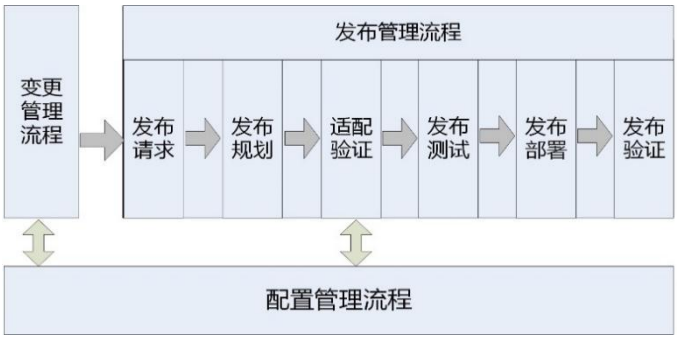

图 5　发布管理流程

5.7 配置管理流程

信创项目配置管理流程是将环境中所有配置项(硬件、软件等)的信息以及配置项之间的关系记录到配置管理库中，从而为其他流程的处理提供详细配置信息。配置管理需要确定配置的范围并制订配置计划，识别本次更新的配置项，并将配置项的详细信息以及配置项之间的关系记录到配置管理库中，并定期对配置管理库进行审验，保证其配置信息被正确地记录下来。

信创项目或组织应建立配置管理流程，记录配置信息，并保证配置信息的可靠性、完整性和时效性，对其他服务过程提供支持。通过配置管理，对信创环境中所有配置项进行版本控制、变更控制、配置控制，提供状态统计和配置审计。配置管理流程见图6。

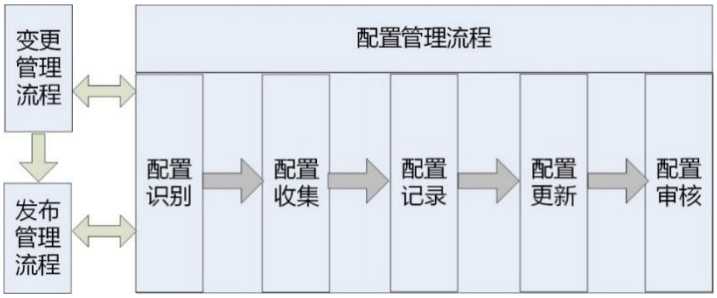

图 6　配置管理流程

6　运维过程监测规范

6.1　软硬件监控要求

6.1.1　信创终端

信创终端监控主要以资源使用情况及终端基础信息监控为主，其核心功能为实现终端的运行情况监控及异常告警规则的关联。使运维人员能实时了解被监控终端的使用情况，并对存在告警的信创终端进行快速运维。具体监控指标详见附录表A.1。信创终端告警（预警）要求如下：

a)　严重告警

当操作系统已挂载的块设备的使用率超出设定阀值时，发出严重告警。告警信息内容包括告警的等级、告警时间、告警的终端（为方便定位具体终端需包含告警终端的唯一标识）及告警事件内容。

b） 一般告警

长期不在线天数，当连续不在线天数超过设定天数时，发出一般告警。告警信息内容包括告警的等级、告警时间、告警的终端（为方便定位具体终端需包含告警终端的唯一标识）及告警事件内容。

c） 预警提示信息

终端持续在一定时间内CPU和内存的使用率都占满设定阀值时，发出提示信息。信息内容包括告警的等级、告警时间、告警的终端（为方便定位具体终端需包含告警终端的唯一标识）及告警事件内容。

6.1.2 信创外设

信创外设包括打印机、扫描仪等，主要以现场部署环境巡检、耗材检查、外设性能及可用性检查为主。及时发现潜在的问题，确保外设在日常使用中能正常运行。具体巡检内容详见附录表A.2。

6.1.3 信创服务器

信创服务器监控主要以资源使用情况、基础信息、服务状态监控为主，其核心功能为实现信创服务器各项运行指标的监控及告警信息的抛出。使管理人员能及时了解到信创服务器的的运行情况，并可通过告警信息准确定位故障或异常点，保障设备的可用性。具体监控指标详见附录表A.3。信创服务器告警（预警）要求如下：

a） 严重告警

当操作系统已挂载的块设备的使用率超出设定阀值时，发出严重告警。告警信息内容包括告警的等级、告警时间、告警的终端（为方便定位具体服务器需包含告警服务器的唯一标识）及告警事件内容。

当服务器状态处于“离线”状态超过一定时间时判断服务器已宕机，发出严重告警。告警信息内容包括告警的等级、告警时间、告警的终端（为方便定位具体服务器需包含告警服务器的唯一标识）及告警事件内容。

b） 一般告警

监控信创服务器操作系统重要文件,通过使用md5sum命令对比文件md5值判断监控的重要文件是否被修改，如当前MD5值与源MD5值不同则作出一般告警信息。告警信息内容包括告警的等级、告警时间、告警的终端（为方便定位具体服务器需包含告警服务器的唯一标识）及告警事件内容。

c） 预警提示信息

监控服务器内存及CPU使用率，当内存或CPU使用率持续在一定的时间内一直保持在设定阀值时，则做出提示信息。信息内容包括告警的等级、告警时间、告警的终端（为方便定位具体服务器需包含告警服务器的唯一标识）及告警事件内容。

6.1.4 信创中间件

通过监控关键性能指标，了解中间件资源使用趋势（例如CPU和内存使用情况），JVM使用情况等。运维人员可密切关注信创中间件的性能，在出现故障时能根据告警信息，快速定位问题的根本原因并修复，确保业务稳定运行。具体监控指标详见附录表A.4。信创中间件告警规则如下：

a） 严重告警

监控JVM堆内存的最大内存大小和已使用的内存大小使用情况,若已使用的内存大小大于最大内存值既判断出现内存泄漏现象，如出现这个现象即做出内存泄漏告警。告警信息内容包括：告警的等级、告警时间、告警的中间件（为方便定位具体服务器需包含告警服务器的唯一标识）及告警事件内容。

b） 一般告警

监控中间件空闲物理内存，当空闲的物理内存达到设定阀值以下影响中间件申请内存大小的情况下则作出一般告警，告警信息内容包括：告警的等级、告警时间、告警的中间件（为方便定位具体服务器需包含告警服务器的唯一标识）及告警事件内容。

c） 提示信息

监控中间件服务器的内存及CPU使用率，当内存或CPU使用率持续在一定时间内超过设定阀值时即发出提示信息。提示信息内容包括：告警的等级、告警的时间、告警的中间件（为方便定位具体中间件需包含告警中间件的唯一标识）及告警事件内容。

6.1.5 信创数据库

信创数据库监控主要以基础信息采集（表空间使用情况、日志大小等）、活动监视（线程、会话等）为主。针对监控指标进行全方位的实时监控，帮助运维人员了解数据库的运行情况和性能，及时发现数据库潜在的问题，确保数据库能稳定运行，防止出现业务中断的情况。具体监控指标详见附录表A.5。信创数据库告警规则如下：

a） 严重告警

监控数据库的网络连通性，当无法访问数据库进行监控时做出离线告警提示。告警信息内容包括告警的等级、告警时间、告警的数据库（为方便定位具体数据库需包含告警数据库的唯一标识）及告警事件内容。

b） 一般告警

监控数据库所有表空间使用率，当监测到有表空间使用率达到设定阀值时做出表空间告警。告警信息内容包括：告警的等级、告警时间、告警的数据库（为方便定位具体数据库需包含告警数据库的唯一标识）及告警事件内容。

c） 提示信息

监控数据库的字典利用率、SQL命中率及SQL回滚数，当字典利用率超出设定阀值，SQL命中率低于设定阀值及SQL回滚数超出设定的运行回滚数量则作出提示信息。提示信息内容包括：告警的等级、告警的时间、告警的数据库（为方便定位具体中间件需包含告警中间件的唯一标识）及告警事件内容。

6.1.6 信创网络设备

监控信创网络设备的资源使用率、网络接口I/O及会话数等，帮助网络管理人员了解每个网络设备的运行状态，端口的IP、MAC、VLAN信息及设备的可用性。网络管理员根据各项指标的监控信息，调整设备的负载等。具体监控指标详见附录表A.6。信创网络设备告警规则如下：

a） 严重告警

实时监控网络设备的网络连通性，当无法与设备通讯时做出严重告警提示。告警信息内容包括告警的等级、告警时间、告警的网络设备（为方便定位具体网络设备需包含告警网络设备的唯一标识）及告警事件内容。

b） 一般告警

当监控网络设备的网络 I/O 超出设定阀值时作出告警提示。告警信息内容包括告警的等级、告警时间、告警的网络设备（为方便定位具体网络设备需包含告警网络设备的唯一标识）及告警事件内容。

c） 提示信息

当监控网络设备的 CPU 及内存占用率超出设定阀值时做出告警提示。告警信息内容包括告警的等级、告警时间、告警的网络设备（为方便定位具体网络设备需包含告警网络设备的唯一标识）及告警事件内容。

6.1.7 信创安全设备

监控信创网络设备的资源使用率、接口I/O及会话数等，帮助网络管理人员了解每个安全设备的运行状态，各网络接口的详细信息及设备的可用性。网络管理员根据各项指标的监控信息，分析设备的运行状态，分析其性能是否达到瓶颈，及时做出相关安全策略的调整。具体监控指标详见附录表A.7。信创安全设备告警规则如下：

a） 严重告警

实时监控安全设备的网络连通性，当无法与设备通讯时做出严重告警提示。告警信息内容包括告警的等级、告警时间、告警的网络设备（为方便定位具体网络设备需包含告警网络设备的唯一标识）及告警事件内容。

b） 一般告警

监控安全设备的网络I/O当超出设定阀值时作出告警提示。告警信息内容包括告警的等级、告警时间、告警的网络设备（为方便定位具体网络设备需包含告警网络设备的唯一标识）及告警事件内容。

c） 提示信息

监控安全设备的CPU及内存占用率，当超出设定阀值时做出告警提示。告警信息内容包括告警的等级、告警时间、告警的网络设备（为方便定位具体网络设备需包含告警网络设备的唯一标识）及告警事件内容。

