ICS 35.240.01
L 67

中华人民共和国国家标准

GB/T 34077.3—2021

基于云计算的电子政务公共平台管理规范 第3部分：运行保障管理

Management specification of electronic government common platform based on cloud computing—Part 3：Operation guarantee management

2021-03-09 发布　　2021-10-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

GB/T 34077《基于云计算的电子政务公共平台管理规范》预计分为以下5个部分：

——第1部分：服务质量评估；

——第2部分：服务度量计价；

——第3部分：运行保障管理；

——第4部分：平台管理导则；

——第5部分：技术服务体系。

本部分为GB/T 34077的第3部分。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分由中华人民共和国工业和信息化部(通信)提出并归口。

本部分起草单位：西安未来国际信息股份有限公司、哈尔滨国裕数据技术服务有限公司、陕西省信息化工程研究院、中国信息通信研究院、中国电子科技集团公司第28研究所、广东省信息工程有限公司、中国联合网络通信有限公司、阿里云计算有限公司。

本部分主要起草人：白峰、钟东江、桑艳娟、张勇、周逊、王宝红、刘述、唐佳俊、秦熹旻、赵昕、黄镇铭。

引　言

电子政务发展正处于转变发展方式、深化应用和突出成效的关键转型期。政府职能转变和服务型政府建设对电子政务发展提出了更新、更高的要求。以云计算为代表的新兴信息技术、产业、应用不断涌现，深刻改变了电子政务发展技术环境及条件。构建基于云计算的电子政务公共平台可以充分发挥既有资源的作用和新兴信息技术潜能，加快电子政务发展创新，提高应用支撑服务能力，增强安全保障能力，减少重复浪费、避免各自为政和信息孤岛。

随着国家电子政务发展方式的改变，对基于云计算的电子政务公共平台的运行保障服务提出了更高的要求。基于云计算的电子政务公共平台运行保障管理标准，明确规定了面向用户提供运行保障服务的服务内容、方式以及对平台资源的管理要求，确保提供优质的服务给机构和用户。

基于云计算的电子政务公共平台的运行保障管理，除遵循本部分外，还应符合国家法律、行政法规及有关强制性标准的规定。

基于云计算的电子政务公共平台管理规范 第3部分:运行保障管理

1 范围

GB/T 34077的本部分规定了基于云计算电子政务公共平台提供的服务和平台自身的运行保障管理。

本部分适用于电子政务公共平台的运行保障管理。

注:除非特殊说明,以下各章中"电子政务公共平台"均指"基于云计算的电子政务公共平台"。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是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 33780.3—2017 基于云计算的电子政务公共平台技术规范 第3部分:系统和数据接口

GB/T 34078.1—2017 基于云计算的电子政务公共平台总体规范 第1部分:术语和定义

GB/T 34080.3—2021 基于云计算的电子政务公共平台安全规范 第3部分:服务安全

3 术语和定义、缩略语

3.1 术语和定义

GB/T 34078.1—2017界定的以及下列术语和定义适用于本文件。

3.1.1

平台资源 platform resources

服务提供机构面向服务使用机构、公务人员和公众提供技术服务时所需的软硬件设施、技术资源和环境条件等多种资源的组合。

3.1.2

服务 service

基于云计算的电子政务公共平台向用户(包括服务使用机构、公务人员、公众)提供的各类网络、计算、存储、应用实例等服务。

3.2 缩略语

下列缩略语适用于本文件。

APP:移动设备应用软件(Application)

B/S:浏览器和服务器架构(Browser/Server)

CPU:中央处理器(Central Processing Unit)

IM:即时通讯、实时传讯(Instant Messaging)

KPI:关键绩效指标(Key Performance Indicator)

MPLS:多协议标签交换(Multi-Protocol Label Switching)

PC:个人计算机(Personal Computer)

SOC：安全运行中心(Security Operations Center)
SQL：结构化查询语言(Structured Query Language)
UPS：不间断电源(Uninterruptible Power System)
VPN：虚拟专用网(Virtual Private Network)

4 概述

本部分以用户(包括服务使用机构、公务人员、公众)使用电子政务公共平台服务的运行保障为主旨，对运行保障管理的服务内容和服务方式进行规定。同时对支撑电子政务公共平台的平台资源的运行保障管理提出要求，主要包括服务机构、服务内容、服务流程和运行服务支撑系统等。

面向服务使用机构的运行保障是指提供基础服务、工单服务、专属服务、咨询服务、代维服务、安全服务及入云用云等方面的运行保障服务；面向公务人员的运行保障是指提供工单服务、网络服务、定制服务及安全服务等方面的运行保障服务；面向公众的运行保障是指提供客服服务、通知服务、投诉服务等基础运行保障服务；面向平台资源的运行保障是指提供监测服务、配置服务、优化服务、运行安全、备份恢复、灾备管理、应急管理等方面的运行保障服务。

