ICS 35.020
CCS L 70

DB3502

福 建 省 厦 门 市 地 方 标 准

DB3502/T 176—2025

信息系统集成工程服务规范

Information system integration enginering service specification

2025－04－09 发布　　2025－04－09 实施

厦门市市场监督管理局　　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。

本文件由厦门市信息系统集成行业协会提出。

本文件由厦门市工业和信息化局归口。

本文件起草单位：厦门市信息系统集成行业协会、厦门银江智慧城市技术股份有限公司、厦门柏事特信息科技有限公司、厦门精图信息技术有限公司、国投智能（厦门）信息股份有限公司、厦门卫星定位应用股份有限公司、厦门兆翔智能科技有限公司、厦门信息港建设发展股份有限公司、厦门理工学院、厦门海洋职业技术学院、厦门市标准化研究院。

本文件主要起草人：陈瀚、肖碧强、李童、涂少波、陈钰、张志辉、饶小炜、李钊茜、王文慧、卢俊文、蔡裕成、吕鑫、俞辉、高东伟。

信息系统集成工程服务规范

1 范围

本文件规定了信息系统集成工程的建设、验收及运维要求。

本文件适用于新建、扩建的信息系统集成工程的建设、验收工作，正式投入使用的各类信息系统集成平台的运维服务工作及运维服务评价工作。

本文件不适用于涉密信息系统集成项目。

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 2887 计算机场地通用规范

GB/T 8567 计算机软件文档编制规范

GB/T 18336（所有部分） 网络安全技术 信息技术安全评估准则

GB/T 18905.6 软件工程 产品评价 第6部分：评价模块的文档编制

GB/T 20269 信息安全技术 信息系统安全管理要求

GB/T 20270 信息安全技术 网络基础安全技术要求

GB/T 20271 信息安全技术 信息系统通用安全技术要求

GB/T 20274.1 信息安全技术 信息系统安全保障评估框架 第1部分

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GB/T 22240 信息安全技术 网络安全等级保护定级指南

GB/T 25000（所有部分） 系统与软件工程 系统与软件质量要求和评价（SQuaRE）

GB/T 25070 信息安全技术 网络安全等级保护安全设计技术要求

GB/T 39786 信息安全技术 信息系统密码应用基本要求

GB 50174－2017 数据中心设计规范

GB 50311 综合布线系统工程设计规范

GB/T 50312 综合布线系统工程验收规范

GB 50314 智能建筑设计标准

GB 50343 建筑物电子信息系统防雷技术规范

GB 50606 智能建筑工程施工规范

GB 51348 民用建筑电气设计标准

09DX001 建筑电气工程设计常用图形和文字符号

03X801－1 建筑智能化系统集成设计图集

3 术语和定义

下列术语和定义适用于本文件。

3.1

信息系统集成 information system integration

以计算机技术、数据库和通信技术为主要手段建立的信息采集、处理、存储、传输、应用及信息安全保障的系统。信息系统集成工程包括各信息系统的新建、扩建，但不包括零星的设备添置。

4 缩略语

下列缩略语适用于本文件。

BMC：基板管理控制器（Baseboard Management Controller）

DDOS：分布式拒绝服务攻击（Distributed Denial of Service）

FC：光纤通道（Fibre Channel）

HBA：主机总线适配器（Host Bus Adapter）

IDS：入侵检测系统（Intrusion Detection System）

IIS：互联网信息服务（Internet Information Services）

iSCSI：互联网小型计算机系统接口（Internet Small Computer System Interface）

LUN：逻辑单元号（Logical Unit Number）

PCI：外设部件互连总线（Peripheral Component Interconnect）

RAID：磁盘阵列（Redundant Arrays of Independent Disks）

SLA：服务级别协议（Service Level Agreement）

UID：用户身份证明（User Identification）

5 建设要求

5.1 项目建设规划

项目建设规划包括但不限于下列内容：

——应分析相关政策、法律法规、周边社会环境、项目目标、原有系统存在的问题、信息系统实际工作中需要解决的问题、相关技术及发展趋势等，明确项目建设的意义、必要性和可行性；

——应基于项目现状、问题及需求分析，确定项目建设范围，包括明确的需求和潜在的需求，避免、减少项目实施的过度变更；

——项目需求分析宜包括项目风险管理、项目建设的资源及项目运营/维护方面的需求，依据国家相关规定或标准规范确定防护级别或防护要求，并进行系统功能需求及安全需求的分析，提出建设内容以及信息系统系统基本框架和主要功能，对于改建项目应对原有系统进行评估和分析，列出原有系统清单并确定拟利用或改造清单。

5.2 信息系统集成项目设计

5.2.1 设计依据

设计依据包括但不限于下列内容：

——项目相关的政策法规文件和标准规范；

——项目建设的相关立项文件、审批文件、评估报告、经批准的项目可行性研究报告、专家论证会议纪要、现场勘察报告、设计任务书、设计合同书等；

——建设单位提供的原有建设情况相关资料；

——其他依据。

5.2.2 设计要求

设计要求包括但不限于下列内容：

——项目建设的概况、现状描述、需求分析、总体原则、设计依据；
——项目设计理念，包括项目的技术路线、设计指导思想、设计目标和设计遵循的基本原则等；
——项目建设的可量化、可考核目标，包括建设目标、建设规模、建设内容及建设周期等；
——系统的整体功能与性能要求及系统点位总体规划；
——系统的整体框架描述，包括系统建设的基本内容和基本组成等；
——系统基础环境设计，包括设备环境监测与控制、供配电及防雷接地等；
——系统硬件设计，包括系统核心设备及终端、数据存储中心、网络通信和传输等；
——系统定制软件设计，简述软件架构、功能、选型等；
——系统安全设计，包括系统安全等级、系统安全域划分、安全策略、安全解决方案和主要软硬件设备选型等；
——系统集成设计,包括系统软、硬件各子系统的集成及相关数据信息资源整合，明确相应的集成接口和通讯协议；
——与其他相关系统对接协调融合关系；
——改/扩建项目应说明改/扩建的内容、范围及与原有信息系统的接口和集成关系。

5.2.3 设计内容

5.2.3.1 基础环境设计

基础环境设计包括但不限于下列内容：

——机房基础环境设计涉及机房供配电/照明系统、机房通风空调及环境监测系统、机房安防设施、机房消防设施、机房防雷接地系统等；
——基础环境设计应符合 GB 50174、GB 50314 的相关要求，其中 UPS 不间断电源容量及应急供电时间应符合 GB 51348 的相关要求，防雷接地设施应符合 GB 50343 的相关要求；
——设备环境监测及控制设计，包括设备环境中照明、温湿度、电磁环境的监测及控制，明确相应的照明、空调、电磁监测等系统设备的配置及性能指标；
——供配电设计，应说明终端设备的供电负荷、供电要求、供电原则、供电方式、电缆选型、管槽规格、敷设方式和电费计量分析等；
——防雷设计，应根据终端防雷要求选择雷电防护措施，确定防护终端与传输的防雷设备选型、性能指标及数量；
——接地设计，应根据终端接地电阻要求选择接地方式和接地来源，建设接地装置的应详细说明接地方案及接地设备与材料的选型、性能指标及数量。

5.2.3.2 硬件设计

硬件设计包括但不限于下列内容：

——核心设备包括系统服务器及相应的存储设备、通讯设备，明确相关设备数量、配置及性能参数，对存储设备应详细描述存储方案；
——终端设备应依据信息系统勘察情况及系统终端设备安全技术要求进行设计，包括终端设置分析、终端点位布设、设备选型及主要技术参数等；
——网络传输设计应符合 GB 50314、GB 50311、GB/T 22239 的相关要求，形成网络拓扑图，详细说明各级传输采用的传输路由、传输方式、传输带宽、传输资源、安全策略、管线规格数量及敷设方式，配置主要网络设备及网管设备等。

5.2.3.3 定制软件设计

对于信息系统集成需求而定制的软件，软件的名称、架构、功能、实现方法、性能指标、接口设计、运行环境、安全措施、升级/更新等应符合GB/T 18905.6及GB/T 25000系列标准要求，主要包括但不限于下列内容：

——定制软件的运行平台、应用环境应符合相关行业或领域的信息技术应用创新要求，如处理器芯片、操作系统、数据库管理系统和中间件等的设计；

——定制软件采用的技术路线、开发手段的规范；

——定制软件总体架构、功能模块等的设计；

——定制软件配置和部署方案设计；

——定制软件需求规格说明书、概要设计说明书、详细设计说明书、数据库设计说明书、接口设计说明书等文档应符合 GB/T 8567 的相关要求并经相关方确认。

5.2.3.4 系统安全设计

应依据 GB/T 22239、GB/T 22240、GB/T 25070、GB/T 39786 等相关标准的要求，以及信息系统集成项目的整体规划和系统总体架构进行信息安全防御体系的规划和设计，主要包括：