6.2 故障监测要求

6.2.1 监测通讯要求

6.2.1.1 信创终端监测通讯要求

至少支持TCP/IP协议的方式，同步频率为可配置的。基于TCP/IP协议的通讯流程分为：服务器初始化-LISTEN、建立连接的过程-三次握手（绿色部分）、数据传输的过程（蓝色部分）、断开连接的过程-四次挥手（红色部分），如图7所示：

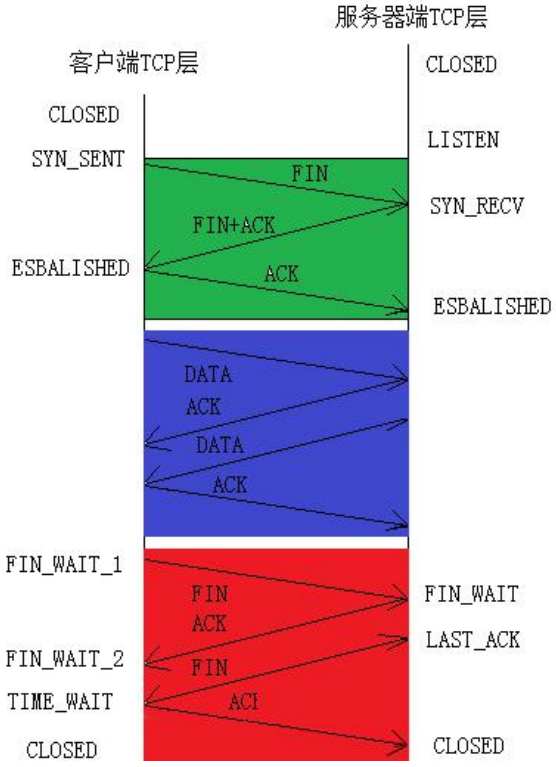

图 7 信创终端通讯流程

6.2.1.2 信创服务器监测通讯要求

至少支持TCP/IP协议的方式，同步频率为可配置的。基于TCP/IP协议的通讯流程分为：服务器初始化-LISTEN、建立连接的过程-三次握手（绿色部分）、数据传输的过程（蓝色部分）、断开连接的过程-四次挥手（红色部分），如图8所示：

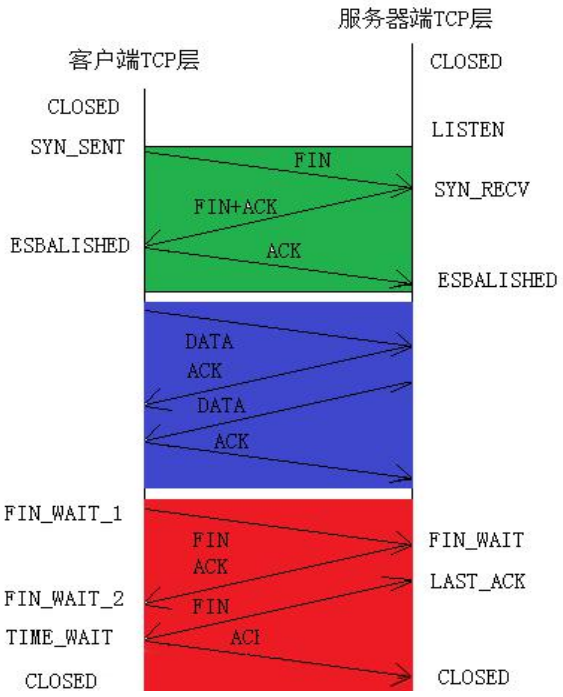

图 8　信创服务器通讯流程

6.2.1.3　信创中间件监测通讯要求

信创中间件监测的至少支持JMX协议的方式进行通讯，同时信创中间件需开启JMX协议及配置相关JMX通讯端口，数据同步频率为可配置的。

6.2.1.4　信创数据库监测通讯要求

信创数据库监控协议应至少支持JDBC协议数据库进行连接，通过数据库的JDBC驱动接口及对应的SQL语句查询数据库性能相关视图数据。为保证数据库的性能，不占用数据库的资源，数据同步频率为可配置的，根据实际资源占用作调整。

6.2.1.5　信创安全设备监测通讯要求

监控信创安全设备（防火墙、入侵防御、入侵检测）需至少支持SNMP协议并在设备上设置对应的团体名及读密码（SNMP协议版本一般使用V2版本，在对安全性要求高的环境下需使用V3版本），数据同步频率应为可配置的。

6.2.1.6　信创网络设备监测通讯要求

监控信创网络设备（交换机、路由器）需至少支持SNMP协议并在设备上设置对应的团体名及读密码（SNMP协议版本一般使用V2版本，在对安全性要求高的环境下需使用V3版本），数据同步频率应为可配置的。

6.2.2　故障告警关联规则分析要求

针对在实际运维过程中，产生大量纷繁复杂的告警数据，需要对这些数据进行一定规划的关联分析，查找在不同类型的设备与设备之间，设备的指标与指标之间的相关性，准确支撑定位信创软硬件设备产生告警的原因，使运维人员快速、有效地排除故障，确保业务系统安全稳定运行。

6.2.2.1　告警数据分析

告警数据分析通过分析多条有联系的告警，将告警时间等信息进行价值分析，对于不具备告警价值的不予显示以此达到降低活动告警的种类和数目，减轻运维人员的工作压力，提高故障精确定位效率，使设备或系统运行更快恢复正常。

6.2.2.2 告警数据处理

在日常运维监控中，设备或系统可能会在同一时间产生同一类型的告警信息，对于这些信息，应进行去重或对同一设备或系统产生的同一类型信息做融合处理，提高告警信息的准确性。基于告警信息的不同时间维度建议采用以下方法处理：

a) 在相同时间间隔出现的关联告警和该告警的统计关系，选择在时间维度上和该告警相似度超过一定比例的所有告警做融合处理，这些告警和该告警有时间上同步的关系。

b) 在该告警出现前一分钟内的所有父告警和该告警的关系，选择在时间维度上和该告警相似度超过一定比例的所有告警做融合处理，这些告警和该告警有时间上先后的关系。

c) 在该告警出现后一分钟内的所有子告警和该告警的关系，选择在时间维度上和该告警相似度超过一定的所有告警做融合处理，这些告警和该告警有时间上先后的关系。

6.2.2.3 告警数据应用

在告警数据经过挖掘、清洗处理等步骤后，获得的是具有价值的告警数据，运维人员可通过关联的规则对告警数据进行判断，符合规则的则通过短信、邮件、IM工具、电话、系统展示等方式进行告警数据的发送及应用。

7 硬件运维服务规范

7.1 调研评估

调研评估是指根据服务内容或业务需求，对信创硬件设备的使用情况、使用环境、维护或管理进行现状调研、分析或评估，提出处理或改进的建议和方案。

7.2 例行操作

按服务级别协议或信创项目运维服务等级提供例行操作服务。分为监督控制、定期检查、日常维护和宣传指引。例行操作服务具体内容见表B.1。

7.2.1 监督控制

采用各类工具和技术，对桌面及外围设备服务对象的动态指标、静态指标、运行状况和发展趋势等进行记录、分析和告警；通过制定流程和制度，控制用户对服务对象的使用行为和使用环境，减少故障或风险的产生。

7.2.2 定期检查

以固定的频率对服务对象进行维护保养和信息记录，包括定期对服务对象的保养、清洁、检测、调试、更换易损/易耗品和设备信息核对、变更等服务活动，以保证信创硬件设备的稳定运行。

7.2.3 日常维护

主动根据服务对象的监控记录、运行条件和运行状况进行检查或趋势分析，发现其脆弱性并消除或改进，以保证服务对象的可用性和可靠性。

7.2.4 宣传指引

制订服务对象的快速恢复指引、操作指引等维护方法指引文件，通过宣传或培训等手段引导需方使用自助服务，以提高故障恢复时效，降低运行维护成本。

7.3 响应支持

根据响应的前提和信创项目运维服务等级的不同，分为事件驱动响应、服务请求响应和应急响应。

7.3.1 事件驱动响应

事件驱动响应是指设备整体或部分性能下降、功能丧失，而触发的将设备在最短时间内恢复到正常状态或可用状态的一系列运行维护活动。事件驱动响应内容包括但不限于：

a）修复硬件故障；
b）修复操作系统或系统软件故障；
c）隔离并恢复感染病毒、木马的固定计算终端；
d）修复应用软件故障；
e）对用户丢失的数据提供数据恢复服务；
f）功能置换服务；
g）恢复性能降级的硬件设备到性能基线水平。