5 面向服务使用机构的运行保障管理

5.1 服务内容

面向服务使用机构用户应提供如下运行保障服务：

a) 基础服务：
   1) 客户服务：网络在线客服、电话客服，并及时响应用户的请求；
   2) 通知服务：邮件、无线应用工具、短信通知服务，及时通知服务的情况、状态等；
   3) 投诉服务：受理产品使用效果与服务效率等方面的投诉服务；
   4) 体验服务：体验真实操作环境的服务，体验查询、报故障、资源申请等操作过程；
   5) 培训服务：线上培训服务，帮助用户提升操作能力，熟练运用云产品与服务等；
   6) 满意度反馈：服务满意度的反馈服务，包括电话回访、满意度评分等；
   7) 云备份服务：虚拟机镜像、业务系统数据、用户数据备份服务。
b) 工单服务：用户在云服务使用过程中遇到的问题或故障，可形成工单并提交，由服务提供机构提供支持处理，并在 24 h 内进行反馈。
c) 专属服务：
   1) 灵活计费：提供多种计费模式，包括共享带宽包、包年包月、按量付费、后付费结算等；
   2) 免费测试：提供免费测试服务，帮助用户进行云产品的压力、性能测试等；
   3) IM 群支持：提供一对一的 IM 群支持，及时对用户进行在线支持；
   4) 无线应用在线支持：提供一对一的无线应用工具支持，及时对用户进行在线支持；
   5) 快速响应：提供专属服务经理一对一服务，在故障处理、特殊需求解决方面，提供 7×24 h 快速响应；
   6) 快速恢复：根据业务特点制定应急预案，并定期进行恢复演练；
   7) 绿色通道：提供域名备案绿色通道服务；
   8) 服务报告：专属服务经理应定期提交服务报告。
d) 咨询服务：提供云产品与服务功能的咨询服务，对用户进行功能介绍、使用方法指导等。
e) 代维服务：提供 7×24 h 的云服务器代维服务，包括系统监控、定期检查、数据备份、故障排查及恢复等。

f) 备案解析服务：
   1) 域名备案：用户登录备案系统，通过信息填写、提交初审、办理拍照、最终审核等流程，完成域名备案；
   2) 云解析：对上线网站分配公网 IP 地址，进行域名解析、域名绑定等。
g) 云安全服务：
   具体服务要求按照 GB/T 34080.3—2021 执行。
h) 入云服务：
   1) 应用部署：提供多种方式的应用入云部署服务，满足应用入云的需求；
   2) 业务迁移：提供流程化的业务迁移服务，保障业务平滑有序迁移入云；
   3) 资源配置：用户根据云资源模板，配置所需资源的数量、类型、容量、关联、策略等。
i) 用云服务：
   1) 服务监测：提供服务实时监测服务，使用户随时了解云服务的运行状态，监测指标包括 CPU、内存、磁盘、缓存和带宽的利用率，会话时长，会话连接数，告警情况等；
   2) 业务系统监测：提供业务系统实时监测服务，使用户随时了解业务系统的运行状态，监测的内容包括用户数量、访问量、端口利用率、数据转发量、告警情况等；
   3) 故障查询：提供云服务故障处理进度的查询服务，使用户能够查看所属服务故障处理的进度状态，故障发起、处理和完结的时间节点等；
   4) 服务优化：提供云服务优化服务，当资源使用过程中，容量、性能等方面接近预警指标时，提出合理化优化方案，并提醒用户进行资源升级或扩容。

5.2 服务方式

5.2.1 概述

面向服务使用机构用户的运行保障管理，应采用云服务门户、移动终端、在线通信的方式提供服务。

5.2.2 云服务门户

云服务门户提供以下服务功能：

a) 提供统一的电子政务公共平台云服务门户，进行各类服务的申请、查看和监控等操作；
b) 提供各类云产品与服务的申请操作入口，分类包括：云计算与网络、云存储、云应用服务、域名和网站、数据库、数据处理和分析、安全服务、监控与管理等；
c) 提供管理控制台，方便注册用户查看或操作相关功能页面，包括云解析、账户管理、费用中心、续费管理、消息中心、工单管理、备案管理等；
d) 提供按照账户分权的云服务监测功能，对云产品与服务的运行状态、带宽情况、连接数、报警情况、端口使用率、内存使用率、缓存使用率等方面进行实时监测，让用户可以随时了解云资源的运行情况；
e) 提供用户备案实名认证或域名实名认证功能，认证内容包括个人身份信息、备案信息、域名信息等；
f) 提供帮助中心，让公众用户通过帮助中心自助查找资源申请、使用、操作等方面的问题解答。