——信息安全防御体系的安全策略，包括安全级别、安全机制、安全服务等；

——评估信息安全防御体系的安全风险，规划安全架构；

——应考虑安全产品的参数、性能、功能等选择的可靠性、可用性和安全性；

——实体安全应根据系统相关的场地、环境、线路、设备、媒介等的安全与服务集成进行衔接；

——系统平台安全包括操作系统、数据库系统、系统支撑软件、协议簇等的安全；

——数据安全包括数据存储、数据管理、数据交换等安全；

——应用系统安全为基于系统平台运行的各类软件系统的安全；

——传输安全包括数据传输链路、网络等的安全；

——所有安全等级的信息系统集成项目均应建立密码应用安全管理制度并制订密码应用方案，根据相关标准中安全级别的要求选配相应的具备密码安全功能的硬件、软件或固件；

——数据安全、传输安全、应用安全评估。

5.2.3.5 系统集成设计

信息系统集成设计是在需求分析基础上，以项目业务流程为核心，满足系统的各项技术要求，强调系统的实用性，兼顾技术上的先进性、扩展性，采用规范化设计，降低系统的技术复杂度，达到设计功能和性能的同时，尽可能减少建设及运营维护成本。系统集成设计主要包括但不限于下列内容：

——总体框架设计：通过文字和图表描述信息系统集成整体框架，包括本单位系统内部结构和与外部系统间的联系，区分出已建系统及功能和新增系统及功能，绘制系统集成或数据集成的总体架构图；

——业务功能设计：详细描述各子系统及业务功能之间通过数据交换服务协议、软硬件接口互联互通，实现集中管理及系统、设备间联动或互锁的要求；

——数据接口集成设计：详细描述各子系统的业务数据之间通过技术协议或其他手段进行的数据交互；

——其他系统集成设计：根据项目需求和特点提出除上述系统建设以外的其它系统集成设计。

5.2.4 设计图纸

系统及工程设计图纸包括但不限于图纸目录、设计说明、图例、总平面图、系统图、设备器材平面布置图、点位示意图等，工程设计图纸应符合GB 50311、09DX001、03X801－1等相关标准的要求，并符合下列要求：

——图纸应清晰、准确、详细、完整体现应绘制内容；
——改扩建项目应在在平面布置图中将原有设备器材与新增设备器材予以区分；
——对于重要防护区域、防护目标集中的区域，应绘制局部的设备器材平面布置图；
——对安装部位、管路敷设有特殊要求的，可根据需要提供安装示意图、局部大样图等工艺性图纸；
——设备连接图应包含线缆编号、信号走向等内容；
——图纸应有相关人员签字，设计单位盖章。

5.2.5 设计评审

信息系统集成工程设计完成后，宜由建设单位组织行业专家组成评审小组进行设计评审，设计评审应包括下列内容：

——对工程设计与相关法规、标准要求及建设单位建设需求的符合性进行综合评价；
——如设计存在缺陷或存在疑义的，应对缺陷导致的风险、损失进行分析或要求设计单位予以说明，并对相应的缺陷提出修正、完善的意见和建议；
——对施工/部署方案及施工工期的合理性提出意见和建议；
——对技术方案、图纸、工程量清单及其它文档资料的完整性、合理性及规范性提出意见和建议。

5.3 信息系统集成项目实施

5.3.1 项目实施总体要求

在项目实施中，应整合用户管理、业务、技术、设备、人员等及其相互关联的各类资源，以及与外部关联的资源，按照系统整体设计原则，确定资源整合、配置及资源管理规划，合理划分资源类型和分布，优化配置项目涉及的各类资源，以最大限度满足项目的资源需求和信息系统建设需求。

5.3.2 项目实施准备

项目实施准备主要包括但不限于下列内容：

——项目人员准备：应成立项目部或项目组，应明确项目经理、项目技术工程师、现场管理人员、安全员、材料员、资料员等相关人员配备及工作职责；
——设计交底及现场勘察：应组织实施项目现场勘察，勘察内容主要包括机房、弱电间、强电间等各处系统设备安装及管线敷设的环境条件，应了解土建、装修、机电、暖通空调等相关专业现场施工初步情况，设计交底前项目经理应提前熟悉相关标准规范及设计文件，对未明确事宜形成记录及处理意见；
——实施方案及进度计划：应根据项目建设工期和建设各阶段的划分，组织编制项目实施方案及各阶段进度计划，包括项目实施所需资源、环境条件及各项质量、进度、成本管理措施；
——设备材料准备：根据项目实施方案及进度计划，明确相关设备材料的采购、到货周期，制订采购计划，确保设备材料及时到货；
——施工机具/工具准备：根据项目实施方案，明确项目实施各阶段施工机具、仪表及软件测试工具的明细清单，相应的机具、仪表及软件测试工具分阶段准备到位。

5.3.3 项目实施管理

项目实施管理主要包括但不限于下列内容：

——质量管理：项目质量管理涉及质量策划、检测/检验、问题纠正及改进等，应制定相应的实施质量标准并对相关人员进行交底，按不同区域、不同系统分阶段进行检测/检验，对检测/检验中发现的问题，应制定整改方案及预防同类问题发生的措施；

——安全管理：项目安全管理涉及现场安全风险识别、制定安全风险控制措施、项目实施团队的安全教育及安全交底、现场施工人员和机具的安全管理、施工安全检查等，对发现的安全隐患应提出纠正措施并落实，对可能发生的安全事故，应制定事故处理预案并按相关要求定期演练；

——进度管理：应按进度计划制定相应的进度管理措施，分析影响项目进度的不同因素，包括设计因素、组织因素、设备材料因素、现场实施环境/条件因素等，列入相应的进度销项表，对相关问题安排人员限期解决，定期对进度计划与实际进度偏差进行分析，采取适当的措施进行纠偏；

——成本管理：应复核设计阶段的工程概算及工程预算，从人员薪资、设备材料成本、机具/工具使用成本、现场管理费用等方面制定相应的成本控制目标及措施，对因项目变更造成的成本变化，应与项目各相关方制定变更流程及确认手续，保留相应的变更资料作为项目结算依据；

——变更管理：在项目设计文件及实施合同确定的项目实施范围基础上，因用户需求变化或项目设计本身存在可优化的因素需要进行变更的，用户与项目实施方宜在项目实施合同中根据变更原因及变更内容对系统架构、功能及成本的影响约定相应的变更类别，明确不同的变更要求及相关方审批流程，在项目实施中按相应的变更类别和审批流程执行，对原合同中未明确的变更，可经相关方评估变更的影响，经协商后按约定的要求和流程实施；

——风险管理：根据防护目标的防护级别及信息系统集成的需求，进行风险识别、分析和评估，其中风险识别和分析包括政策风险、系统风险和操作风险，针对项目可能存在的风险提出应对风险的对策和风险管理措施；

——文件资料管理：应对项目设计文件、图纸及实施过程中涉及质量、进度、成本的文件资料和记录归档保存，与项目相关方制定收发文流程及手续，确保项目文件资料与项目实施状态的一致性。

5.3.4 系统试运行及售后培训

系统试运行及售后培训主要包括但不限于下列内容：

——信息系统集成项目各系统完工后，应组织对各系统试运行，试运行时间不宜少于 30 天，试运行应做好相关的试运行记录，出具系统试运行报告，试运行报告应包括项目各系统简介、试运行期间各系统运行基本情况、故障处理情况等内容；

——系统管理/使用单位入驻后，可组织对管理/使用单位相关人员进行培训，包括系统基础知识、前端设备分布情况、系统实际操作及各级管理权限等，系统培训宜保留相应的培训记录，宜对受训人员的相关知识和实际操作情况进行测验。

6 验收要求

6.1 验收依据和标准

工程验收依据和标准主要包括但不限于下列内容：

——工程立项文件、合同、招投标文件、正式设计文件、变更文件等；

——硬件、软件、布线、信息安全、网络等领域的各级相关标准等。

6.2 验收前提条件

项目验收前提条件包括：

——相关国家标准规定的强制性要求已完成；
——建设的信息系统的功能、性能、安全等技术指标符合合同及设计要求；
——承建单位已完成自验，并按合同要求完成规定时间的试运行；
——各分项工程全部验收合格；
——外购的操作系统、数据库、中间件、应用软件和开发工具符合知识产权相关法律法规的要求；
——已完成对使用单位相关人员的技术培训，系统的主要使用人员应能够独立操作使用；
——工程建设的文档资料齐全、规范，文档资料要求见 6.4.2.1；
——监理报告已编制完成；
——工程建设中网络安全建设内容已进行了网络运行安全保护和网络信息安全保护；
——已按 6.3.2 要求完成相应的第三方测评；
——承建单位已提出验收申请。