7.3.2 服务请求响应

服务请求响应是指供方响应非故障类服务申告所采取的一系列运行维护活动。服务请求响应内容包括但不限于：

a）设备的采购、领用、借用、归还、报废；
b）硬件设备的软件和硬件安装、升级、迁移；
c）用户帐号的开立、变更和注销；
d）解答用户提出的操作方法咨询或疑问。

7.3.3 应急响应

应急响应是指在信创硬件设备出现大规模故障、触发应急响应阀值的重大事件、重大自然灾害或需方提出要求时，所启动的应急处理运行维护活动。应急响应内容包括但不限于：

a）制定应急响应预案；
b）演练应急响应预案；
c）完善应急响应预案；
d）应急响应需求出现时，执行应急响应预案。

7.4 优化改善

优化改进服务是通过对硬件设备配置和运行情况的监测分析，为适应业务发展变化，提高设备使用效能，主动采取的一系列运行维护活动。优化改进内容包括但不限于：

a）建立服务改进机制；
b）对不符合策略要求的行为进行总结分析；
c）对未达成的服务指标进行调查分析；
d）根据分析结果确定改进措施，制定服务改进计划。

在运行维护过程中，对平台资源进行优化改善时，应根据不同的运行维护对象和系统运行要求，确定适应性改进、增强性改进和预防性改进的具体服务内容。

7.5 评估分析

评估分析是评估和分析业务数据，给出业务数据质量报告或数据运行维护改进建议，保证数据对业务的有效支持。评估分析包括数据质量评估、数据修改影响评估、数据规范评估、业务数据分析和软件变更对数据影响的评估。调研评估的内容包括但不限于：

a）根据硬件设备的运行和管理结果，评估硬件设备的管理与国家、行业、单位、部门相关标准和规范的符合程度，并提出完善方案；

b）根据硬件设备的统计结果，评估硬件设备的利用和成本占用情况，并提出优化方案；

c）根据硬件设备安全检测结果，评估硬件设备的防非法操作、防入侵、防病毒等安全情况，并提出改进方案；

d）根据硬件设备的性能检测结果，评估硬件设备的使用、维修、报废等价值，并提出处理方案。

8 软件运维服务规范

8.1 基础软件

8.1.1 运行服务对象

供方按服务级别协议为操作系统、数据库软件、中间件软件提供例行操作、响应支持、优化改善和调研评估的服务。

8.1.2 调研评估

通过信创基础软件的运行现状进行分析，根据运行维护的需求，提出服务方案。

8.1.3 例行操作

8.1.3.1 监控

在按照服务协议运行维护过程中，对平台资源进行监控时，应根据具体的运行维护对象，确定监控内容和指标。数据库软件监控具体内容见附录表 B.2，中间件软件监控具体内容见附录表 B.3。

注：由于规模和应用不同，本部分不规定各类平台资源的监控指标和采集。

8.1.3.2 预防性检查

在根据服务协议运行维护过程中，对平台资源进行预防性检查时，应根据具体的运行维护对象，确定性能检查内容和脆弱性检查内容。数据库软件预防性检查具体内容见附录表B.4，中间件软件预防性检查具体内容见附录表B.5。

注：由于规模和应用不同，本部分不规定各类平台资源的预防性检查的指标和检查周期。

8.1.3.3 常规作业

在根据服务协议运行维护过程中，对平台资源进行常规作业时，应根据具体的运行维护对象，确定操作内容和周期。

注：由于规模和应用不同，本部分不规定各类平台资源的常规作业的周期。

8.1.4 响应支持

在根据服务协议运行维护过程中，对平台资源进行响应支持时，应根据不同的运行维护对象和系统运行要求，确定事件驱动响应和服务请求响应的具体服务内容。

8.1.4.1 事件驱动响应

事件驱动响应包括操作系统、数据库和中间件三个方面，确定事件驱动响应的具体服务内容如下：

表 2 事件驱动响应

响应事件范围	具体内容
操作系统	a）操作系统崩溃 b）操作系统CPU、内存等资源 c）操作系统服务进程无效 d）操作系统网口无法通讯

	e) 操作系统无法识别外置存储空间
数据库	a)数据库宕机、锁死 b)数据文件坏块修复 c)数据库重启 d)数据库侦听重启 e)数据库备份恢复 f)数据库解锁
中间件	a)程序恢复 b)中间件重启 c)配置文件恢复 d)守护服务调整

8.1.4.2 服务请求响应

服务请求响应包括操作系统、数据库和中间件三个方面，确定服务请求响应的具体服务内容如下：

表 3 服务请求响应

响应请求范围	具体内容
操作系统	a)操作系统版本升级 b)操作系统死机修复 c)操作系统文件系统损坏修复 d)操作系统文件系统空间扩容 e)操作系统IP地址修改 f)操作系统参数调整 g)操作系统日志清理
数据库	a)数据库版本升级 b)数据库灾难恢复 c)数据清理和维护
中间件	a)中间件服务器更换 b)中间件参数调整 c)中间件软件版本升级

8.1.5 优化改善

在根据服务协议运行维护过程中，对平台资源进行优化改善时，应根据不同的运行维护对象和系统运行要求，确定适应性改进、增强性改进和预防性改进的具体服务内容。

8.1.5.1 适应性改进

适应性改进包括操作系统、数据库和中间件三个方面，确定适应性改进的具体服务内容如下：

表 4 适应性改进

改进范围	具体内容
操作系统	a)操作系统交换区容量调整 b)操作系统内核参数调整 c)操作系统文件系统使用空间调整划分
数据库	a)数据库索引调整 b)数据库执行SQL计划调整

	c)数据表参数调整 d)数据库对象的调整 e)主机操作系统内核参数调整 f)数据库参数调整 g)临时表空间、用户表空间调整 h)数据库物理部署的调整（迁移至新服务器或者数据库存储阵列调整） i)调整数据库备份策略
中间件	a)中间件参数配置优化 b)数据库连接参数调整 c)连接池参数调整 d)相关操作系统参数调整

8.1.5.2 增强型改进

根据信息系统及其软硬件环境的运行要求，对平台资源进行必要的调整，包括但不限于：

表 5 增强型改进

改进范围	具体内容
操作系统	a)操作系统版本升级 b)操作系统内存扩容 c)操作系统磁盘空间扩容 d)操作系统增加网卡、光纤卡数量 e)操作系统参数调优
数据库	a)数据库版本升级、打补丁 b)由于主机 CPU 个数、内存容量增加调整数据库相应参数 c)由于主机存储的增加调整数据库表空间容量 d)数据库安全备份架构构建以提高可用性 e)数据库调优等
中间件	a)中间件版本升级、打补丁 b)由于主机 CPU 个数、内存容量增加调整中间件相应的参数

8.1.5.3 预防性改进

预防性改进包括操作系统、数据库和中间件三个方面，确定预防性改进的具体服务内容如下：

表 6 预防性改进

改进范围	具体内容
操作系统	a)操作系统删除垃圾数据，释放数据空间 b)操作系统文件系统扩容 c)操作系统增加网卡、光纤卡冗余 d)操作系统用户权限合理分配 e)操作系统服务端口调整
数据库	a)增加数据库表空间、数据文件空间使用范围; b)对数据库存在的无效对象处理 c)数据库用户的权限合理分配

中间件	a)删除临时文件，释放数据空间 b)监控主要参数以及时调优 c)应用备份策略调整 d)定期备份

8.1.6 评估分析

评估分析是评估和分析业务数据，给出业务数据质量报告或数据运行维护改进建议，保证数据对业务的有效支持。评估分析包括数据质量评估、数据修改影响评估、数据规范评估、业务数据分析和软件变更对数据影响的评估。应满足下列要求但不限于：

a） 数据质量评估，包括基础数据质量评估、辅助数据质量评估和业务数据的影响分析；

b） 数据修改影响评估，包括业务参数修改的景影响评估、数据字典修改的景响评估。基础数据修改的影响评估和业务数据修改的影响评估；

c） 数据规范评估，包括基础数据共同遵守规则和命名的评估、业务场景对应业务类型数据的规则评估和业务关键数据应遵循的规则评估；

d） 业务数据分析，包括面向业务重点支撑运营和战略需求的数据分析和面向预测重点支撑业态发展趋势的数据分析；

e） 软件变更对数据影响的评估，包括业务扩展、功能扩展等应用软件变更引起对数据完整性、一致性的评估，以及软件升级、变更、迁移等对数据完整性、一致性的评估。

8.2 应用软件

8.2.1 服务对象

信创项目运维组织按服务级别协议为信创项目应用软件及其运行环境提供调研评估、例行操作、响应支持、优化改善和变更发布的服务。

8.2.2 调研评估

调研评估即对应用软件及其运行环境的调查研究和分析评价，形成信创项目业务系统的运行报告或建议。调研评估包括信创项目业务系统组成要素的构成分解、关联关系分析和业务系统的维护性分析。应用软件调研评估要求具体内容见附录表B.6。

8.2.3 例行操作

例行操作即对应用软件及其运行环境的预定运行维护，以保障信创项目业务系统的正常运行。例行操作包括业务系统运行的监控指标体系设计、业务系统运行的监控、客户回访、问题分析。应用软件例行操作具体内容见附录表B.7。

8.2.4 响应支持

响应支持即对信创项目业务系统应用软件及其运行环境的服务请求或故障申报提供即时运行维护，以保障应用系统的正常运行。响应支持包括服务受理、非故障请求处理、故障诊断定位、解决方案制定、故障处理、新用户和新功能上线、应急响应。应用软件响应支持要求具体内容见附录表B.8。

8.2.5 优化改善

优化改善即对信创项目业务系统的功能和性能进行调优，并满足新的需求。优化改善包括功能性改进、性能优化改进、适应性改进、预防性改进。应用软件优化改善要求具体内容见附录表B.9。

8.2.6 变更发布

管理、控制变更的过程，通过变更有序实施，确保变更的成功导入。变更发布包括变更请求响应、变更评估、变更开发、制定发布计划、制作发布包、并实施发布，配置信息更新，应用系统性能监控和回顾总结。应用软件变更发布要求具体内容见附录表B.10。