5.2.3 移动终端

提供移动终端访问方式，通过终端 APP 或公众号，采用移动设备进行访问。

5.2.4 在线通信

提供电话在线或网络在线的通信方式，及时响应用户在门户访问中的提问和咨询等。

5.3 服务管理

5.3.1 概述

应面向服务使用机构，提供运行服务响应、运行故障服务、运行服务协议、运行服务方案、运行服务分级、运行服务报告、运行服务关闭等方面的服务管理。

5.3.2 运行服务响应

运行服务响应方面的具体要求如下：

a) 应提供统一服务接口，设立服务台。

b) 应提供多种服务台响应方式，包括但不限于：

1) 热线电话：统一的热线号码、自动应答分类选择、坐席应答等；

2) 服务门户：在线账户注册、在线工单提交、在线投诉提交等；

3) 无线应用工具和微博：统一的公共服务账号、政务微博服务地址等；

4) 移动终端：通过移动终端 APP 等方式进行问答、咨询、投诉、查询等。

c) 应提供 7×24 h 热线服务，并设置服务使用机构技术服务岗位。

d) 应记录各类服务响应请求，通过运行服务支撑系统进行处理、分派、解决和关闭。

e) 应建立运行服务投诉相关的流程和机制，相关内容包括：

1) 建立投诉处理流程，开通云服务门户、电话、微博等投诉渠道；

2) 记录投诉意见，15 min 内分派任务，及时处理，并形成处理过程记录；

3) 根据投诉处理进度，每隔 1 h 将处理情况反馈给用户，可采用电话、短信、邮件等方式；

4) 建立投诉升级机制，分派更高级的服务管理人员对投诉进行处理；

5) 建立运行服务投诉处理事后的问责机制，追究引起用户投诉的相关服务人员的责任；

6) 建立服务质量反馈机制，用户对每次服务可进行打分及提交评价等。

f) 应提供查询服务，用户可查看服务故障处理、投诉处理的状态等：

1) 服务故障的处理进度状态应包括：响应、分派、执行、反馈、评价等；

2) 服务投诉的处理进度状态应包括：响应、升级、分派、执行、反馈等。

g) 应提供多种服务查询的方式，包括但不限于：

1) 网络查询：桌面终端、智能终端等；

2) 电话查询：电话询问客服坐席人员；

3) 服务门户查询：登录服务门户进行处理进度的查看；

4) 移动终端查询：登录移动终端 APP 进行各类信息查询。

5.3.3 运行故障服务

运行故障服务方面的具体要求如下：

a) 应建立运行故障服务流程，形成作业文件和流程图。

b) 运行故障的来源，包括但不限于：

1) 服务提供机构主动检查、巡检、监控发现的服务故障；

2) 用户向服务台发起的服务故障请求等。

c) 按照故障等级定义，应创建服务故障请求任务工单，30 min 内分派技术人员处。

d) 对服务故障进行诊断分析，判定故障点，及时处理，并形成记录：

1) 用户端设备原因引起的服务故障，客服及技术人员应指导解决；

2) 电子政务公共平台原因引起的服务故障，应分派技术人员解决；

3） 托管业务系统自身原因引起的服务故障，技术人员应分析故障原因，形成解决办法，通知并配合业务系统开发人员进行故障的处理。

e） 根据故障等级定义的更新间隔，应将处理进展进行反馈，反馈方式包含电话、短信、邮件、云服务门户提醒等；服务故障反馈的内容，包括但不限于：

1） 故障发生：造成服务故障的原因及故障的表象；

2） 故障处理：服务故障处理进度、措施或方案；

3） 故障关闭：服务故障的处理结果以及恢复服务情况；

4） 故障复盘：针对故障进行复盘，并制定改进措施。

f） 应建立运行故障处理和反馈的管理制度，规范故障反馈的操作和通告过程等。

5.3.4 运行服务协议

运行服务协议方面的具体要求如下：

a） 应与服务使用机构签署运行服务协议，内容主要包括双方职责、服务内容、服务期限、安全保密要求、违约责任、处理机制、服务边界、绩效考核要求和费用等条款；

b） 服务协议应以纸质或在线电子确认，电子确认应支持PC终端、智能终端等；

c） 服务协议应以纸质或电子方式保存，保存期为服务到期时间的后续一年。

5.3.5 运行服务方案

运行服务方案方面的具体要求如下：

a） 应向服务使用机构提供套餐式的运行服务，将多项运行服务打包组合，制定运行服务方案；

b） 运行服务方案的内容应包括但不限于：

1） 服务范围：基础设施、支撑软件、应用功能、信息资源技术、信息安全方面等；

2） 服务内容：例行服务、响应服务、优化服务、评估服务等；

3） 服务级别：制定差异化服务级别；

4） 服务目标：应提供可用性、安全性、及时性和规范性目标；

5） 资源配备：配备服务资源，包括人员、软硬件系统、维护工具等；

6） 服务方式：现场响应支持、远程响应支持等。

5.3.6 运行服务分级

应对运行服务进行分级，适应用户的多种选择。运行服务的分级，由高到低，分为一到四级服务，具体分级情况如下：

a） 一级服务，服务受理时间7×24 h，服务响应时间为常驻、即时响应，人员到场时间为常驻、即时响应，故障恢复时间≤2 h，系统备件为关键部件及备件库，巡检周期为每日或每周定期，服务支持为现场及远程人员支持；

b） 二级服务，服务受理时间7×24 h，服务响应时间≤15 min，人员到场时间≤2 h，故障恢复时间≤4 h，系统备件为关键部件及备件库，巡检周期为每月一次，服务支持为现场及远程人员支持；

c） 三级服务，服务受理时间5×8 h，服务响应时间≤30 min，人员到场时间≤6 h，故障恢复时间≤8 h，系统备件为备件库，巡检周期为每季度一次，服务支持为远程人员支持；

d） 四级服务，服务受理时间5×8 h，服务响应时间≤30 min，人员到场时间为下个工作日，故障恢复时间≤24 h，系统备件为备件库，巡检周期为每半年一次，服务支持为远程人员支持。