6.3 验收流程

6.3.1 验收准备

承建单位进行验收准备内容包括：

——各种设备经试运行，状态正常；
——系统已按合同规定的时间稳定试运行，承建单位编制项目试运行报告；
——按照合同的要求，完成并提交技术文档及工程实施管理资料；
——向建设单位提交验收申请。

6.3.2 验收测评

依据相关标准规范，项目建设内容中涉及强制要求进行功能及安全测评的，建设单位应委托第三方检验（测评）机构进行相应测评，测评费用由建设单位承担。第三方检验（测评）机构进行工程验收测评的主要步骤包括：

——检验（测评）机构在接到委托后与建设单位签订测评合同，并按照工程要求编制测评方案，测评检测要求见附录 A，测评实施前将测评方案提交给建设单位，建设单位组织对测评方案进行评审；
——检验（测评）机构根据评审后的测评方案实施测评；
——检验（测评）机构完成验收测评后，将测评报告提交给建设单位和承建单位，如测评未通过，承建单位应经过整改后再次申请验收测评，测评费用由承建单位承担。

6.3.3 验收会议

建设单位收到检验（测评）机构的测评报告后，组建验收组，召开验收会议，验收组织和评审费用由建设单位承担。验收会议主要步骤包括：

——建设单位作关于工程情况的报告；
——承建单位作关于工程建设情况、自检情况及竣工情况的报告；
——监理单位作关于工程监理内容、监理情况以及项目竣工意见的报告；
——检验（测评）机构作项目测评情况的报告；
——建设单位作试运行情况的报告；
——验收组进行现场检查(根据具体项目情况选择)；
——验收组对关键问题进行抽样复核和资料评审；

——验收组对项目进行全面评价，形成验收意见和验收结论并签字。

6.3.4 初验

初验的验收条件为项目完成合同约定的功能，系统试运行正常，文档齐全。初验主要验收内容包括功能完整性、系统性能、文档资料、用户培训与试运行情况等。

6.3.5 终验

终验的验收条件为初验合格，系统稳定运行，所有问题整改完成。终验的验收内容包括功能完备性、性能稳定性、安全与合规性、用户满意度等。

6.3.6 验收交接

工程验收交接内容包括：

——工程验收通过后，建设单位将验收文档资料作为工程档案进行存档；

——承建单位向建设单位办理工程交接。

注：项目涉及的项目实体及有关设备等资产根据合同的约定进行交接，交接双方应在移交清单上签字确认。

6.4 验收的组织

6.4.1 验收组构成

验收组由建设单位根据相关要求组织成立，宜由相关行业专家担任验收组成员。

6.4.2 验收组任务

6.4.2.1 资料审查工作

资料审查工作主要对项目的相关资料进行评审，检查资料是否齐全、规范、正确。审查资料包括但不限于以下内容：

——总结资料：工程概要、验收文档概要说明；

——工程立项审核资料：立项审核申请、项目建设方案；

——工程变更资料：项目变更申请、项目变更审批文件；

——工程经费资料：概算、预算、经费使用情况表；

——合同资料：招标书、投标书、合同文件；

——工程施工资料：工程说明、合同范围的设备清单、工程开工报告、施工组织方案、系统技术方案、安全策略文档、设备进场记录及到货验收资料、工程量总表、设备移交清单、设备明细及位置、数据资源录登记表及数据汇聚情况报告、施工过程文档（隐蔽工程验收及检验批、分项、分部/子分部验收资料）、设备自检自测记录、设备安装工艺检查情况表、系统功能检测记录、项目变更资料、重大工程质量事故报告、试运行报告及问题整改记录、项目自评及初验报告、系统测试报告（含第三方软件测评、信息安全风险评估、信息安全等级保护测评、密码应用安全性评估报告等）、用户手册、随机技术资料、系统安装配置手册、系统维护手册 （管理员级）、系统日常维护及应急处理方案、竣工验收申请报告、用户试用报告或用户意见书、用户培训资料（培训教材、培训记录等）；

——信息应用系统相关文档：需求说明书、概要设计说明书、详细设计说明书、数据库设计说明书、测试计划、测试报告、用户手册、项目计划书、用户培训计划、会议记录和开发进度月报；

——工程监理报告。

注：软件开发类项目的文档资料包括软件需求说明书、概要设计说明书、详细设计说明书、数据库设计说明书、软

件验收测试报告等，文档资料应符合GB/T 8567的要求。

6.4.2.2 工程评审工作

工程评审工作主要包括听取建设单位、承建单位、监理单位对项目建设情况的介绍，组织现场检查以及听取资料审查的情况汇报，用户试运行情况的汇报。评审的内容包括：

——工程的实施过程是否符合规范；
——工程是否达到合同书的各项指标与要求；
——技术文档是否齐全，是否符合国家或有关部门的技术要求；
——运行管理人员和操作使用人员的技术培训是否达到合同要求。

6.5 验收结论与处理

6.5.1 验收结论

验收结论分为验收合格和验收不合格。

6.5.2 验收合格

满足以下所有条件，为验收合格：

——验收文档资料齐全、正确；
——工程变更通过审核；
——工程设计和合同约定的各项内容都已实现；
——工程已经通过检验（测评）机构测评，且测评结果合格；
——运行管理人员和操作使用人员已完成培训。

6.5.3 验收不合格

工程具有下列情况之一的，为验收不合格：

——工程变更未经审核，工程的内容、工程或技术路线等已进行较大调整，未得到建设单位认可；
——未按工程考核指标或合同要求达到预定的主要技术指标；
——所提供的验收材料不真实；
——实施过程中出现重大问题，尚未解决和作出说明，或工程实施过程及结果等存在纠纷尚未解决；
——经检验（测评）机构测评，测评结果不合格。

6.5.4 工程验收结论处理

工程验收结论处理分为：

——验收结论为验收合格的，进行工程交接和资料交接；
——验收结论为验收不合格的，限期整改，整改后重新申请验收。

7 运维要求

7.1 基本规定

7.1.1 一般要求

7.1.1.1 建设/使用单位要求

7.1.1.1.1 建设/使用单位应提供相应的技术资料包括但不限于：

——项目需求说明书；
——项目设计说明书；
——数据字典；
——系统使用手册；
——系统测试报告；
——系统部署文档；
——系统常见问题说明。

7.1.1.1.2 涉及集成平台管理子系统，建设/使用单位应提供 7.1.1.1.1 中相应技术资料及子系统相关资料，子系统相关资料包括但不限于：
——系统设备移交清单及点位表；
——图纸资料，包括系统原理图、平面图、设备接线图、安装大样图等；
——子系统产品说明书、产品手册及维护手册；
——子系统软件及部分系统的软件设置工具、系统备份数据；
——子系统测试记录和各主要设备运行记录；
——子系统供应商、集成商及分包商通讯录；
——子系统其它验收相关资料。

7.1.1.2 运维供方要求

7.1.1.2.1 运维供方可由项目实施单位、专业维保单位、物业管理单位、相关设备供应商根据实际情况联合组建，运维服务人员应包括专业技术维护人员、用户系统技术管理人员、系统运行操作人员等。
7.1.1.2.2 由专业维保单位和物业管理单位联合组建的运维供方，专业维保单位和物业管理单位应签订维保协议，约定维保责任、服务模式和服务等级。
7.1.1.2.3 服务模式宜根据项目的业态和重要性，从服务方式、服务时间、巡检频次、故障/事件响应、解决时间等分为不同等级。
7.1.1.2.4 运维供方在工作实施前应进行技术资料审查并现场勘察复核，现场勘察复核情况与技术资料不符，应由移交单位说明原因，对技术资料进行修订或另行书面补充说明。
7.1.1.2.5 运维供方应核查项目各系统备品备件，明确型号规格及数量。
7.1.1.2.6 运维供方在工作实施前应对系统进行移交测试，测试内容应根据项目实际情况和运维工作内容制订，包括但不限于：
——功能测试：验证系统各项功能，查看菜单执行情况、帮助信息及特殊控件是否正常运行；
——可靠性测试：检测系统在规定时间、条件下持续运行的能力以及系统异常警示机制，不应存在无法运行、崩溃或数据严重破坏的情况；
——安全性测试：根据项目的安全需求测试安全防护策略的有效性，包括系统入侵防护、应用防护、漏洞扫描、数据存储、传输和访问的安全机制等；
——可维护性测试：系统应有维护专用登录账号、相关数据查询手段、检查诊断系统故障工具和手段，测试《系统常见问题说明》中常见故障处理手段的可操作性。
7.1.1.2.7 系统基础环境及相关硬件、接口设备的运维应由相关设备供应商、服务商提供技术保障。