8.3 数据资源

8.3.1 服务对象

信创项目运维组织按服务级别协议为信创项目应用软件系统数据提供例行操作、响应支持、优化改善和评估分析的服务。

8.3.2 调研评估

通过对应用软件运行相关的系统数据进行调查研究和分析评价，根据运行维护的需求，制定系统数据监控、检查、问题处理、优化完善等方面的服务方案。

8.3.3 例行操作

例行操作即预定运行维护，确保数据的可用、准确、完整、安全。例行操作包括数据监控、预防性检查、常规检查。数据资源例行操作要求具体内容见附录表B.11。

8.3.4 响应支持

响应支持提供即时运行维护，以确保数据的可用性、准确性、完整性。响应支持包括数据问题处理、服务请求处理和应急响应。数据资源响应支持要求具体内容见附录表B.12。

8.3.5 优化改善

优化改善即改善数据质量，满足业务需求。优化改善包括诊断分析、解决和改进。数据资源优化改善要求具体内容见附录表B.13。

8.3.6 评估分析

评估分析是评估和分析业务数据，给出业务数据质量报告或数据运行维护改进建议，保证数据对业务的有效支持。评估分析包括数据质量评估、数据修改影响评估、数据规范评估、业务数据分析和应用软件变更对数据影响的评估。数据资源评估分析要求具体内容见附录表B.14。

9 运维综合保障平台

9.1 概述

运维综合保障平台是运维支撑管理工具软件，用于实现运维的信息化、加强运维过程管控及事后分析。平台需涵盖信创项目实施管理、网络资源监控管理、运行维护管理、运维知识管理等内容。

9.2 项目实施管理

运维综合保障平台中存在多个运行项目，平台需求满足从信创项目的实施过程到运维过程和无缝衔接，同时满足对项目实施过程的管控。解决在信创项目中参与单位众多造成的重复投资、成本浪费，孤岛效应造成信息闭塞、效能低下等问题。

项目实施管理需满足：

a）实现项目建设过程深度管理及多方协同，降低参建各方重复工作量，提升项目管理效能；

b）实现现场执行人员灵活调度，提高人员利用率，并加强现场费用管理，有效降低现场成本；

c）利用远程监管、质控监督技术，有效提升项目管控的质量，提高业主满意度；

d）利用系统平台进行数据分析、统计及挖掘，为企业决策提供专业的分析依据。

9.3 网络资源监控管理

平台需实现对资产设备运行的实施监控，如发现异常自动告警，生成工单通知运维人员处理。

a）资产设备监控

对于监控的PC终端和服务器，系统监控CPU信息、内存信息、磁盘信息和系统信息。

b）应用监控

平台需支持监控生产应用的存活状态，被监控应用需提供状态信息获取的api接口。

c）数据库监控

平台需支持监控数据库运行的基本信息和存活情况等，被监控的数据库平台需提供可登陆对接的配置信息。

d）运维脚本编排及下发

- 平台可提供自动化运维套件，支持运维脚本的存储、在线编辑、多工具编排组合、批量一键下发等；
- 平台可预设工具，如自动化软件部署工具、补丁安装工具、等保安全加固工具、批量配置/密码更新工具、故障自愈处理工具、客户自定义批量执行工具、自动化巡检工具。

e）告警信息统一呈现

平台在告警展示页面展示实时告警和历史告警信息，用户可以按设备类型、告警时间、告警等级、安全域等维度组合查询告警信息。

平台可根据预设的采集时间规则，针对出现告警的资产及相关资产，从数据库读取并整合资产历史状态信息和实时状态信息。

9.4 运行维护管理

运维综合保障平台需实现各运维参与角色及运维流程的管控，需包含事件管理、问题管理、巡检管理、资产管理、日志管理、信息安全管理等模块。

a）事件管理

平台需建立服务请求和计划外服务中断的故障的处置过程，确保具有及时解决事件的能力，支持事件的通知、响应、处置、跟踪，实现事件闭环管控，需满足：建立与事件管理流程相一致的活动，包括事件识别、报告、受理、调查和诊断、解决、进展监控与跟踪、关闭等；建立事件分级、分类及升级机制；定期统计分析事件数据与执行情况，建立事件评估及改进机制；将未知、无法解决和共性的事件与问题管理建立必要的关联。

b）问题管理

平台需建立问题管理过程，分析问题根本原因和确定解决方案，为了消除引起事件的深层次根源，防止类似的事件频繁发生，至少应包括：建立与问题管理流程相一致的活动，包括问题识别、分类、调查和诊断、解决、关闭等；建立问题分类、分级机制，包括问题的影响范围、重要程度、紧急程度并确定优先级；应识别已知错误，在没有彻底解决前，组织应采取措施以减轻或消除问题对服务的影响；建立问题解决评估机制。

c）巡检管理

巡检是运维中经常发生的工作，平台需满足：支持对巡检配置、巡检对象、巡检模板进行管理；需实现灵活的巡检计划配置，可对资产设备、操作系统、数据库等IT运维对象的运行状态、配置、安全、性能情况进行全方位巡检；生成直观的巡检报告，配合趋势报告展示巡检对象变化情况，辅助IT运维人员及管理人员掌握IT系统总体状况及存在的风险，及时优化调整。

d）设备管理

平台需支持各类IT设备的全生命周期集中管理，优化设备的利用并保证资产的合规性，保证设备信息的准确性，平台需实现：设备与配置项的建立、调整、变动、清理过程的管理，通过工作流程严格控制了设备与配置项的生命周期过程，从而保证设备与配置项的有效性；设备与配置项基本信息的

维护，对关键信息字段进行受控管理，系统记录完整的信息变更日志；管理配置项之间的关联关系，支持配置库的管理；提供设备与配置项的变动审批过程，确保设备与配置项的管理可控、可查。

e）服务水平协议

服务水平协议（SLA）是用于约定不同级别故障的响应及处理时效要求，需包含：可以定义和实施服务种类及服务目标；可以监控SLA达成状况；对延迟、逾期等不同状态事件进行预警；事件处理过程与SLA标准直接挂钩。

f）信息安全管理

平台需确保运行维护服务过程中涉及的信息安全的保密性、可用性、完整性，需包括：建立符合相关法律法规的信息安全管理制度，满足需方对运行维护服务过程的信息安全需求和供方本身信息安全需求，包括信息安全方针、目标和安全策略；建立与信息安全管理过程一致的活动，包括计划、识别、评估、处置和改进等，并保留相关记录。

g）发布管理

平台需实现发布管理过程，控制部署实施活动，确保一个或多个变更的成功导入，发布管理过程与变更管理流程、配置管理流程一起计划、监视、确保软件和相关硬件成功、安全的导入到生产环境，提供IT服务的可用性，应包括：建立与发布管理过程一致的活动，包括规划、测试、部署和验证等；建立发布类型、范围及相配套的管理机制；制定合适的发布方案，包括发布计划、测试方案、回退方案等；记录部署活动中的主要动作、结果和相关信息；对发布完成情况进行统计分析，包括发布成功率、发布及时率、是否更新配置管理数据库等。

h）运维报表

平台需提供运维数据统计分析报表来辅助运维人员及管理人员的工作，包括设备运行状态报表、运维服务质量监控及评估报表、服务体系运行状况报表等，为运维管理人员等参与方提供全面的运维分析支撑。

i）日志管理

平台需提供足够的运行日志，用于安全审计及平台故障分析。确保日志采集的高效性，需实现：监控平台运行能力，日志关键字监控告警和日志字段的汇聚统计监控告警；提供快速查询、实时日志、日志上下文查询等功能；提供日志文件批量下载及日志文件权限管理功能。

9.5 知识库管理

知识库管理需实现整个管理流程的管控，涉及到的管理流程包括：知识收集管理、知识分类管理、知识评审管理、知识发布管理、知识访问管理。

a）知识收集管理

知识库的知识收集应根据实际需求进行分析，确定知识的收集类型后进行收集工作。对于收集渠道可分为内部收集及外部收集，进行知识收集时要确保其合法性、安全性、可用性，使整个知识收集流程安全、顺利的进行。

b）知识评审管理

知识评审人员针对收集的知识进行评审，需要对其的正确性、可用性、严谨性、进行验证和审核，确保知识的准确，可用和有效。对于不可用的知识进行否决，对于不准确的知识给出修改建议，待完成修改后重新进行知识评审。

c）知识发布管理

知识提交后，经评审人员进行评审后进行发布，将知识纳入对应的分类目录，记录知识的提交人、评审人、发布时间以及知识的适用范围等信息。供各人员角色在知识库中查阅使用。

d）知识维护管理

知识库管理人员应根据技术更新、产品迭代、行业动态、业务实际情况等定期对知识进行维护，判断知识是否需要更新、删除。知识库各用户角色均可对知识提出意见和建议，以便进一步完善知识体系。

9.5.1 经验范围

经验知识按照技术服务对象的不同进行分类，大致可分为终端设备、外设设备、服务器设备、中间件、数据库、操作系统、网络设备、存储设备及应用系统。

a）终端设备

终端设备的经验范围涉及安装部署：终端部署的流程、数据备份方案、部署注意事项；安全配置：操作系统安全漏洞修补、高危端口封堵；日常运维：软硬件的故障定位及修复、常用运维命令及工具。

b）外设设备

外设设备的经验范围涉及安装部署：外设设备部署流程、安装部署注意事项；日常运维：外设设备耗材更换方法、故障定位修复、日常巡检项目。

c）服务器设备

服务器设备的经验范围涉及安装部署：服务器上架规范、操作系统网络及运行环境配置；安全配置：操作系统安全漏洞修补、高危端口封堵；日常运维：软硬件的故障定位及修复、常用运维命令及工具。

d）中间件

中间件的经验范围涉及安装部署：安装路径规划、安装指引、安装过程问题处理、安装环境搭建、安装注意事项；性能调优：内存分配优化、并发数优化、操作系统调节；安全配置：三员账号管理、高危端口关闭、漏洞修补；日常维护：性能监控方法、业务负载能力分析、日志分析方法。

e）数据库

数据库的经验范围涉及安装部署：安装目录账户及目录规划、安装环境搭建、安装操作步骤、安装注意事项；性能调优：SQL 语句优化、表结构设计、操作系统调节、内存分配；安全配置：三员账号管理、通讯加解密、访问控制；日常维护：数据备份方法、表空间占用情况分析方法、日志分析方法。

f）操作系统

操作系统的经验范围涉及安装部署：操作系统安装方法、安装过程问题处理方法、安装注意事项；安全配置：高危端口关闭；漏洞扫描及修复方法；日常运维：故障的定位及修复；常见问题处理方法；常用命令详解。

g）网络设备

网络设备的经验范围涉及日常巡检项目：端口状态，网络流量分析、性能瓶颈分析；安全配置项：三员账号管理、VLAN 划分、ACL 访问控制规划、高危端口禁用；管理方法：划分管理专用网段、使用安全工具进行管理访问。

h）存储设备

存储设备的经验范围涉及日常巡检项目：告警指示灯状态、硬盘健康度、容量使用情况分析；存储配置：存储 LUN 规划方法、容量配置标准；安全配置项：三员账号管理、高危端口禁用；维护操作指引：存储容量扩容、回收、重分配。

i）应用系统

应用系统的经验范围涉及应用部署：运行环境搭建、应用部署指引、应用部署注意事项；性能调优：业务逻辑优化、数据库及中间件联合调优、安全配置：三员账户管理、漏洞修补、通讯加解密；日常维护：操作指引、应用系统故障定位及修复。