5.3.7 运行服务报告

运行服务报告方面的具体要求如下：

a) 应向服务使用机构提供运行服务报告，包括例行服务报告、响应服务报告、优化服务报告和评估服务报告四类报告。

b) 应提供例行服务报告，不定期或每月提交一次，报告内容包括但不限于：

1) 基础设施：实时监控、巡检、清洁保养相关记录等；

2) 支撑软件：实时监控、巡检、资产管理相关记录等；

3) 应用功能：实时监控、巡检、数据初始化、数据维护相关记录等；

4) 信息资源：实时监控、巡检、资产管理相关记录等；

5) 信息安全：安全事件监测、病毒态势、系统漏洞、数据备份相关记录等。

c) 应提供响应服务报告，在故障、投诉处理完毕后的第二天内向服务使用机构进行提交，报告内容包括但不限于：

1) 基础设施：现场值守、故障处理、耗材更换、配件更换相关记录等；

2) 支撑软件：故障处理、备份恢复相关记录等；

3) 应用功能：故障处理、升级变更、参数调整相关记录等；

4) 信息资源：故障处理、参数调整相关记录等；

5) 信息安全：数据加解密、接入控制、身份识别、访问授权相关记录等。

d) 应提供优化服务报告，不定期或每季度提交一次，内容包括但不限于：

1) 基础设施：耗材更换、系统升级、配置优化、空间扩容相关记录等；

2) 支撑软件：升级、配置优化、参数调优相关记录等；

3) 应用功能：升级优化、配置优化相关记录等；

4) 信息资源：升级优化、配置优化相关记录等；

5) 信息安全：系统加固、漏洞修复、行为管理控制相关记录等。

e) 应提供评估服务报告，不定期或每半年提交一次，内容包括但不限于：

1) 基础设施：性能评估、流量评估、改进建议等；

2) 支撑软件：性能评估、容量可用性分析、运行记录分析等；

3) 应用功能：性能评估、运行记录分析、日志审计分析、进程资源消耗分析等；

4) 信息资源：性能评估、运行记录分析、数据完整有效分析等；

5) 信息安全：业务连续性、安全风险评估、系统安全测评、门户网站安全测评等。

f) 应采用纸质或电子的方式提交报告，报告保存在服务提供机构，保存周期等同服务协议保存期。

5.3.8 运行服务关闭

运行服务关闭方面的具体要求如下：

a) 服务提供机构在服务协议到期前两个月，应以书面形式向服务使用机构发出服务到期的提示。

b) 服务提示内容，应包括但不限于：

1) 运行服务的名称、内容和期限，提醒服务即将到期；

2) 征求服务是否续期，续签联系人及方式。

c) 应对到期服务产生的相关数据进行离线保存，保存期为一年。

d) 应释放到期服务占用的资源，提高资源利用率。

6 面向公务人员的运行保障管理

6.1 服务内容

应向公务人员用户提供以下服务：

a) 基础服务：
   1) 客户服务：网络在线客服、电话客服，并及时响应用户的请求；
   2) 通知服务：邮件、无线应用工具、短信通知服务，及时通知服务的情况、状态等；
   3) 投诉服务：受理产品使用效果与服务效率等方面的投诉服务；
   4) 满意度反馈：服务满意度的反馈服务，包括电话回访、满意度评分等。
b) 工单服务：用户在网络及在线办公服务使用过程中遇到的问题或故障，可形成工单并提交，由服务提供机构提供支持处理，并在 24 h 内进行反馈。
c) 网络服务：
   1) 互联网：向用户提供互联网开通服务，通过电子政务公共平台的统一互联网出口连接到互联网，并在互联网出口提供相应的管控策略和安全审计；
   2) 政务网：向用户提供电子政务外网网络连接服务，通过连接电子政务公共平台访问平台上提供的各类办公应用系统，并在网络接入口提供相应的管控策略和安全审计。
d) 定制服务：
   1) 信息定制：根据用户的需求，定制并组合推送云资源信息；
   2) 个性化定制：根据用户的个性化需求，定制个性化的服务界面、个人隐私保护、专属服务人员和个人兴趣信息等。
e) 安全服务：提供数据的安全加密，实现用户信息和数据的安全传输与存储。

6.2 服务方式

应向公务人员用户采用以下的服务方式提供服务：
a) 提供统一的电子政务公共平台云服务门户，方便用户进行注册、登录、身份认证等；
b) 提供移动终端访问方式，通过终端 APP 或公众号，采用移动设备进行访问；
c) 提供电话在线或网络在线的响应方式，及时响应用户在门户访问中的提问和咨询等。

7 面向公众的运行保障管理

7.1 服务内容

应向公众用户提供以下基础服务：
a) 客户服务：网络在线客服、电话客服，并及时响应用户的请求；
b) 通知服务：邮件、无线应用工具、短信通知服务，及时通知服务的情况、状态等；
c) 投诉服务：受理产品使用效果与服务效率等方面的投诉服务。

7.2 服务方式

应向公众用户采用以下的服务方式提供服务：
a) 提供统一的电子政务公共平台云服务门户；
b) 提供移动终端访问方式，通过终端 APP 或公众号，采用移动设备进行访问；
c) 提供网络在线或电话在线的响应方式，及时响应用户在门户访问中的提问和咨询等。