7.1.2 运行维护工作内容

7.1.2.1 日常巡检

日常巡检内容包括但不限于：
——依据运行维护方案，制定日常运行巡检计划、问题管理计划等；

——日常巡检内容包括检测系统工作状态、监测系统运行效率、系统运行问题的处理等，巡检要求见附录 B；
——进行运行基础数据采集、整理、分析，填写相关巡检记录表见附录 D，形成相关报告，如日常监测报告、状态监测报告、常规维护报告等；
——对应用系统进行系统和数据的备份与恢复，填写备份/恢复记录；
——发现并记录运行过程中产生的问题，形成问题清单，提交给维修人员；
——根据巡检情况，对系统运行情况、环境情况进行总结和分析，提出调整、整改意见。

7.1.2.2 系统维修

系统维修内容包括但不限于：
——根据运维协议中的故障等级、处理方式、响应时间和处理时间进行维修；
——系统运行中故障的诊断、处理，故障/事件宜划分为 4 个等级，等级定义见表 1；
——故障维修要求见附录 C；
——分析故障原因，提出防患措施；
——形成维修报告，维修报告内容应包括故障原因、责任及处理措施、更换的备品备件等；
——对系统经常出现的故障进行统计、分析，提出系统性能优化建议。

表1 系统故障/事件等级定义

故障/事件级别	定义	备注
1级	系统运行期间出现的重大故障，导致系统瘫痪，业务中断或基本功能无法实现。	系统服务器瘫痪或网络整体瘫痪，系统功能无法实现。
2级	系统运行期间出现潜在危险，可能导致系统业务中断或功能性能全面退化。	系统较多前端设备不在线或故障，或系统工作站/服务器故障、部分网络中断导致功能无法实现。
3级	系统运行期间出现的故障，部分或间接影响系统性能或部分功能，不会造成业务中断。	系统较多前端设备不在线或故障，或系统工作站/服务器故障、部分网络中断但未影响系统运行。
4级	系统运行期间出现的偶发故障，不影响或较少影响系统性能或相关业务运行。	系统少量前端设备故障，或系统工作站软硬件故障但未影响系统运行。

7.1.2.3 系统优化升级

系统优化升级内容包括但不限于：
——依据运行维护的情况及出现的问题，制定运行维护阶段的系统优化升级方案，确定系统优化升级的目的、功能和实施方法；
——优化升级服务内容超出项目原维保协议范围的，宜另行签订维保协议；
——根据实际情况以及用户需求，在不影响应用系统的正常使用情况下，按相应的优化升级方案进行应用系统升级；
——辅助用户完成升级后的系统重新部署。

7.1.2.4 运维培训

运维供方应定期组织对运维工程师及运维需方的系统日常操作人员、管理人员的培训，培训内容包括但不限于：
——系统架构、设备部署及当前状态；
——日常管理、操作要求；
——系统异常或故障的记录、上报、处置要求；

——系统扩展、优化后的新设备或新功能。

7.1.3 运行维护服务等级与服务考核

7.1.3.1 运维服务等级及服务目标

运维供方通过对运维服务需求的识别、获取及分析，结合项目规模及项目运维资金情况，确定服务级别需求和目标，作为编制服务等级协议（SLA）的依据。系统服务等级宜根据服务方式、服务项目/业态等分为四个等级，相关要求见表2。

表2 系统 SLA 服务等级

服务级别	服务方式	服务说明	主要服务项目/业态	服务时间	巡检频次	故障/事件级别	响应时限	解决时限
一级	驻场+现场响应	安排常驻人员以外对用户的重大活动或事件增配人员支持	政府机关、车站/机场、三甲医院等	7*24	每周≥1次	1级	30分钟	4小时
						2级	30分钟	4小时
						3级	30分钟	4小时
						4级	1小时	4小时
二级	驻场	至少安排1人常驻现场进行巡检及故障处理	医院、酒店、办公楼/商业综合体、工厂等	5*24	每月≥1次	1级	30分钟	4小时
						2级	30分钟	6小时
						3级	1小时	8小时
						4级	1小时	8小时
三级	远程+现场	针对巡检或故障处理等任务到现场支持	高端住宅、办公楼/商业综合体、酒店等	5*8	每季度1次	1级	2小时	8小时
						2级	2小时	16小时
						3级	4小时	24小时
						4级	4小时	24小时
四级	远程	通过电话指导或远程桌面操作进行支持服务	普通住宅、办公楼等	5*8	每季度或半年1次	1-2级	4小时	24小时
						3级	8小时	48小时
						4级	8小时	72小时
注：SLA一级～三级参照厦门市工业和信息化局及厦门市财政局发布的《关于印发厦门市政务信息化项目造价评估规范（试行）的通知》中运维等级。								

7.1.3.2 服务等级协议（SLA）拟制及签订

服务等级协议（SLA）应通过运维需方和运维供方共同组织的评审，经过协商修订，作为运维协议附件进行签订，SLA应包含服务内容和范围、服务时间、服务级别目标、服务指标等。

7.1.3.3 客户回访及满意度调查

客户回访及满意度调查主要包括：

——运维供方宜定期对运维需方进行回访，可采用电话回访、电子邮件及现场走访等形式，客户满意度调查宜以电子邮件方式发送客户满意度调查表；

——定期调查运维需方对维保工作整体满意度情况，根据调查结果现场核实并予以整改；

——客户满意度调查的内容包括维保工作的计划及时性、现场及维修热线接收人员的服务态度/礼节礼仪、故障维修响应速度、故障原因等；

——客户回访及满意度调查宜半年 1 次或一年 1 次。

7.2 基础环境运行维护

7.2.1 一般规定

基础环境运行维护一般规定包括:

——基础环境运维对象符合本文件 5.2.3.1；

——机房依照 GB 50174－2017 划分为 A、B、C 三个等级；

——A 级数据中心机房每日现场巡检次数应不少于 2 次，B 级和 C 级数据中心机房每日现场巡检次数应不少于 1 次；

——基础环境设施巡检要求见附录 B；

——基础环境设施维修要求见附录 C。

7.2.2 基础环境改扩建及搬迁

7.2.2.1 准备阶段

机房改建、扩建及搬迁准备阶段主要包括：

——制定机房改建、扩建及搬迁实施方案；

——完成改建、扩建或搬迁后机房基础环境设计，明确利旧设备和新增设备的清单明细；

——对拆换、利旧设备分类并准备标识标签，利旧设备的标识标签号宜体现在安装、排布图纸上；

——准备实施工具，包括钻孔/开孔机具、高处作业机具、切割工具、线缆及模块加工工具、设备拆卸/安装工具、检测及调试工具等，列出完整工具清单；

——制定数据备份及恢复方案，数据备份恢复的要求见 7.4.3.3；

——制定拆换设备的安全运输措施，准备好包装、保护材料及临时存放场所。

7.2.2.2 设备拆除及安装阶段

7.2.2.2.1 拆卸设备前关机、断电

在准备工作完成后，应依次对机房设备关机，断电时应断开机柜内设备电源，再切断机房配电系统对应负载回路，要求包括但不限于：

——切断电源前，确认设备已完全关闭，部分设备应待风扇完全停转后切断电源；

——停机顺序按照先停运业务系统，再停运数据库、存储系统、备份系统、网络系统的原则进行；

——设备停机时应按不同业务系统有序停机，根据业务系统软件停运注意事项，按照系统软件停运步骤进行操作；
——系统停机时如发生软件或系统故障，应先排除故障再进行停机操作；
——切断电源时应先关闭电源插座，再拔下设备电源线。

7.2.2.2.2 设备/机柜拆除

设备/机柜拆除要求包括但不限于：
——设备下架时，应严格按照设备安装和拆卸指南进行；
——设备下架时，应严格遵守设备的放置要求，杜绝将设备倒置、倾斜等随意堆放；
——设备及机柜拆除应先拆卸设备周边连接附件及线缆，再拆卸主机；
——设备下架时，应由上自下，对机柜内设备进行逐一拆除；
——拆卸存储柜、核心交换机等体积和重量较大设备时应注意对设备保护，确保设备和人员安全。

7.2.2.2.3 设备安装

设备安装要求包括但不限于：
——设备安装应符合 GB 50606 中的相关要求；
——安装应前做好技术、安全交底；
——安装前应检查设备接口及组件，确保无故障、损伤；
——安装过程中应采取防静电措施，佩戴防静电手环或在操作前洗手以释放操作人员身上静电荷；
——安装过程中保证设备接地，机柜柜体连接到接地排，柜门与柜体用黄绿线连接。