9.5.2 信创运维知识库要求

信创运维知识库作为运维服务的核心支撑内容，其建设内容建议具备以下要求：

a）知识分类

拥有完善的分类层级和条目，使知识能有序地进行归口管理。知识的分类应遵循“相互独立，完全穷尽”的原则，也就是对于一个知识类型，能够做到不重叠、不遗漏的分类，建议分类包括：运维知识、政策知识、标准规范、业务知识等。其中运维知识的组成可分为：

- 针对于问题产生原因，做出的分析，以及解决问题时所使用的方法或策略、工具等信息；
- 针对日常巡检过程中，发现的问题或者隐患，经过分析，可能在未来带来问题，这类问题的处理方式及应对策略所形成的解决方案；
- 在日常运维过程中，遇到的问题进行处理时，对问题进行分析，得出问题的产生原因和可行的解决方案；
- 日常工作中搜集到有利于运维工作的知识及工具。

b）知识数据分析与统计

设置知识统计分析功能，实现包括对知识阅读量、贡献量、知识错误率、知识纠错量、知识错误及时更正时间、知识上传审核时间、知识下载量、用户在线时长的信息进行自动统计。

c）知识分享

可对知识进行内部及外部共享，以知识推送等方式进行知识的内部分享，以生成分享链接等方式进行知识外部分享，实现根据不同的分享对象进行知识分享的控制。

d）知识应用

可根据对已入库的知识内容进行深入挖掘，结合日常运维及业务场景使知识能真正的运用起来，让知识产生最大的价值。通过对知识的挖掘，形成运维脚本等技术工具。

9.5.3 经验知识分享规范

9.5.3.1 经验知识分类规范

基于知识本身的复杂性，建立科学的知识体系，才能保证知识库能够高效的利用起来。所以需对知识的入库进行分类，具体如下：

a）运维知识

按运维对象（终端设备、外设设备、服务器设备、中间件、数据库、操作系统、网络设备、存储设备及应用系统）进行知识的分类归集，提供相关对象的运维问题、方法、产品及工具的知识经验分享。

b）政策知识

收集并汇总信创行业的政策知识，提供相关政策的解读知识分享。

c）标准规范

收集并汇总信创项目建设的相关标准规范，包括通用标准及团体标准等。

d）业务知识

信创项目中运维、管理等业务流程及注意事项的经验分享。

9.5.3.2 经验知识入库规范

知识的来源主要分为内部知识和外部知识，内部知识为主，外部知识为辅。

a）内部知识：

主要是在知识原料或经验的基础上，根据需求做知识分析及推理总结出来的具有典型意义的知识并已形成文档的，可以作为对技术员学习的参考依据或直接利用的经验。

b）外部知识：

从外部知识里捕获到对运维工作和未来工作实施有用的知识，进行集成以利用传播。对采集的外部知识经过过滤、归类、评价，存优去劣后才能存入知识库。

9.5.3.3 知识库访问规范

知识库的内容理论上是对全员开放的，但为保障知识库的有效使用及安全性，不同的人员角色要进行访问权限的控制。没有相关知识阅历权限的角色不具备访问对应的知识，具体访问流程规范如下：

a）建立基于访问者角色权限的账户，访问者根据开通账号的权限，访问知识库进行查阅、新增等操作；

b）访问知识库后拥有对应权限的可查看已上传的知识点，可访问对应知识的“附件”等进行在线浏览学习或者下载保存。

10 运维组织及人员

10.1 运维组织架构

信创运维组织架构由现场运维人员、远程技术支撑人员、运维专家团队组成。

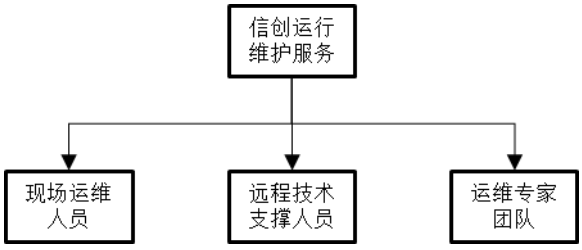

图 9 项目运维组织架构

在运维过程中，针对信创项目运维要求不同时，可根据实际能力需求，选择不同能力等级的运维服务人员担任。

现场运维人员负责故障请求判断处理以及日常运维巡检和保养等现场支撑服务工作；远程技术支撑人员负责对现场运维人员上报的故障进一步分析，根据信创相关经验和专业技能进行远程技术支持，提出解决方案协助现场运维人员完成工作；运维专家团队是信创领域的技术专家或原厂商技术支持专家，负责提供包括服务器、操作系统、数据库、中间件、业务系统等方面专家会诊，协助现场运维人员或远程基础支撑人员解决复杂技术问题。

10.2 人员能力要求

10.2.1 定义

信创运维人员具备信创信息系统和软件产品的版本控制能力，熟悉基础软件产品的使用方法，能够开展信创项目运行维护质量管理和运行维护系统管理工作。能够结合信创项目服务场景对运行维护服务能力进行整体策划并提供必要的支持，形成运行维护服务能力计划，确保运行维护服务工作顺利进行的专业人员。

10.2.2 人员能力等级

根据信创项目的具体实施和对运行维护的规范化要求，将信创项目运维人员能力划分为高级、中级、初级三个等级，信创项目运行维护人员能力等级见表7。

表 7　信创项目运行维护人员能力等级

能力维度	能力需求	能力描述	评价等级		
			初级	中级	高级
知识	按照信创运维标准规范进行运维工作	掌握计算机相关基础知识，熟悉信创运维相关法律法规和标准规范。	至少 6 项达到要求	至少8项达到要求	至少12项达到要求
	能独立对信创涉及机房和基础网络设备维护	掌握机房和网络设备基础知识及常见通讯协议。			
	能独立规范使用信创运维工具	掌握信创规范运维流程及信创相关运维工具使用。			
	能依据保密安全要求开展信创运维工作	掌握保密安全相关法律法规内容，了解信创项目保密相关规定。			
	搭建信创技术架构和运行环境	掌握国产信创 CPU 技术路线架构知识，掌握信创操作系统、终端的兼容性及功能性，熟悉信创软硬件适配过程			
	能独立完成信创相关设备性能排查和维护	掌握计算机系统以及各主要设备的性能，并了解其工作原理，具排错知识，可带领团队有效完成工作，确保系统运行。			
	能独立完成LINUX操作系统排错	掌握 LINUX 操作系统知识及原理，能够带领团队高效完成相关配置和排错任务。			
	能独立完成信创数据库系统故障调试	掌握数据库基本原理，熟悉常用信创数据库管理系统的安装、配置、优化和维护、故障调试诊断相关知识。			
	能独立完成局域网日常维护	掌握计算机网络的基本原理，精通 TCP / IP，LAN，WAN 等相关理论知识，熟悉局域网的布线及日常维护，能够带领团队完成重要事件支。			
	能独立使用网络安全产品及排错	掌握信息安全原理，掌握网络安全产品和密码产品的配置和使用相关知识，具高效排错和修复能力。			
	能完成信创机房各运行系统维护	掌握机房安全设施、空调系统和电力系统原理，可带领团队有效完成工作。			
	能独立完成信创基础软件适配	掌握各大技术路线 CPU 架构与工作原理；熟悉信创操作系统、数据库、中间件的适配过程与适配方法。			
技能	能独立完成信创基础系统及设	熟练对计算机，服务器，办公设备，操作系统，数据库，办公软件的运	至少8项达到要求	至少12项达到要	至少15项达到要