8 面向平台资源的运行保障管理

8.1 服务机构

服务提供机构应对电子政务公共平台的服务保障设置以下机构和岗位：

a) 根据电子政务公共平台的规模和运行要求，设置相应的运行保障机构及负责人。
b) 运行保障机构包括服务管理、运行维护、安全服务等部门或组。
c) 设置客户服务岗、服务操作岗、技术服务岗、服务管理岗、服务安全岗等岗位。
d) 建立各岗位的职责说明书，定岗定责定员。
e) 客户服务岗职责：
   1) 接收用户的服务请求，记录服务请求信息，协调技术人员处理服务故障；
   2) 向用户提供业务咨询、受理与交付请求、用户回访和用户投诉等服务；
   3) 能够与用户进行良好的沟通；
   4) 具备计算机及网络专业知识，能为用户提供有效的解决方案；
   5) 熟悉运行保障机构各部门职责、服务请求分类，具备协调能力，能及时准确的分派服务台无法解决的问题。
f) 服务操作岗职责：
   1) 提供日常设备系统的监控和巡检；
   2) 按照操作流程规范和手册提供操作服务，并对违规和失误操作负责；
   3) 能够与客服、技术服务人员进行良好的沟通；
   4) 掌握机房、主机、网络、系统、虚拟化、应用等方面的知识，具备及时发现服务故障和初步判断和处理故障的能力；
   5) 具有两年以上服务操作经验。
g) 技术服务岗职责：
   1) 具备基础设施、支撑软件、云资源、应用软件、配置数据、管理工具和安全服务的技术支持能力；
   2) 及时响应并处理运行保障服务过程中的请求、故障和问题；
   3) 提供电子政务公共平台虚拟资源的配置等服务；
   4) 能够同厂商工程师、管理岗位人员进行良好的技术沟通；
   5) 具备网络、主机、系统、虚拟化、应用方面的专业知识，能对软硬件设备系统进行调试，对云服务故障进行分析、解决；
   6) 具备专业任职资格证书，包括软考证书、硬件厂商认证证书、培训证书等；
   7) 具有三年以上技术服务经验。
h) 服务管理岗职责：
   1) 提供运行保障服务管理工作，包括服务运行规划、质量控制、业务关系维护、操作规程和运行制度编制等；
   2) 提供规划、检查方面的运行保障服务，负责服务策划、实施、检查、改进的范围、过程、安全和成果；
   3) 提供规划、评估电子政务公共平台服务资源的使用情况；
   4) 负责制定服务管理、服务运行维护等的制度和规范；
   5) 能与用户、客服、技术、操作人员进行良好的沟通；
   6) 掌握服务规划、设计、管理等方面的专业知识；
   7) 具备专业任职资格证书，包括软考证书、硬件厂商认证证书、培训证书等；
   8) 具有五年以上服务管理。
i) 服务安全岗职责：
   1) 负责服务资产的收集和风险评估，完成服务安全方案设计，安全事件、投诉的协调处理；
   2) 负责服务安全实施工作，评估服务安全风险，制定服务安全策略和安全制度；
   3) 负责制定和更新服务安全应急预案并更新，并对安全隐患提出解决方案，组织参与应急预