7.2.2.3 系统试运行阶段

系统试运行阶段要求包括但不限于：
——通电及数据恢复：设备加电前，应对机房供电系统进行检测，确保供电系统正常，设备电缆连接就位，设备加电后，检查系统设备及网络是否处于运行状态，按数据备份及恢复方案进行数据恢复；
——系统检测：设备加电后，检测网络路由及通畅情况，按照网络拓扑结构，对相应的网络设备，进行配置，通过网络管理软件或远程登录系统检测系统运行状态；
——系统试运行：完整记录系统软、硬件及基础环境设施运行情况，及时发现问题并进行处理，试运行宜持续不少于 30 天。

7.2.2.4 验收移交阶段

系统验收、移交见第6章。

7.3 设施设备运行维护

7.3.1 服务器运行维护

7.3.1.1 一般规定

服务器运行维护一般规定包括但不限于：
——服务器巡检准备工作：应掌握服务器 CPU、内存、硬盘、电源、网卡、显卡及其它扩展设备的配置情况及相应的运行指标，熟悉服务器各类端口和状态指示灯的状况；
——服务器巡检要求见附录 B；
——服务器故障维修要求见附录 C。

——有备份服务器的系统，进行服务器故障维修时应启用备份服务器以保证系统正常运行。

7.3.1.2 优化升级

服务器硬件升级应根据当前系统运行中存在问题和相关业务变化、更新、拓展需求制订相应的升级方案，主要包括但不限于：

——CPU 升级，根据服务器硬件架构、CPU 的接口及最大可支持的 CPU 数量以及当前 CPU 升级空间确定 CPU 升级配置方案；

——内存升级，根据服务器的相关技术参数，确定服务器可支持的内存最大容量；

——网卡升级，应根据服务器硬件兼容性进行网卡升级；

——存储系统升级，应根据存储容量、读写速度和数据安全性的需求，择存储系统升级模式，包括容量扩充、RAID 阵列调整和存储系统架构优化等。

7.3.2 网络设备运行维护

7.3.2.1 一般规定

网络设备运行维护一般规定包括但不限于：

——网络设备巡检准备工作：掌握网络设备的基本情况包括设备名称、IP 地址、位置、功用、序列号、各设备模块种类及型号及设备软件版本，设备性能基准参数包括 CPU 及内存参数、设备端口流量的初始数据及计数器初始状态等，相关数据可通过手动输入命令、专用工具或网络管理平台等方式进行采集；

——网络设备巡检要求见附录 B；

——网络设备故障宜采用分段或分层方式进行排查、处理，各层主要故障及维修要求见附录 C。

7.3.2.2 优化升级

网络设备优化升级应根据用户业务需求变化及当前网络运行状况进行需求分析，提出网络设备优化目标，制订优化升级方案，包括相关软硬件配置、实施流程及相关资源和预算要求，网络设备升级前应对现有网络运行数据、日志进行备份。网络设备优化升级主要包括但不限于：

——网络系统性能提升及规模扩展，主要包括网络带宽扩容及相关设备交换能力提升；

——网络管理、维护提升，主要有采用网络拓扑管理、配置管理、性能监测及事件管理等网络管理工具、设备，采用虚拟化技术将网络设备合并，减少日常网络管理的节点等；

——网络可靠性提升，提升网络的容错能力，冗余设计优化，网络系统冗余设计主要有：

- 核心设备引擎冗余及双机热备；
- 电源冗余，对核心层和汇聚层设备采用双电源设计；
- 传输链路冗余，包括主干网络的双链路及网络汇聚层双机热备设计；
- 虚拟路由冗余，如采用虚拟路由冗余协议配置VRRP路由器。

——网络安全性提升，对网络系统配备防火墙、漏洞扫描、审计系统等安全设备提升网络的安全监测和防范能力，优化网络拓扑结构，主要包括：

- 内外网进行物理隔离；
- 不同业务、不同需求的用户在网络层进行隔离；
- 网络关键出口处设置防火墙或完善访问控制列表，限定外网与业务系统的交互应用类型；
- 摒除网络中可能旁路绕过安全防护设备的链路。

7.3.3 存储设备运行维护

7.3.3.1 一般规定

存储设备运行维护一般规定包括但不限于：

——存储设备运行维护对象包括面向存储设备中的磁盘阵列、存储用光纤交换机、光盘库、磁带机及网络存储设备等；

——存储设备巡检要求见附录 B；

——维修人员应得到授权后按照解决方案进行存储设备的恢复，操作过程宜进行双人复核；

——维修人员应在不影响业务恢复的同时进行故障信息收集；

——存储设备发生故障过程中，应检查应用系统服务状态、恢复时间和业务影响范围，在存储设备恢复后，进行业务验证工作；

——存储设备内数据存储介质更换，应对更换后的存储介质进行信息消除；

——存储设备故障维修要求见附录 C。

7.3.3.2 优化升级

存储设备优化升级要求包括但不限于：

——存储设备优化升级变更方案应考虑硬件安全、系统安全、数据安全，选择适当的变更方案及时间窗；

——存储设备变更前，根据变更方案准备备品备件及冗余备件，变更过程中对相应线缆进行标记；

——存储设备变更过程中，操作系统配置变更应进行相关配置信息备份；

——存储设备变更开始及结束后，应对存储设备进行检查，对重要配置内容进行变更前后的对比检查；

——存储设备优化升级主要包括：

- 适应性升级，存储设备的读写高速缓存比例调整、RAID级别调整、逻辑盘容量调整、分配主机调整，存储池配置调整以及光纤交换机存储网络区域规划调整；
- 增强型升级，部件的微码升级，存储池的容量扩展，高速缓存容量增加，光纤模块新增、扩容和升级，管理软件的版本升级。

7.3.3.3 备份和恢复

存储设备备份和恢复要求包括：

——存储管理员每季度对存储设备及光纤交换机配置文件进行一次备份，备份保留周期不低于 6 个月；

——存储管理员应在每次变更前后，将备份过的存储和光纤交换设备的配置文件与定期备份数据一同保存。

7.3.4 桌面及其它硬件运行维护

7.3.4.1 一般规定

桌面及其他硬件运行维护的一般规定包括：

——桌面及其它硬件运行维护对象包括C/S或B/S用户界面及相关的工作站、云桌面系统及瘦客户机、移动终端、行业专用终端、输入输出设备等；

——采用移动便携式终端设备登录系统，除登录口令外，宜进行用户身份验证方可访问系统；

——输出设备产生的纸质资料，应建立专项发放、查阅、回收、报废及销毁的管理制度；

——巡检前应掌握桌面及相关硬件的配置、性能及当前运行状态，系统用户分类、分组基本情况，系统用户权限分配状况等；

——桌面及其他硬件巡检要求见附录 B；
——桌面及其他硬件故障维修要求见附录 C。

7.3.4.2 优化升级

桌面及相关硬件设备优化升级应根据用户需求和系统当前运行情况制定相应的优化升级方案，宜同信息集成平台服务器、操作系统及应用软件的优化升级方案进行综合设计，桌面及相关硬件设备优化升级主要包括以下方面：

——用户工作站计算机升级，包括计算机硬件性能升级、操作系统/应用程序版本升级及病毒防护软件版本升级等，升级前应进行运行数据备份；
——云桌面系统升级，包括云桌面服务器性能升级及云桌面管理软件版本升级，云桌面系统升级应与瘦客户机兼容；
——显示及播放设备系统升级，包括显示设备性能、屏幕尺寸升级、监视墙系统扩展及控制模式优化、播放器及相关功放、扬声器性能升级等；
——移动终端应用程序升级，包括软件功能扩展及用户身份验证、登录的安全性优化等。

7.4 软件运行维护

7.4.1 系统软件运行维护

7.4.1.1 一般规定

系统软件运行维护一般规定包括：

——巡检前准备：应掌握系统软件当前版本、服务器 CPU 性能及状态、内存和分配情况、存储配置、网络适配器等信息，配合用户制订系统文件备份策略；
——系统软件巡检要求见附录 B；
——系统软件故障维修要求见附录 C。

7.4.1.2 优化升级

系统软件优化升级应根据用户需求变化及硬件配置情况而进行升级，宜在服务器及软件供应商支持下进行系统软件优化升级。主要要求包括：

——制定系统软件升级计划，包括系统软件升级的策略、流程、时间及资源配置；
——系统的硬件配置及相应的驱动程序应符合系统升级要求；
——操作系统版本和应用程序应与升级后的系统兼容；
——具备稳定的服务器网络环境，网络配置符合系统升级后的要求；
——对系统所有重要的数据和文件进行备份；
——清理过期失效的程序及垃圾文件。

7.4.2 应用软件及接口运行维护

7.4.2.1 一般规定

应用软件及接口运行维护一般规定包括：

——巡检前准备包括：

- 了解集成平台的系统架构、各应用软件的功能及相应的系统接口配置；
- 准备巡检工具和软件，如性能监测工具、日志分析工具、网络分析工具等；
- 收集系统信息，如系统硬件配置、操作系统版本、应用软件版本、网络拓扑结构等；