	备运维	维过程；		求	求
	能独立完成信创系统运维的保密安全防护工作	熟练掌握保密防护软件的功能，掌握身份鉴别措施，信息数据访问控制措施，有效开展系统保密防护			
	能独立完成网络设备及产品运维	熟练网络基础设备，主流网络产品，局域网，广域网，网络技术的运维			
	能独立完成脚本编写	熟悉简单 Shell 脚本编写；			
	能独立使用和维护网络安全产品	熟悉网络安全和密码安全产品的使用、配置和维护方法			
	能独立完成运维过程记录	熟知各类常用的运维文档编制			
	能独立完成信创运维需求分析	需求分析能力，可通过收集、分析、导出的方法，将用户、业务的需求转换为对应的运维操作需求			
	能独立完成信创操作系统安装及维护	操作系统维护能力，可独立完成操作系统的安装、配置和漏洞修复，能够熟悉使用操作系统常用功能；可以定位诊断操作系统故障			
	能独立完成信创系统数据库维护	数据库维护能力，可根据维护流程完成数据库日常基本维护工作，熟悉 SQL 语句使用，根据日志处理数据库简单故障			
	能独立完成网络设备调试及维护	网络维护能力，可独立完成网络设备的安装、配置调试，对网络故障进行定位诊断			
	能对完成信创安全事件处理	信息安全维护能力，能够根据安全事件进行处理响应，发现安全事件原因，协助处理			
	能独立完成应用部署维护	应用部署与维护能力：能够对线上应用进行配置、部署、监控和优化，并能够撰写相关脚本提高部署、配置效率			
	能独立使用常用信创运维工具	运维工具使用能力：能够使用监控类、分析类运维工具，主动发现问题并处理			
	能处理信创突发运维事件	突发运维事件处理能力：能够处理突发运维事件，进行问题跟踪与反馈，攥写运维报告			
	能完成信创机房设施日常维护使用	机房维护能力，可完成安全设施、空调系统和电力系统的使用和维护工作。熟悉操作机房动环境系统并对机房进行监控运维			
	能独立完成信创系统兼容性测	熟悉信创外设或应用与操作系统、数据库、中间件的兼容性适配测试			

	试				
	确保完成与信创运维团队日常沟通	沟通能力，清楚地传达和接受信息来满足所有的需求，包含倾听、解释说明、系统阐述和评论			
	能独立学习信创运维新知识	学习能力，以最快的速度、在最短的时间内把学习的新知识和获得的新信息应用在工作中，并将知识进行总结沉淀			
	指导信创运维团队完成运维工作	指导能力：能够根据运维现状、优化运维过程，指导团队成员，协同完成工作			
工程实践经验	能独立完成信创事件分析及处理	具备独立处理与分析运维事件的能力	具备一定的计算机软硬件、机房的基础知识； 具备计算机类或计算机类、电气类、电子信息类、 自动化类相关专业大学科学位，连续从事本岗位工作 1 年以上；	具备独立处理与分析运维事件的能力； 具备计算机类或计算机类、电气类、电子信息类、自动化类相关专业大学科学位,连续从事本岗位工作3年以上； 具备一定的项目实施经验。	具备指导团队处理运维事件的能力； 具备计算机类或计算机类、 电气类、 电子信息类、自动化类相关专业大学科学位，连续从事本岗位工作 5 年以上； 具备项目实施经验，带领带领团队完成计算机设备、操作系统、数据库、信息安全、机房等一种或几种领域的运维

10.3 组织服务评价

根据运维服务响应支持、运维服务质量、运应急事件处理、安全保密措施等方面情况，对信创运维组织的服务进行综合评价，满分为 100 分，整体分为优秀、良好、一般三个等级，其中 85-100 分为优秀，70-85 分为良好，60-75 分为一般。

表 8 组织服务评价表

评价指标	指标说明
运维服务响应（10分）	服务热线来电准时接听，记录反馈问题，并按照故障类型在规定时间，安排对应运维人员进行响应（5分）
	快速响应，按照规定和故障类型进行现场及远程支撑运维，遇到无法解决故障及时上报处理，并协调信创软硬件厂家快速技术支撑（5分）
运维服务质量（25分）	运维工作按照制定方案进度有序完成，运维过程、结果文档化，并根据要求提交按时提（5分）
	根据运维服务要求，制定例行维护服务计划，定期对系统软硬件巡检并形成故障事件管理日志（5分）
	配合用户进行备件安装替换，系统软硬件升级，软件版本及时更新维护，以改进完善现有系统运维状况（5分）
	运维人员服务过程保持沟通，及时反馈和更新进度，必要时申请专家或信创原厂商技术支撑及培训（5分）
	运维故障处理按照故障分类处理，针对问题进行经验总结，优化运维过程，提高效率，保障信创软硬件设备的稳定性，减少对系统业务的影响，故障的重复处理率低（5分）
应急事件处理（15分）	与相关的业务部门、信创厂家密切配合，共同开展应急事件响应工作，严格按照相应的规章制度进行应急事件处理（5分）
	根据制定应急事件处理预案，对运维人员进行定期演练与预案修订（5分）
	应急事件处理完成后，对事件进行总结，分析原因并形成书面事件分析报告（5分）
运维服务管理（30分）	日常按时进行运维工作，不迟到早退，严格遵守现场办公秩序及信创保密安全管理（5分）
	运维服务团队内部建立相应管理制度、工作协助流程、定期的例会、定期提交工作报告（5分）
	运维服务团队人员稳定，人员能力符合要求。（5分）
	运维过程能够形成维护手册、用户FAQ、故障FAQ、故障处理报告和用户操作手册等，并建立知识库。（5分）
	定期进行运维人员培训，包括技能培训、保密培训、制度培训等，能够及时掌握信创软硬件最新的技术动态。（5分）
	根据信创技术的发展，及时掌握信创软硬件版本更新信息，对运维的信创软硬件进行适配更新，并对适配过程进行优化或适配建议。（5分
运维安全管理（20分）	运维人员具备保密安全岗位资格，同时定期进行保密培训教育，签订保密协议（5分）
	运维人员不得未经授权利用服务器或办公终端（计算机）访问互联网（5分）
	定期进行系统安全漏洞扫描，发现系统安全隐患、漏洞和风险，及时进行安全加固（如进行补丁升级等）（5分）
	运维人员严格遵守数据安全规定，禁止将生产环境数据、敏感数据拷贝到本地磁盘或向外发布（5分）

附 录 A

（规范性附录）
软硬件过程监测指标

A.1 信创终端监控指标见表A.1

表 A.1 信创终端监控指标

设备类型	监控信息	描述	信息项
信创终端	注册信息	监控客户端注册时录入或生成的信息。	终端类型、终端码、信创终端使用信息、责任人等。
	终端信息	终端信息为被监控信创终端的软硬件信息，其信息内容为可被采集的。	终端状态、内存总大小、硬盘总大小、CPU 信息（包括核心数）、监控客户端的版本信息、固件信息、操作系统信息（包括操作系统版本信息及操作系统内核信息）。
	CPU使用率监控	取值范围为瞬时值，不单独获取每个核心的使用率，直接获取总的使用率。	各 CPU 核心使用率的总和。
	磁盘使用率监控	对操作系统已挂载的硬盘使用率进行监控。	硬盘块设备使用率。
	内存使用率监控	取值范围为瞬时值，数据获取物理内存的使用率；	物理内存使用率。
	使用时长监控	使用时长根据信创终端成功注册被监控后开始计算，数据展示建议分时段显示。	成功监控后所计算得出的时长。

A.2 信创外设监控指标见表 A.2

表 A.2 信创外设监控指标

设备类型	监测信息	描述	信息项
打印机	运行环境	以人工巡检的方式，检查打印机运行的环境，确认打印机是否运行在一个干燥无潮湿的环境。	环境温湿度
	运行状态	以人工巡检的方式，对打印机的运行状态进行检查，检查内容包括打印机的运行指示灯、有无卡纸现象、有无漏粉或漏墨现象。	指示灯状态、滚轮状态、耗材容器
	设备耗材	以人工巡检的方式，对打印机的耗材消耗情况进行检查，检查内容包括碳粉或墨水是否充足、硒鼓或墨盒喷头寿命是否达到。	碳粉、墨水、硒鼓、墨盒喷头
扫描仪	运行环境	以人工巡检的方式，检查打印机运行的环境，确认扫描仪是否运行在一个干燥无潮湿的环境。	环境温湿度
	扫描仪的协调性	以人工检验的方式检验扫描仪在正常工作时发出的声音是否有节奏，扫描仪的传送速度是否匀速。	滚轮状态
	黑白扫描效果	以人工检验的方式检验扫描仪黑白扫描效果，使用一张有清晰黑色字迹的白纸作为扫描稿，放到扫描仪平面玻璃中扫描，扫描结果应为除字迹外没有其它任何痕迹。	/

	彩色扫描效果	以人工检验的方式检验扫描仪彩色扫描效果，使用一张色彩丰富的照片或色卡作为扫描稿，放到扫描仪平面玻璃中扫描，扫描结果与扫描稿对比色彩饱满无明显偏色现象。	/

A.3 信创服务器监控指标见表 A.3

表 A.3 信创服务器监控指标

设备类型	监测信息	描述	信息项
服务器	注册信息	监控客户端注册时录入或生成的信息	服务器类型、服务器ID、信创服务器使用信息、信创服务器名称、部署位置、责任人
	服务器信息	服务器为被监控信创服务器的软硬件信息，其信息内容为可被采集的。	服务器状态、IP 地址、MAC 地址、CPU 信息、内存总大小、硬盘总大小、固件信息、操作系统信息（操作系统版本信息及操作系统内核信息）
	CPU 使用率	采集 CPU 使用率（单位：%），取值范围为瞬时值，此项数据不需要单独采集每个核心的使用率，直接取总的 CPU 使用率即可。	各 CPU 核心使用率的总和
	磁盘使用率	采集硬盘使用率（单位：%）	硬盘块设备使用率
	磁盘 I/O	采集磁盘总 I/O 信息（单位：KB/s）	读取字节数、写入字节数
	内存使用量	采集内存使用量（单位：%），取值范围为瞬时值，数据取物理内存使用率，不采集虚拟内存使用率。	物理内存使用率
	网络 I/O	采集网络 I/O 信息（单位：Mbps），多网卡启用情况下取总网络 I/O。	上行带宽、下行带宽
	系统进程	采集 CPU 和内存占用最高的进程（建议为前五项），数据更新频率为可配置的	进程名称、进程 ID、CPU 使用率、内存使用率、所属用户、进程数、I/O 读取（字节）、I/O 写入（字节）。
	服务器运行时长	服务器使用时长的统计可分为服务器从通电后正常运行的时间或从服务器被正常监控后通过计算后的时间，建议直接采集服务器通电的后正常运行的时间。	设备通电运行时间、设备被监控后运行时长。