案的测试和维护等相关工作；

4） 负责制定服务安全管理的目标，制定服务运行安全管理的规划方案；

5） 能与用户、客服、操作岗、技术岗人员进行良好的沟通；

6） 掌握服务安全技术、安全管理体系的相关知识。

8.2 服务内容

8.2.1 概述

面向平台资源的运行保障管理的服务内容，具体包括：资源监测、资源配置、资源优化、运行安全、备份恢复、灾备管理、应急管理、资产管理方面的内容。

8.2.2 资源监测

提供监控场所和监控终端，对资源的运行状况进行监测、记录和趋势分析，具体要求如下：

a） 监测的内容，应包括但不限于：

1） 机房资源：机房温湿度、漏水告警、电流电压、UPS 负载、消防气体钢瓶压力等；

2） 网络资源：链路负载、网络流量、网络连接数、网络设备健康状况、硬件资源开销；

3） 主机资源：主机 CPU、内存负荷（含虚拟机）、网络连通性、工作指示灯状态；

4） 存储资源：空间占用率、网络连通性、存储状态、数据备份状态；

5） 支撑软件资源：端口、连接数、CPU 和内存使用率、磁盘使用率、文件系统空间；

6） 环境资源：环境变量、类库信息、连接数、文件系统、表空间大小；

7） 信息资源：数据流、数据流向、实例状态、SQL 执行和授权状态；

8） 应用功能资源：用户数量、访问统计、用户接口、文字内容、门户首页；

9） 应用性能：加载时间、响应时间、并发用户、资源实例、实时会话数。

b） 应对服务资源进行分类管理监测，将设备分为核心资源、关键资源、一般资源，根据资源的重要程度，设置不同的监测频度、监测点数量等。

c） 应配置监控工具，通过声音、短信、电话和邮件等告警方式进行报警提醒。

d） 应建立运行服务资源监测制度，规范人员操作和监测指标等。

e） 应对监控记录数据进行保存，保存周期至少半年。

8.2.3 资源配置

对电子政务公共平台的服务资源进行统一管理，集中调度，按需弹性分配资源，具体要求如下：

a） 应对电子政务公共平台的服务资源进行配置管理，具体分类为：

1） 机房资源：机柜、空调、UPS、配电柜等；

2） 网络资源：运营商链路、负载均衡设备、网络拓扑、防火墙、入侵防御设备等；

3） 主机资源：虚拟机、物理服务器（含小型机）等；

4） 存储资源：存储设备、带库设备、虚拟存储空间、虚拟备份设备等；

5） 支撑软件和环境资源：操作系统、数据库、中间件、开发环境、测试环境、运行环境等；

6） 信息资源工具：数据采集工具、数据对比工具、数据库管理控制台、信息交换工具、数据融合工具、对数据服务发布工具、对数据分析工具等；

7） 应用功能资源：电子邮箱、市民邮箱、自助建站、呼叫中心、搜索引擎、通用办公等。

b） 应建立各类资源之间的配置关联关系，进行配置项的管理。

c） 应建立配置管理数据库，每月更新一次配置项的状态。

8.2.4 资源优化

应提供电子政务公共平台各类资源的统一管理和优化，具体措施如下：

a) 资源优化的具体措施包括：
   1) 机房资源：机柜空间释放、机房的温湿度调整、机房高低压配电调整、机房 UPS 设备负载调整、消防气体钢瓶增压等；
   2) 网络资源：网络流量控制策略调整、网络设备模块更换、网络拓扑更新、路由条目清理等；
   3) 主机资源：主机 CPU、内存、磁盘容量的增加等；
   4) 存储资源：读写速度的调整、存储空间的调整等；
   5) 公共性支撑软件资源：软件系统版本升级、补丁修补，数据工具的交换、融合、叠加、采样等性能的调优等；
   6) 基础应用系统：应用系统模板的更新、参数调整、进程数优化、空间容量扩容等；
   7) 公共性应用功能：应用功能模板更新、线程进程优化、版本升级等。
b) 每三个月进行优化操作。

8.2.5 运行安全

提供平台资源安全运行的相关制度规范，具体要求如下：

a) 应制定运行安全管理制度，包括但不限于：
   1) 物理与环境安全管理：机房环境安全、线缆通信安全、设备安全等；
   2) 通信与安全操作管理：恶意代码防护、网络安全、移动介质安全、信息交换安全等；
   3) 访问控制管理：网络访问、主机访问、应用和信息访问、移动设备访问、远程访问等；
   4) 账号与口令管理：账号权限申请、账号使用、账号变更、账号消除、口令管理等；
   5) 病毒及防护：病毒防御、邮件门户防护、补丁管理、攻防测试、边缘及端点防护等；
   6) 安全事件管理：处理原则、人员职责、事件分类分级、报告与处置、记录与总结。
b) 应制定保密管理规范，严禁各类涉密设备接入电子政务公共平台，严禁涉密资料、文件、信息在电子政务公共平台上进行交换、传输和存储。
c) 应提供公共平台各类安全系统的定期检查和监测服务，包括防病毒管理系统、VPN 系统、加解密系统、登录认证系统、虚拟资源隔离和防护系统、安全审计系统等的运行保障。
d) 应提供服务连续性计划，具体内容见 8.2.6 和 8.2.7。
e) 具体技术要求按照 GB/T 34080.3—2021 执行。

8.2.6 备份恢复

提供业务系统和数据的日常备份和恢复测试，具体要求如下：

a) 日常备份：
   1) 应采取近线和离线的方式，对数据进行增量备份或全备份；
   2) 增量备份应每天进行一次，全备份应每周进行一次；
   3) 应制定备份策略，记录数据的备份方式、存放位置、备份时间、备份频度等；
   4) 需采取加密处理的数据，加密操作时应有两名工作人员在场，并形成加密记录；
   5) 数据的保存期限应为三年。
b) 恢复测试：
   1) 应对备份数据导出测试，检查备份介质的有效性，周期为每季度一次；
   2) 应对备份数据恢复测试，验证数据的有效性，周期为每半年一次；
   3) 应对业务应用恢复测试，验证应用的可用性，周期为每半年一次；