- 备份系统数据和配置信息；
- 了解当前系统应用情况。

——应用软件及接口巡检要求见附录 B；

——应用软件及接口的故障维修应结合软件的功能、使用方法、配置参数及接口状态等进行故障排查和分析，故障维修要求见附录 C；

——故障处理后应进行相应的检测和验证，形成维修记录和报告，报告内容包括问题描述和分析、维修方法和结果、预防和改进措施。

7.4.2.2 优化升级

应用软件优化升级要求包括：

——优化升级前准备主要有：

- 确定升级版本：根据业务需求和系统状态，选择应用软件升级版本，进行版本验证和测试；
- 制定升级计划：制定升级计划，包括升级时间、升级步骤、升级注意事项等；
- 数据备份：优化升级前对系统数据进行备份；
- 资源准备：对系统的硬件和软件资源进行准备，包括存储空间、内存、网络带宽等；
- 人员准备：确定人员和角色，包括管理员、维护人员、测试人员等，并进行相应的培训；
- 风险评估：进行升级风险评估和预测，制定应急措施，并进行备份和恢复工作。

——确定升级策略：根据升级版本和系统需求，确定升级策略，主要升级策略包括直接升级、跨版本升级、重新安装等；

——测试环境验证：优化升级前，应在测试环境中进行测试和验证；

——安装过程记录：优化升级过程中，应记录所有操作和变更，包括升级前状态、升级过程中的操作及升级后状态等；

——系统回滚：优化升级过程中，应设置系统回滚方案；

——安全检查：优化升级过程中，应对系统安全性进行检查和验证，包括防火墙设置、安全策略、用户权限等；

——系统验证：优化升级完成后，应对系统进行全面验证和测试，系统的功能和性能应符合优化升级要求；

——完善文档：优化升级完成后，应及时更新系统文档，包括升级过程记录、系统配置文件的修改等。

7.4.3 数据库运行维护

7.4.3.1 一般规定

数据库运行维护一般规定包括：

——数据库巡检要求见附录 B；

——数据库故障维修要求见附录 C。

7.4.3.2 优化升级

数据库优化升级方式包括但不限于：

——表设计优化，包括表类型优化、分区表优化、临时表优化，表字段类型优化，外键索引优化等；

——索引设计优化；

——数据库参数优化，查看数据库参数信息，资源类参数配置优化调整，查询优化参数。

7.4.3.3 数据库备份和恢复

7.4.3.3.1 数据库备份

运行维护需方和维护供方应制订数据备份方案，明确相应的数据备份策略和方式。数据库备份要求包括但不限于：

——维护人员应根据运维要求填写《数据库备份记录表》见表 E.1 及《数据库备份恢复测试表》见表 E.2；

——应对数据库系统的配置参数及相关文件进行备份，当配置发生变更时应重新备份；

——应制定数据库系统的备份策略，定期对数据库系统进行自动备份，宜采用物理备份与逻辑备份相结合；

——应对备份介质进行标识，存放位置的物理环境应符合要求；

——对备份权限进行设置；

——数据备份内容应包括生产、经营、管理等应用系统中的所有关键业务数据；

——对计算机和设备进行软件安装、系统升级或更改配置时，应进行系统和数据、设备参数的完全备份；

——应用系统更新后，原系统及其数据的完整备份资料应保存一年以上；

——应建立备份文件档案及档案库，记录备份数据的信息；

——应对数据备份进行文卷管理，备份应有明确标识，包括卷包、运行环境、备份人，卷名按统一规则命名；

——存档数据保存时间根据数据重要程度和有效利用周期确定；

——重要数据应设计和实施异地容灾方案，异地容灾备份的方式和频率要结合对数据的完全恢复或不完全恢复等因素考虑；

——每年应使用专业校验工具对长期保存的备份进行校验。

7.4.3.3.2 数据库恢复

维护需方和维护供方应制订数据恢复方案，明确相应的数据恢复策略和方式，并在数据库备份完成后定期进行备份恢复测试。数据库恢复操作要求包括：

——恢复前确认故障原因；

——制定恢复计划，包括应恢复的内容、恢复的时间、恢复的操作步骤、恢复对应用造成的影响等；

——恢复前对现有内容作相应备份；

——恢复后应测试恢复的结果，恢复结果测试成功后，对恢复后的系统进行相应备份。

7.5 系统安全性运行维护

7.5.1 一般规定

系统安全性运行维护一般规定包括：

——系统安全运维服务内容，包括确定安全运维管理范围、日常安全巡检、安全设备故障维修、安全问题/事件处置、安全评估与咨询、安全设备及安全机制优化等；

——系统安全运维对象，包括信息系统基础设施、系统硬件及软件、系统数据、系统操作及管理人员、系统安全设备和安全机制等；

——常见安全设备及安全技术，主要包括防火墙(安全网关)(NF)、入侵检测系统(IDS)、入侵防御系统(IPS)、WEB 安全防护(WAF)、漏洞扫描系统(RSAS)、安全审计系统（DAS）、数据加密、访问控制、堡垒机等；

——建立系统安全运维管理制度，对安全策略、数据安全性、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面做出规定，同时规定：

- 在日常巡检及故障维修时，所有维修设备及工具应按安全管理制度经许可后才能接入信息系统设备或网络，操作过程中应保留不可更改的审计日志，操作结束后应删除工具中的敏感数据；
- 制定安全事件报告和处置管理制度，规定不同安全事件的报告、处置和响应流程，以及安全事件的现场处理、事件报告和后期恢复的管理职责等；
- 及时向安全管理部门报告发现的安全弱点和可疑事件，在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结问题和经验教训；
- 宜设置专人对信息系统安全设备操作进行检查、审计并进行堡垒机运维管理，上述人员与信息集成平台维护及安全性维护人员宜由不同的人实施。

——系统安全性巡检要求见附录 B；

——安全设备发生较重大故障时，应断开或旁路设备，进行相应的重装软件系统或设备更换，更换设备或重装软件之前应对设备参数及日志进行备份；

——系统安全设备维修要求见附录 C。

注：信息系统安全管理范围包括网络安全管理、操作系统安全管理、用户访问授权管理、密码管理、防病毒管理、系统补丁管理、安全监控和审计管理等相关内容。

7.5.2 系统安全事件处置

运维供方应制定系统安全事件响应、处置的专项预案，规定事件处置的组织、人员、工作职责、处置工具、知识库、数据和其它资源。对系统安全事件应开展事件报告、原因分析、风险程度评价、问题或灾害抑制/隔离、故障/问题修复及排除、系统运行恢复、事后保障及改进措施等相应工作。主要安全事件处置方式包括：

——病毒攻击或有害程序：应排查病毒或有害程序产生及传播的设备及网段，断开设备并关闭相应的端口，根据病毒及有害程序的特征采取查杀、删除措施；

——外部非法入侵、攻击：宜先关闭系统外部入侵的端口，分析非法入侵、攻击的类型和来源，排查相应的设备、程序存在的漏洞并进行漏洞修复；

——内部非法访问：宜先检查用户账户、用户权限、用户身份认证设置情况及相关的登录访问日志，相应设置被非法修改或越权访问情况，对相应的口令、密码进行修改或清理相关的账户；

——对受到攻击、入侵及非法访问的设备、网段进行清查，确认正常后方可接入系统网络及运行，同时对现有的漏洞扫描安全设备及访问控制机制进行评价，提出调整或优化意见；

——系统数据丢失、损坏或被篡改：应通过系统日志查找数据丢失、损坏或被篡改的原因，评价数据损失的程度，排除造成数据损失的因素后，按数据备份恢复的预案进行恢复，必要时需调整数据访问的权限或口令；

——其它事件：对于造成安全事件的系统物理环境或其它软硬件的故障或问题，参照附录 C 相关内容处理。

7.5.3 优化升级

7.5.3.1 基本要求

系统安全优化升级主要包括：

——运维供方根据系统安全设备和安全机制运行状态及安全事件发生的情况，定期进行安全风险评估，并根据安全风险评估对现有安全设备和安全机制提出优化升级建议；

——系统安全优化升级主要包括身份鉴别、访问控制、安全审计、资源控制、入侵防范、恶意代码防范、剩余信息保护等方面；
——安全设备升级或数据加密优化前，应将相关的日志及数据进行备份。

7.5.3.2 安全防护软/硬件优化

系统安全防护软/硬件优化主要包括：
——安全设备软件版本升级或补丁；
——安全设备硬件性能升级或配置扩充；
——安全策略或规则库升级、调整；
——系统安全审计范围扩展及调整。