A.4 信创中间件监控指标见表 A.4

表 A.4 信创中间件监控指标

设备类型	监测信息	描述	信息项
信创中间件	基础信息	获取中间件基础信息	当前状态（在线/离线）、中间件IP、产品名称、监控协议、操作系统内核、处理器数量及操作系统版本。
	实时并发数	监测中间件的实时并发数	JVM活动线程数、进程线程、非守护进程线程。
	健康度	中间件健康度数值正常状态为 100%，当内存或 CPU 使用率达到在一定时间内持续超出设定阀值（建议时间阀值为 30 分钟）时中间件健康的减少一定的百分比，若内存和 CPU 使用率同时	CPU使用率、内存使用率、内存是否泄漏。

		达到设定阀值即健康度减少两个监控项的百分比；当出现内存泄漏现象时，中间件健康度也要相应减少，但此现象会比性能问题严重（会导致应用或系统崩溃），所以减少的百分比值需大于 CPU 和内存占比的和。	
	JVM 内存信息	监视堆内存及非堆内存使用量，取已申请大小、最大值、已使用大小及最初申请大小为数据值。	堆内存、非堆内存
	JVM 共享资源	获取 JVM 的空闲物理内存、总交换空间、总物理内存、提交的虚拟内存及空闲交换空间。	物理内存、交换空间、虚拟内存、虚拟交换空间
	JVM 类加载	获取中间件 JVM 类的加载信息。	当前加载类、总加载类、卸载类
	线程池	获取中间件线程池的使用情况	总线程、活动收获线程、高峰线程及活动线程。
	垃圾回收器	获取中间件垃圾回收器状态	PS MarkSweep、PS Scavenge
	代码缓存区	获取代码缓存区中堆内存的使用情况	已使用大小、最大使用大小、初始化大小、可使用大小。

A.5　信创数据库监控指标见表 A.5

表 A.5　信创数据库监控指标

设备类型	监测信息	描述	信息项
信创数据库	基础信息	获取数据基础运行信息，相关数据获取可通过数据库SQL语句查询。	数据库名称、实例名、驱动版本、当前状态（在线/离线）、端口
	线程数	获取数据库当前的线程总数，使用动态数据+时间轴展示，时间轴定义建议为 12 个小时，相关数据获取可通过数据库 SQL 语句查询。	线程池线程总数
	会话数监控	获取数据库当前的会话总数，使用动态数据+时间轴展示，时间轴定义建议为12个小时，相关数据获取可通过数据库SQL语句查询。	会话总数
	字典利用率	获取数据库字典缓存使用率，使用率由缓存池总空间（字节）与实际使用的空间（字节）计算得出，相关数据获取可通过数据库SQL语句查询。	字典缓存使用率
	SQL缓存	获取数据库 SQL 缓存总数，相关数据获取可通过数据库 SQL 语句查询。	SQL缓存总数
	表空间使用率监控	获取数据库各表空间使用率，支持对新建的表空间进行监视，相关数据获取可通过数据库 SQL 语句查询。	表空间使用率
	数据缓冲区命中率	监控数据库缓冲区命中率，相关数据获取可通过数据库 SQL 语句查询。	数据库缓冲区命中率
	SQL 回滚数	监控数据库事务回滚率，相关数据获取可通过数据库 SQL 语句查询。	数据库事务回滚率
	日志大小	监控数据库的日志大小，日志包括运行日志、归档日志、事件日志、错误日志等，相关数据获取可通过数据库 SQL 语句查询。	数据库日志大小

A.6　信创网络设备监控指标见表 A.6

表 A.6　信创网络设备监控指标

设备类型	监测信息	描述	信息项
信创网络设备	基本信息	获取网络设备的基本信息	产品型号、设备名称、IP地址、MAC地址、监控协议、系统软件版本、序列号
	CPU占用率	获取设备的 CPU 占用率，其数据在获取后写入数据库，为监控展示作数据支撑。	设备CPU占用率
	内存占用率	获取设备的 CPU 占用率，其数据在获取后写入数据库，为监控展示作数据支撑。	设备内存占用率
	设备运行温度	获取设备的运行温度,其数据在获取后写入数据库，为监控展示作数据支撑。	设备温度
	网络I/O	获取设备的总网络 I/O 流量统计	接收流量、输出流量
	接口信息列表	获取设备的所有网络接口信息通过列表进行展示	接口编号、接口状态、接口描述、接口速率、接收流量及输出流量。
	运行时长	采集网络设备的运行时长	设备通电运行后至采集时间的运行总时长。
	会话数监视	获取设备的会话数，其数据在获取后写入数据库，为监控展示作数据支撑。	设备会话数
	连接数监视	获取设备每秒新建的连接数，其数据在获取后写入数据库，为监控展示作数据支撑。	设备连接数

A.7　信创安全设备监控指标见表 A.7

表 A.7　信创安全设备监控指标

设备类型	监测信息	描述	信息项
信创安全设备	基本信息	获取防火墙的基本信息	产品型号、设备名称、IP地址、MAC地址、监控协议、系统软件版本及序列号
	CPU占用率	获取设备的CPU占用率，其数据在获取后写入数据库，为监控展示作数据支撑。	设备CPU占用率
	内存占用率	获取设备的内存占用率，其数据在获取后写入数据库，为监控展示作数据支撑。	设备内存占用率
	设备运行温度	获取设备的运行温度，其数据在获取后写入数据库，为监控展示作数据支撑。	设备温度
	会话数监视	获取设备的会话数，其数据在获取后写入数据库，为监控展示作数据支撑。	设备会话数
	连接数监视	获取设备每秒新建的连接数，其数据在获取后写入数据库，为监控展示作数据支撑。	设备连接数
	网络I/O	获取设备的总网络I/O流量统计。	接收流量、输出流量。
	接口信息列表	获取设备的所有网络接口信息通过列表进行展示。	接口编号、接口状态、接口描述、接口速率、接收流量及输出流量。
	运行时长	采集防火墙设备的运行时长	设备通电运行后至采集时间的运行总时长

附 录 B

（规范性附录）

软硬件运维服务规范

B.1 例行操作服务见表 B.1

表 B.1 硬件运维服务规范-例行操作服务

信创台式计算机	监督控制	操作系统变更、软硬件配置变更、系统安全性、访问目标、操作行为、能耗、资产管理等
	定期检查	操作系统配置、软硬件配置、资源占用、接口占用、网络接入、网络访问、补丁更新、安全 防护、使用人员、运行情况等
	日常维护	系统备份、数据备份、补丁更新、病毒库、密码备份、硬件检测、部件更换、除尘、默认操作设置等
	宣传指引	培训、指引文件、知识库、设备检测工具等
	版本更新	管理、控制变更的过程，通过变更有序实施，确保变更的成功导入。变更发布包括变更请求响应，变更评估，变更开发，制定发布计划、制作发布包、并实施发布，配置信息更新和回顾总结。
信创瘦客户机	监督控制	开关机、软件配置变更、访问目标、操作行为、能耗、报废等
	定期检查	软件配置、资源占用、接口占用、网络接入、网络访问、补丁更新、安全防护、使用人员、运行情况等
	日常维护	数据备份、补丁更新、病毒库、密码备份、除尘等
	宣传指引	培训、指引文件、知识库、设备检测工具等
	版本更新	同台式计算机
移动计算终端	监督控制	操作系统变更、软硬件配置变更、系统安全性、访问目标、操作行为、能耗、资产管理等
	定期检查	操作系统配置、软硬件配置、资源占用、接口占用、网络接入、网络访问、补丁更新、安全、电源适应能力
	日常维护	系统备份、数据备份、补丁更新、病毒库、密码备份、硬件检测、部件更换、除尘等
	宣传指引	培训、指引文件、知识库、设备检测工具等
	版本更新	管理、控制变更的过程，通过变更有序实施，确保变更的成功导入。变更发布包括变更请求响应，变更评估，变更开发，制定发布计划、制作发布包、并实施发布，配置信息更新和回顾总结。
信息采集设备	监督控制	支撑软件及硬件配置变动、易损件使用、操作行为、能耗、报废等
	定期检查	按监督控制要求记录、核对、更新设备信息，机械动作情况，信息采集情况，电源线、联机线路的老化情况
	日常维护	外围输入输出设备日常维护内容分为测试类操作和基础类操作 测试类操作：信息采集测试