4） 应形成恢复测试相关的记录。

c） 具体技术要求按照 GB/T 34080.3—2021 执行。

8.2.7 灾备管理

提供同城灾备和异地数据恢复管理服务，具体要求如下：

a） 应制定灾备和恢复服务方案，包括人员、环境准备、流程等。

b） 应规定灾备演练频度：

1） 业务应用级灾备，每年至少一次；

2） 数据级灾备，每年至少两次。

c） 应制定灾备演练步骤：

1） 制定演练方案、确定场景、演练步骤、演练预案等；

2） 准备物资材料、仪器仪表、后勤保障、指挥部场地、办公及通信条件、车辆食宿和演练前的培训等；

3） 严格按照演练方案实施，详细记录演练的每个步骤、时间点和操作痕迹；

4） 进行复盘推演，分析各环节所消耗的时间，检查时间是否是可以接受的。

d） 应总结分析灾备演练中发现的问题，并逐步优化完善。

e） 具体技术要求按照 GB/T 34080.3—2021 执行。

8.2.8 应急管理

提供运行供应急管理相关管理机制、演练计划，具体要求如下：

a） 应建立运行应急管理机制，管理内容包括但不限于：

1） 建立应急响应组织，设置应急响应责任人、现场负责人、现场执行人等；

2） 制定应急响应制度，规定应急响应的目标、范围、处置原则、管理措施等；

3） 制定应急响应预案，规定应急响应的组织结构、人员职责、监测预警、预案启动、处置流程及方法、保障措施等。

b） 应制定演练计划，演练步骤包括：

1） 对演练进行准备，包括预案演练方案准备、演练步骤、物资准备和后勤保障；

2） 演练过程中，详细记录时间点和操作痕迹，收集证据，作为查找原因、追究责任的依据；

3） 对演练进行总结分析，包括预案事件发生原因的追溯、当前损失以及潜在影响的估算、责任人岗位职责及动机分析等，并根据讨论结果制定相关预防措施；

4） 对服务安全应急预案进行优化，包括应急故障的发现和预案流程的改进等；

5） 每年至少进行一次安全应急预案演练。

c） 应急管理具体技术要求应符合 GB/T 34080.3—2021。

8.2.9 资产管理

应提供平台资源的资产管理制度与流程，具体内容如下：

a） 建立资产管理制度与流程，对资产的采购、入库、维修、借调、领用、折旧和报废等进行管理。

b） 配置资产管理系统，将资产信息录入系统数据库。

c） 资产信息的静态管理，包括但不限于：

1） 对资产信息进行维护，包括信息的收集、手动录入等；

2） 对资产信息进行统计分析，计算资产的利用率，合理使用资产。

d） 资产信息的动态管理，包括但不限于：

1） 对资产信息进行自动发现和采集；

2） 对资产信息进行自动同步和更新。

e） 建立资产台账，记录资产的账、卡、物信息，做到账物相符、账卡相符。

f） 每年进行至少一次资产状况检查，形成资产清查报告。

g） 提供资产绩效管理，每年评估资产的利用率，形成资产绩效报告。

8.3 运行服务流程

应面向平台资源提供如下运行服务管理流程：

a） 建立运行保障过程中的核心管理流程，包括服务级别管理流程、事件管理流程、问题管理流程、配置管理流程、变更管理流程、服务报告流程、信息安全管理流程；

b） 核心管理流程的具体内容可参照ITSS、ISO 20000以及ITIL等执行。

8.4 运行服务支撑系统

8.4.1 概述

应从系统功能、系统性能、系统接口三个方面对运行服务支撑系统进行规范要求。

8.4.2 系统功能

提供运行服务支撑系统的具体系统功能要求如下：

a） 应提供服务门户管理功能，包括但不限于：

1） 用户注册：基本信息录入、信息修改、账户添加、账户删除、实名认证；

2） 服务目录：运行服务分类、运行服务介绍、运行服务目录、运行服务检索；

3） 计费(量)管理：充值记录、订单查询、账单查询、账户查询；

4） 在线支付：网银支付、第三方支付、智能终端支付；

5） 在线培训：模拟环境试用、培训视频；

6） 在线查询：故障处理查询、投诉处理查询；

7） 在线投诉：语音响应、在线留言、投诉请求、投诉处理；

8） 在线评价：运行服务评价、问卷调查、留言评价。

b） 应提供服务台(呼叫中心)管理功能，包括但不限于：

1） 服务请求：请求创建、信息记录、请求分派、请求处理、请求关闭；

2） 服务回访：日常回访、故障回访、满意度评价；

3） 服务投诉：投诉创建、投诉记录、投诉处理、投诉关闭；

4） 服务咨询：咨询创建、咨询解答、咨询关闭。

c） 应提供云平台监测管理功能，包括但不限于：

1） 机房监测：机房整体集中展现、机柜运行状态展现、应急集中关机；

2） 网络监测：网络拓扑发现、拓扑管理、拓扑工具、性能监视、设备面板、网络资源、监测策略、性能分析、设备信息展现、历史性能数据分析、MPLS VPN管理；

3） 业务监测：主机性能、数据库性能、中间件性能、应用服务、存储性能；

4） 专项管理：拓扑、告警、性能、配置；

5） 巡检管理：巡检内容设定、巡检执行、巡检统计；

6） 流量统计分析：流量采集、流量监控、流量排名、流量快照、高级分析统计；

7） 统计报表：告警统计、性能统计、TOP N综合报表、关键KPI统计；

8） 支撑业务应用系统：数据库基本信息、中间件信息、构件运行资源消耗、容量节点数量、性能测量数量和应用系统状态；

9） 云生命周期管理：服务定义、自助请求、流程管理、自动部署和调度、性能管理、合规管理、服务延期、服务终止、资源回收；

10） 虚拟资源管理：配置管理、资源分析、资源回收、资源池管理、配置信息收集、容量管理；

11） 自动化和标准化管理：智能巡检、资源调度、动态资源调配、介质库（系统、补丁、镜像、软件）、自动化部署（虚拟机、软件、操作系统、镜像、补丁）、自动化流程库、脚本库、审核基线库、与流程管理的集成、与配置管理的集成；