7.5.3.3 数据安全性优化

数据安全优化主要包括：
——优化数据加密算法；
——优化数据备份策略；
——采用数据库远程机制并增加相应容灾设施。

7.5.3.4 访问机制优化

系统访问机制包括物理环境访问和逻辑环境访问两方面：
——物理环境访问机制优化，主要是系统机房安防设备升级，主要包括：
- 视频监控系统图像采集、存储清晰度优化及增加图像保存时间；
- 机房门禁权限优化、门禁入口识别技术升级；
- 安全告警事件系统检索方式、处置方式优化。

——逻辑环境访问机制优化，应根据系统平台、安全设备配置变更及安全风险评估情况对用户账户、用户权限、用户身份认证等进行优化升级，主要包括：
- 最大用户访问数量调整；
- 用户访问权限调整；
- 用户登录密码、口令升级；
- 用户身份认证识别技术升级。

7.6 应急响应

7.6.1 应急准备

7.6.1.1 应急响应组织

应急响应组织要求包括：
——应急响应组织应负责信息系统集成项目应急管理制度及应急预案的制定、日常监测和预警、应急预案演练、事件处置及事后总结改进等相关工作；
——应急响应组织宜由项目使用单位和运维供方相关人员共同组成，应急响应人员应包括项目使用单位管理人员、系统日常管理/操作人员、运维供方负责人、运维工程师、设备供应商工程师、专家顾问等，并确定应急事件响应第一责任人；
——对应急响应组织的相关人员应建立考核机制，考核至少每年进行一次。

7.6.1.2 应急响应制度和应急预案

应急响应制度和应急预案要求包括：

——应急响应组织应建立应急响应制度及应急预案；

——应急响应制度应包括日常监测和预警、应急预案演练、事件处置及事后总结等相关工作的流程和要求，明确组织成员、分工和职责、工具和物资等资源，并规定相关资源的管理要求；

——应急预案宜根据故障/事件类别制订专项应急预案，预案应包含事件报告、故障检查、问题分析、事件处理、系统恢复、损失评估、事件总结及整改意见等环节的具体工作要求；

——信息系统集成项目发生表 1 中的 1 级故障，应立即启动应急预案；

——专项应急预案针对的故障类别包括系统服务器或核心网络设备故障导致的系统瘫痪、系统数据库损坏或数据大量丢失、操作系统崩溃或应用软件主要功能故障、系统因病毒或受到攻击影响主要业务的运行、因灾害或安全问题导致基础环境严重破坏等；

——应急管理制度应规定不同类别专项应急预案演练的频次，并根据系统运行发现的问题和预案演练情况对后续演练频次进行调整。

7.6.1.3 人员培训及相关资源准备

人员培训及相关资源准备包括：

——应急响应组织应开展对组织成员及项目使用单位相关部门人员的应急响应制度、应急预案及相关知识的培训，相关培训应每年至少开展一次；

——应急响应组织应根据应急响应制度的要求，准备事件处置和应急预案演练的资源，包括管理工具、检测工具、维修工具、知识库、备品备件、灾备系统及资金等，并按制度要求对相关资源进行日常管理。

7.6.2 监测、预警和应急预案演练

7.6.2.1 日常监测和预警

日常监测和预警包括：

——运维供方应根据信息系统集成项目相关软、硬件及基础环境的巡检工作要求，定期进行巡检，对巡检中发现的问题向应急响应组织汇报，项目使用单位管理人员、操作人员发现系统运行的问题和故障，应及时与应急响应组织沟通；

——应急响应组织对巡检和系统运行中发现的问题进行整理分析，对表 1 中的 2 级故障/事件及频繁发生的 3 级故障/事件进行重点分析；

——应急响应组织在对日常监测中发现的问题进行应急事件风险评估，并提出风险预警报告，对相关问题和风险采取相应的处置、改进措施。

7.6.2.2 应急预案演练

应急预案演练包括：

——应急响应组织定期举行专项应急预案演练，应急预案演练至少每年进行一次；

——应急响应组织应制定相应的应急预案演练计划，应急预案演练计划应包括演练时间、地点、模拟应急事件/事故类别、参与部门/人员、应急演练步骤/流程及演练所需资源等内容；

——应急预案演练计划应经信息系统集成项目使用单位相关负责人审批后实施，并在实施前通知项目使用单位相关部门，应急预案演练在不影响系统集成项目正常运行的基本原则上进行；

——应急预案演练结束后，应急响应组织应对应急预案演练目标完成情况进行评价，并提交应急预案演练实施报告，报告内容应包括演练中事件上报、问题分析与追踪、组织分工处置、相关部门配合、系统恢复与重建等工作是否达到应急预案的要求，并进行分析和总结。

7.6.3 应急处置

应急处置包括：

——当发生表 1 中的 1 级故障/事件时，现场相关人员应立即向应急响应组织报告，由应急事件响应第一责任人判断故障/事件的类别、性质，启动相应的专项应急预案，并安排处置人员和相关资源；

——应急响应组织相关人员根据应急预案分工要求和应急事件响应第一责任人的安排，进行故障、问题的排查、分析，根据问题/故障的定位、诊断情况，提出相应的处置方法；

——应急响应组织根据预案安排维修工程师及相关技术人员对问题和故障进行处置，在问题和故障解决完毕后，方可恢复系统正常运行状态；

——相关故障/事件由病毒攻击或非法访问造成的，应安排相关技术人员追查攻击或非法信息的来源；

——在事件处置的全过程中，应急响应组织应对问题排查、分析及故障排除、处置进行记录，作为事件追溯和总结的依据。

7.6.4 总结改进

总结改进包括：

——应急响应组织对应急事件按相关制度、预案进行处置后，应对事件处理情况进行分析、复核，主要包括事件原因分析、问题来源追溯、应急处置准备工作充分性、应急预案针对性、事件处置经验及事件影响、损失和趋势，根据事件处置情况形成应急响应改进措施和应急预案完善建议，提交应急响应事件处理总结报告；

——应急响应事件处理总结报告应由项目使用单位相关负责人及运维供方负责人审核，就报告中的应急响应改进措施和应急预案完善建议形成一致意见，并批复相关内容；

——应急响应组织根据项目使用单位负责人与运维供方负责人对应急响应事件处理总结报告批复意见，组织实施对事件响应工作的改进和应急预案的完善，并就报告的经验总结内容及相关改进、完善措施对本组织成员及项目使用单位相关部门进行培训。

附 录 A
（规范性）
检测要求

A.1.1 基础环境集成验收检测

A.1.1.1 机房工程

机房工程的验收检测内容和检测要求如表A.1所示。

表A.1 机房工程验收检测内容和检测要求

检测内容	检测要求
温度湿度	在开机时和停机时的温度和湿度满足GB/T 2887的场地环境条件对温度和湿度的要求。
照度	符合GB/T 2887的场地环境条件对照明要求。
接地	符合GB/T 2887的接地要求。
电能质量	符合GB/T 2887的供配电系统要求，并应建立不间断供电系统。
机房面积	符合GB/T 2887的计算机机房面积要求。
防静电	符合GB 50174对静电防护的要求。
尘埃	符合GB/T 2887的场地环境对尘埃要求。
噪声	符合GB/T 2887的场地环境对噪声要求。
电磁干扰	符合GB/T 2887的场地环境对电磁干扰要求。
振动	符合GB 50174环境对振动的要求。

A.1.1.2 综合布线系统

综合布线系统的检测按照GB/T 50312的相关要求进行，综合布线检测分为系统安装质量检测和系统性能测试，系统安装质量检测内容和检测要求见表A.2，系统性能检测内容和检测要求见表A.3。

表A.2 系统安装质量检测内容和检测要求

检测内容	检测要求
缆线敷设	缆线敷设和终接应符合GB/T 50312中线缆敷设的规定，对以下项目进行测试： 1.缆线的弯曲半径； 2.预埋线槽和暗管的敷设； 3.电源线与综合布线系统缆线应分隔布放，缆线间的最小净距应符合设计要求； 4.建筑物内电、光缆暗管敷设及与其他管线之间的最小净距； 5.对绞电缆芯线终接； 6.光纤连接损耗值。
机柜安装	机柜、机架、配线架安装应符合GB/T 50312设备安装的规定，同时还应符合以下要求： 1.卡入配线架连接模块内的单根线缆色标应和线缆的色标相一致，大对数电缆按标准色谱的组合规定进行排序； 2.端接于RJ45口的配线架的线序及排列方式按有关国际标准规定的两种端接标准(T568A或T568B)之一进行端接，同时应与信息插座模块的线序排列使用同一标准； 3.机柜不应直接安装在活动地板上，应按设备的底平面尺寸选配底座，底座直接与地面固定，机柜