		基础类操作：信息采集接触面的清洁，更换老化电源、联机线路
	宣传指引	a）为用户提供外围输入输出设备使用培训和指引文件； b）为用户提供运行维护服务流程的培训和指引文件； c）为用户提供信息安全风险教育； d）为用户提供降低能耗的指导培训； e）为用户提供简易明了的使用说明、注意事项及禁用操作，规范服务对象的使用，避免误操作
	版本更新	管理、控制变更的过程，通过变更有序实施，确保变更的成功导入。变更发布包括变更请求响应，变更评估，变更开发，制定发布计划、制作发布包、并实施发布，配置信息更新和回顾总结。
打印设备	监督控制	介质、耗材、易损件的使用，支撑软件及硬件配置变动、操作行为、能耗、报废等
	定期检查	按监督控制要求记录、核对、更新设备信息，进退纸通道、传感器污染情况，设备启动、运行情况，打印字迹清晰度，打印颜色准确度，耗材消耗情况，传动、打印部件的磨损情况，电源线、联机线路的老化情况
	日常维护	测试类操作：自检测试、进退纸测试、打印测试、联机测试、业务测试等 基础类操作：检查及清洁进退纸通道，机械部位加油、调校，补充或更换磨损部件，补充耗材，更换老化电源、联机线路
	宣传指引	同信息采集设备
	版本更新	同信息采集设备
服务器	监控	在运行维护过程中，对服务器进行监控时，应根据具体的运行维护对象，确定监控内容和指标，包括服务器整体情况、电源工作情况、CPU 工作情况、内存工作情况、硬盘工作情况、网络端口工作情况等
	预防性检查	在运行维护过程中，对服务器进行预防性检查时，应根据具体的运行维护对象，确定性能检查内容和脆弱性检查，包括服务器的资源分配情况和策略、CPU 使用峰值情况、内存使用峰值情况、文件夹系统、文件系统空间使用情况、I/O 读写情况、网络流量情况等、与存储的链路性能测试
	常规作业	在运行维护过程中，对服务器进行常规作业时，确定操作内容和周期，包括系统微码升级、配置文件备份、过期日志和文件系统空间清理、服务器硬盘 RAID 配置检查（如有 RAID 控制器）、更换控制器电池（如有 RAID 控制器）
	版本更新	管理、控制变更的过程，通过变更有序实施，确保变更的成功导入。变更发布包括变更请求响应，变更评估，变更开发，制定发布计划、制作发布包、并实施发布，配置信息更新和回顾总结
操作系统	监控	操作系统 CPU 使用情况 操作系统内存使用情况 操作系统磁盘使用情况 操作系统网络端口状态和流量 操作系统光纤端口状态和流量 操作系统重要文件系统空间使用情况 操作系统日志情况
	预防性检查	性能检查内容、脆弱性检查内容
	常规作业	操作系统版本升级 操作系统磁盘读、写正常性测试 操作系统输入、输出设备读写测试（光驱、内置磁带机）操作系统配置文件备份操作系统备份 操作系统过期运行日志清理 网络通信正常性测试 操作系统临时文件清理

		操作系统端口访问测试 周期性关键设备主备切换/应急演练

B.2　数据库软件监控内容见表 B.2

表 B.2 数据库软件监控的内容

运行维护对象	监控内容
数据库软件	数据库主要进程运行情况 数据库连接是否正常 数据库表空间使用情况 数据库日志是否有异常 数据库日常备份是否正常等

B.3　中间件软件监控内容见表 B.3

表 B.3 中间件软件监控的内容

运行维护对象	监控内容
中间件软件	中间件运行状悉 主要进程运行状态 应用服务运行情况 中间件通信网络连接情况 中间件日志是否有报错信息

B.4　数据库软件预防性检查内容见表 B.4

表 B.4 数据库软件预防性检查内容

运行维护对象	性能检查内容	脆弱性检查内容
数据库软件	数据库的 TOP SQL 情况（如果数据库支持） 数据库 CPU 使用情况 数据库内存使用情况 数据库表空间使用情况 数据库锁情况 数据库会话数和操作系统进程数情况 数据库缓冲区（BUFFER）等命中率情况 数据库等待事件情况（如果数据库支持）	数据库是否安装相关风险补丁 表空间的使用是否达到了预定阀值 数据库关键文件是否做了镜像 数据库备份策略是否合理 数据库是否存在异常用户（如果数据库支持） 数据库版本一致性检查

B.5　中间件软件预防性检查内容见表 B.5

表 B.5 中间件软件预防性检查内容

运行维护对象	性能检查内容	脆弱性检查内容
中间件软件	中间件服务器业务 CPU 使用峰值 中间件服务器业务内存使用峰值 中间件服务器业务会话连接数	中间件是否满足运行冗余度要求 中间件是否安装相关风险补丁 中间件的数据库连接密码配置文件是否存在明码 相关重要运行程序是否有保留备份 操作系统配置是否符合中间件运行的要求 系统使用资源是否超过预定阀值等 中间件版本一致性检查

B.6　应用软件调研评估要求说明见表 B.6

表 B.6 应用软件调研评估要求说明表

项目	要求说明
系统运行环境	业务系统对国产化软硬件系统运行环境，能够满足系统的运行与维护要求，适应信创项目的快速变更与持续交付
系统组成要素	业务系统组成要素的构成分解应根据业务流程和应用系统架构设计进行层次化分解，识别关键业务点和核心业务系统
关联关系分析	业务系统构成的关联关系分析，包括与核心业务系统关联的非核心业务系统、接口连接、依存关系等
维护性分析	业务系统的维护性分析，包括业务系统的可监控性、易用性、安全性、可维护性，明确系统运行方式、组成要素及运行维护特点

B.7　应用软件例行操作要求说明见表 B.7

表 B.7　应用软件例行操作要求说明表

项目	要求说明
监控指标	业务系统运行的监控指标体系设计包括识别应用系统运行监控点，建立监控指标，以支撑实施监控和预防性检查
运行监控	业务系统运行的监控用于监控业务系统的运行及状态
客户回访	调查客户对运行维护的满意度及改进建议等
运维分析	分析维护事件，识别问题和风险

B.8　应用软件响应支持要求说明见表 B.8

表 B.8　应用软件响应支持要求说明表

项目	要求说明
服务受理	受理服务请求，包括故障请求和非故障请求
非故障请求处理	按服务级别协议分类处理
故障诊断定位	排查、诊断定位故障
解决方案制定	解决方案制定应基于应用系统重要性，确定解决方案
故障处理	执行故障解决方案，检测、监控、跟踪故障处理效果，将处理经验和建议纳入知识库
新用户与功能上线	在新用户、新系统功能上线前、上线中、上线后的服务工作，内容包括配置用户及用户权限、数据初始化、安全性检查和功能使用培训等
应急响应	针对业务系统故障影响范围大且不能在业务连续性规定要求内解决所采取的措施，内容包括应急组织架构确定、应急预案编制、应急演练、应急处置和应急回顾

B.9　应用软件优化改善要求说明见表 B.9

表 B.9　应用软件优化改善要求说明表

项目	要求说明
优化机会识别	业务系统的监控指标接近或超出阈值
	例行操作中未解决根本原因的问题
	响应支持中重复出现事件、用户不满意等
	例行操作和响应支持中识别出的风险

	应用系统支持的业务需求变化
功能性改进 (改正性维护)	应用软件的功能缺陷修复、满足业务需求变化(如流程改造、政策适应性改造等)而对应用软件功能的修改、完善和新增开发
性能优化改进 (完善性维护)	应用软件性能问题而对其功能的修改和完善，包括应用消息队列、共享内存优化，应用服务能力优化等
	对应用软件运行软环境(中间件、数据库、操作系统等)实施调优、升级或扩容等
适应性改进 （适应性维护）	应用软件因适应变化对其功能的修改和完善
	对应用软件运行软环境(中间件、数据库、操作系统等)的适应性实施调整等
预防性改进 （预防性维护）	应用软件可能存在某种威胁或风险而对其功能的修改和完善
	对应用软件运行软环境(中间件、数据库、操作系统等)的脆弱点实施改进等

B.10　应用软件变更发布要求说明见表 B.10

表 B.10　应用软件变更发布要求说明表

项目	要求说明
变更请求	变更请求响应来源于响应支持和优化改善，明确变更目的、内容和要求，满足需求变化的变更请求已得到用户确认
变更评估	评估变更的影响范围、成本、风险和合理性，决定是否接受变更请求
变更授权	变更开发需要获得授权才能执行
发布管理	制定发布计划、制作发布包并实施发布，对发布结果进行确认。发布失败时执行回退
配置更新	检查整理所有发布信息，更新配置信息
性能监控	变更发布后监控业务系统性能
回顾总结	回顾和总结变更发布过程，以持续改进

B.14　数据资源例行操作要求说明见表 B.11

表 B.11　数据资源例行操作要求说明表

项目	要求说明
数据监控	制定监控策略，依据业务规则设置告警，对应用软件功能模块各项异常操作告警，保证数据的完整性、准确性
预防性检查	针对与应用软件承载业务直接关联的数据(包括初始数据、基础数据、业务数据、配置数据、报表数据和授权数据等)，建立授权及一致性的标准和规则，依据标准和规则检查数据之间的一致性、符合性和安全性；
常规检查	抽样检查业务数据的真实性、有效性，防止数据错误，影响业务的正常开展

B.15　数据资源响应支持要求说明见表 B.12

表 B.12　数据资源响应支持要求说明表

项目	要求说明
数据问题处理	针对数据问题(包括数据错误、数据丢失、数据冗余和数据截断等)进行处理，检查和测试数据的完整性、准确性，并在测试环境正进行验证
服务请求处理	确定服务协议，按数据授权规定提供数据服务(包括数据提取、数据加工、数据质量清理、数据查询统计分析、数据挖掘、数据脱敏、特殊数据维护、回退数据维护、数据迁移、数据备份等)

B.16　数据资源优化改善要求说明见表 B.13

表 B.13　数据资源优化改善要求说明表

项目	要求说明
分析	围绕例行操作和响应支持中出现频率多、影响范围、重要程度的数据问题诊断分析
解决	针对诊断分析结果，制定解决方案并实施
改进	根据调研评估请求，改进数据例行操作和数据响应支持，提出优化方案并实施改进

B.17　数据资源评估分析要求说明见表 B.14

表 B.14　数据资源评估分析要求说明表

项目	**要求说明**
数据质量评估	包括基础数据质量评估、辅助数据质量评估和业务数据的影响分析
数据修改影响评估	包括业务参数修改的影响评估、数据字典修改的影响评估、基础数据修改的影响评估和业务数据修改的影响评估
数据规范评估	包括基础数据共同遵守规则和命名的评估、业务场景对应业务类型数据的规则评估和业务关键数据应遵循的规则评估
业务数据分析	包括面向业务重点支撑运营和战略需求的数据分析和面向预测重点支撑业态发展趋势的数据分析
应用软件变更对数据影响的评估	包括业务扩展、功能扩展等应用软件变更引起对数据完整性、一致性的评估，以及应用系统升级、变更、迁移等对数据完整性、一致性的评估