12） 服务报告：服务监视报告、服务响应报告、服务故障报告、服务变更报告。

d） 应提供云应用性能监测管理功能，包括但不限于：

1） 自动学习：服务路径学习、业务路径生成、服务架构生成；

2） 故障定位：告警视图数据挖掘、快速定位、自动定位；

3） 回放识别：服务架构回放、存储会话快照、逻辑节点回放、故障程度识别；

4） 预警规则：动态添加、即刻生效、历史数据匹配；

5） 监听解析：非耦合监听解析、会话数据监听、会话数据还原；

6） 可视化：会话数据、应用可用性、应用性能、应用负载量；

7） 组件状态展现：会话类型展现、会话渠道展现、组件指标、组件关联；

8） 关键指标展示：会话数、成功率、响应时间、响应率、返回码；

9） 监视范围覆盖：端到端应用服务路径、双中心应用服务路径。

e） 应提供运行服务流程管理功能，包括但不限于：

1） 服务支持流程：服务台、事件管理、问题管理、变更管理、配置管理；

2） 服务交付流程：持续性管理、可用性管理、能力管理、安全管理；

3） 辅助管理：报表管理、值班管理、应急预案管理、规章制度管理、系统配置管理；

4） 知识库管理：信息添加、级别分类、引用统计、入库审批、版本更新；

5） 资产管理：设备类型、型号、厂商、管理域、机构、服务商、责任人、合同、文档维护。

f） 应提供服务安全管理功能，包括但不限于：

1） 信息采集处理功能：用户信息、安全信息、安全策略的采集处理的，安全信息预处理等；

2） 信息分析处理功能：管理对象的识别定位，合规性分析，状态分析，威胁分析等；

3） 安全事件响应处置功能：响应方式和处置方式；

4） 信息展示功能：用户信息展示、资产信息展示、分析信息展示；

5） 系统支撑功能：系统维护、工单系统、自身安全；

6） 报告功能：安全故障报告、安全检查报告。

g） 应提供服务安全审计功能，包括但不限于：

1） 安全审计管理功能：信息综合展示、审计报表、综合配置等方面的功能；

2） SOC 审计功能：安全管理用户审计、安全管理行为审计；

3） 安全应用支撑审计功能：单点登录行为审计、应用访问行为审计、应用系统安全行为审计、统一用户管理审计；

4） 上网行为审计功能：行为分析审计、网页内容关键字审计、非 TCP21 端口行为审计、互联网事件管理审计；

5） 数据库审计功能：用户及权限审计、数据库访问审计、数控操作审计；

6） 服务过程审计功能：故障流程审计、问题流程审计、变更流程审计、报告流程审计。

h） 应提供业务视图管理功能，包括：视图结构和视图需求等方面。

i） 应提供分级分域管理功能，根据地域、机构、用户进行域的划分，提供差异化个性服务等。

j） 应提供系统维护管理功能，管理的范围包括用户管理、权限管理、日志管理和自身管理等方面。

k） 应提供统一单点登录功能，实现用户权限分级分层管理。

l） 应提供运行服务协议管理功能，实现在线协议签订或确认。

8.4.3 系统性能

提供运行服务支撑系统的具体系统性能要求如下：

a） 系统可靠性

1） 系统的退出和停止，应不影响其管理的IT基础设施和应用系统；

2） 应提供7×24 h不间断服务，年系统可用性应达到99.95%以上。

b） 系统容量

1） 应至少支持2 000个用户及200个并发用户，具有良好的扩展性并预留二次开发接口；

2） 支持所有主流IT设备和系统，应支持信息安全自主可控设备和系统；

3） 监控规模网络设备应达5 000台以上，主机设备应达1 000台以上，支持1 000项以上业务应用；

4） 监控轮询时间应小于5 min并可根据业务重要程度进行自行设定阈值，误报漏报率小于1%；

5） 能够从不同类型的数据源进行数据采集，处理的能力应不小于每秒2 000条记录；

6） 当数据库中的日志记录数达到200万条时，模糊查询的响应时间应不超过10 s；

7） 在主流服务器配置下，高性能的嵌入式数据，每秒处理数达到十万个SQL语句分析。

c） 系统实时性

1） 简单操作及平台数据查询操作界面响应时间应小于2 s，大数据量报表数据查询操作界面响应时间小于15 s；

2） 能设置监控轮询时间小于5 min，并可根据设备或系统重要级别进行自行阈值设定，误报漏报率应小于1%。

d） 系统安全性

1） 应具备系统管理、用户权限管理及分级分域权限管理能力，支持单点登录；

2） 应具备高可靠性和稳定性，采用牢固的体系结构设计，具备容错容灾能力、纠错自恢复安全机制和自动诊断告警。

e） 系统可扩展性

1） 应采用分布式结构、模块化设计，支持通过增加硬件设备提高系统的管理容量；

2） 应采用B/S架构，采用可靠、安全、可移植性高的编程语言，兼容各类操作系统；

3） 应支持各类大型数据库作为后台数据库。

f） 系统存储能力

1） 告警数据、性能数据在系统中应存储3个月；

2） 资源数据在系统中应存储6个月；

3） 经系统处理后的报表数据、分析数据在系统中应存储12个月；

4） 经用户设定为重要的数据应长期保持。

g） 系统易用性

1） 用户界面应简洁、友好，操作简单、提示清晰，提供系统操作在线帮助；

2） 用户界面显示应采用简体中文；

3） 系统应支持多种方式来呈现各类管理信息，对于统计信息，应具有表格或直观图形化（如直方图、曲线图、饼图等）输出方式。

h） 应具备系统可维护性，提供对系统自身运行情况的维护和管理，包括系统软硬件运行状态监控、系统数据库备份和恢复等。

i） 应具备可移植性，运行在不同的操作系统平台，支持集中、分布式部署。

j） 应具备先进性，能够最大限度地适应未来网络发展和业务发展的需要。

8.4.4 系统接口

提供运行服务支撑系统的具体系统接口要求如下：

a） 应提供与电子政务公共平台基础设施、支撑软件、信息资源、应用功能的管理接口。

b） 应提供与呼叫中心系统的集成接口。

c） 应提供与业务应用监控的接口。

d） 应提供与公共平台服务运营系统的接口。

e） 应提供与第三方产品对接的接口：

1） 支持通用的网络产品和安全产品；

2） 支持存储、备份以及其他类型设备；

3） 支持安全信息和审计信息输出的接口。

f） 应提供与其他电子政务公共平台监测系统的互联接口。

g） 接口的具体技术要求按照 GB/T 33780.3—2017 执行。

中 华 人 民 共 和 国
国 家 标 准
基于云计算的电子政务公共平台管理规范
第 3 部分：运行保障管理
GB/T 34077.3—2021
*
中 国 标 准 出 版 社 出 版 发 行
北京市朝阳区和平里西街甲 2 号(100029)
北京市西城区三里河北街 16 号(100045)
网址：www.spc.org.cn
服务热线：400-168-0010
2021 年 3 月第一版
*
书号：155066·1-65772

GB/T 34077.3-2021