表 A.2（续）

检测内容	检测要求
机柜安装	固定在底座上，底座高度应与活动地板高度相同，铺设活动地板，底座水平误差每平方米不大于2mm； 4.安装机架面板，架前应预留800mm空间，机架背面离墙距离应大于600mm，背板式跳线架应经配套的金属背板及接线管理架安装在墙壁上，金属背板与墙壁应紧固； 5.壁挂式机柜底面距地面不宜小于300mm； 6.桥架或线槽应直接进入机架或机柜内； 7.接线端子各种标志应齐全。
信息插座	信息插座安装在活动地板或地面上时，接线盒应严密防水、防尘，信息插座的安装应符合GB/T 50312中的相关要求。
光缆芯线终端	连接盒面板应有标志。

表A.3 系统性能检测内容和检测要求

检测内容	检测要求
工程电气性能测试	按GB/T 50312工程电气测试的规定执行。
光纤特性测试	按GB/T 50312工程电气测试的规定执行。
综合布线系统管理	采用计算机进行综合布线系统管理和维护时，应符合以下要求： 1.采用中文平台、系统管理软件； 2.显示所有硬件设备及其楼层平面图； 3.显示干线子系统和配线子系统的元件位置； 4.实时显示和登录各种硬件设施的工作状态。
注：系统性能测试应采用专用测试仪器对系统的各条链路进行测试，并对系统的信号传输技术指标及工程质量进行评定，光纤布线应全部测试，测试对绞电缆布线链路时，以不低于10%的比例进行随机抽样测试，抽样点必须包括最远布线点。	

A.1.2 硬件集成验收检测

硬件集成验收检测包括网络设备、存储备份系统、服务器设备、用户终端设备、计算机外部设备的质量检测、设备性能及安全性检测和网络性能检测。硬件集成检测内容和检测要求见表A.4。其中：

——检测指标应符合设计要求或国家相关标准要求，有特殊要求的产品，可按合同要求或设计要求进行检测；

——对不具备现场检测条件的产品，可要求进行工厂检测并出具检测报告；

——测试所需要的文档主要有网络系统设计文档，包含网络设计方案、网络拓扑结构图、网络设备、备份存储设备和服务器清单等；

——对核心层的骨干链路，应进行全部测试：

- 对汇聚层到核心层的上联链路，应进行全部测试；
- 对接入层到汇聚层的上联链路，以不低于10%的比例进行抽样测试；
- 抽样链路数不足10条时，按10条进行抽样，上链链路数不足10条时应全部测试；
- 对于接入层的网段，以10%的比例进行抽样测试；
- 抽样网段数不足10个时，按10个进行抽样，网段数不足10个时应全部测试。

表A.4 硬件集成检测内容和检测要求

检测内容	检测要求
设备质量检查	1.应包括列入《中华人民共和国实施强制性产品认证的产品目录》或实施生产许可证和入网许可证管理的产品，未列入的产品应按照规定程序通过产品检测后方可使用； 2.检查确认外观、资料、配件、文档等是否符合合同或设计要求，具备产品检测报告。
网络设备测试	验证网络设备配置、功能设置、性能、安全性和远程管理功能是否能与满足设计要求。
服务器系统测试	检测服务器操作系统配置、功能设置、性能和安全性是否符合设计要求。
用户终端系统测试	检测用户终端操作系统配置、功能设置、性能和安全性是否符合要求。
存储和备份系统测试	检测存储系统的配置、功能设置、性能和安全性是否符合设计要求，对重要数据的及时恢复能力是否与设计要求一致。
网络设备、存储设备和服务器设备安全性测试	网络设备、存储设备和服务器设备的安全性指标，主要指设备得到有效配置，设备本身不存在弱点、漏洞或误配置，并且得到有效管理，不会引入新的威胁点对网络系统安全造成影响。
网络连通性测试	网管计算机能够与任何一台计算机连通，各子网之间根据网络要求可以进行连通。
网络路由功能测试	检测网络拓扑与网络设计要求是否一致，网络无旁路。
网络链路传输性能测试	检测网络链路传输性能与网络设计要求是否一致。
网络吞吐量测试	在网络关键站点进行网络吞吐量测试，检查测试结果是否与网络设计要求相一致。
注：设备性能指标主要包括吞吐量、延迟、丢包率、响应时间等，网络性能指标包括吞吐量、连通性测试、传输性能测试、路由测试、容错功能、网络健康状况等。	

A.1.3 软件集成验收检测

A.1.3.1 定制软件检测

定制软件测试内容和测试要求见表A.5，其中：

——定制软件的测试应从软硬件配置、涵盖的基本功能、界面操作的标准性、系统可扩展性和管理功能等方面进行测试，并根据设计要求测试其行业应用功能；

——测试依据包括软件开发合同、软件需求规格说明书、GB/T 25000.2、GB/T 25000.10、GB/T 25000.22、GB/T 25000.23、GB/T 25000.40、GB/T 25000.41、GB/T 18905.6；

——测试参考文档包括但不限于概要设计说明书、详细设计说明书、数据库设计说明书、用户文档，用户文档包括用户手册、操作手册、安装手册和维护手册等；

——测评机构通过现场核查、技术测试以及安全管理评估等方式，对信息系统的安全运行情况进行测评，测试内容主要包括环境适应性、主要安全性技术指标、功能、性能、密码及密钥管理、系统具有的一些特殊安全功能等。

表A.5 定制软件测试内容和测试要求

检测内容	测试要求
功能测试	1.系统的程序和数据应符合功能需求； 2.应在单元测试及综合测试的基础上进行功能测试，一般用黑盒测试方法，如等价类划分法、边界值分析法、因果图/判定表法等。
安全性测试	1.通过现场核查、技术测试以及安全管理评估等方式进行测评； 2.测试内容主要包括环境适应性、主要安全性技术指标、功能、性能、密码及密钥管理、系统具有的特殊安全功能等； 3. 测试所需文档包括通过审查的系统安全设计方案、系统安全管理机构和安全管理制度汇编。

表 A.5（续）

检测内容	测试要求
可靠性测试	1.测试系统的可用度、平均失效间隔时间(MTBF)、平均失效恢复时间(MTTR)等指标； 2.系统在出现故障或者违反指定接口的情况下，仍能维持规定的性能级别； 3.系统具有避免由软件故障导致失效的能力。
性能测试	系统的性能包括可承受的并发量、响应时间、吞吐量等，包含性能测试、负载测试、容量测试、压力测试、疲劳强度测试、大数据量测试等。
适应性测试	系统毋需采用额外的活动或手段就可适应需求中明确的必须适应的软硬件环境。
互操作性测试	系统与一个或多个规定信息应用系统交互正确。
易用性测试	系统的操作命令界面为标准图形交互界面，风格统一，层次简洁，操作命令的命名无二义性。
易安装性测试	安装符合习惯，安装手册清晰明白，用户根据安装手册能独立进行正确安装和运行系统。
用户文档测试	满足GB/T 25000.51的要求，用户文档应包括安装、维护、功能说明、操作说明方面的信息，并符合完整性、正确性、一致性、易理解性、易浏览性的要求。

A.1.3.2 系统软件安装检测

系统软件安装检测应包括：

——软件型号、版本、软件授权码、介质及随机资料应与合同相符；

——执行各类系统命令或系统操作,检查执行结果应正确；

——执行操作系统与系统支撑软件及各类软件产品的连接测试，检查执行结果应正确。

A.1.4 安全集成验收检测

安全集成验收检测内容和检测要求见表A.6，其中：

——网络安全和管理平台主要包括防火墙、入侵检测系统、漏洞扫描系统、防病毒、安全审计、身份认证系统、安全网关、网络隔离与交换系统、内容过滤系统等网络安全防护设备和网络管理软件等；

——网络安全和管理平台应进行相应配置，符合网络系统安全策略；

——测试依据：GB/T 18336、GB/T 20269、GB/T 20270、GB/T 20271、 GB/T 20274.1、GB/T 39786；

——测试参考文档：主要有系统设计文档，包含安全策略、安全技术方案等。

表A.6 安全集成验收检测内容和检测要求

检测内容	检测要求
产品要求	1.信息系统安全专用产品必须具有“计算机信息系统安全专用产品销售许可证”； 2.密码产品符合《商用密码管理条例》的要求； 3.特殊行业有其他规定时，应遵守行业的相关规定。
防火墙测试	防火墙系统应具有根据不同身份或角色进行访问控制，支持网络地址转换、日志统计分析等功能，检测防火墙设置是否符合安全设计要求。
防病毒系统测试	1.防病毒软件应具有实时扫描、立即扫描、病毒代码更新、日志管理、集中管理等功能； 2.检测防病毒系统是否符合设计要求。
入侵检测系统测试	使用常见的攻击手段进行模拟攻击,应能被入侵检测系统发现和阻断。
内容过滤系统测试	1.访问受限网址或内容，访问应被阻断； 2.访问未受限的网址或者内容，应能够正常访问。
漏洞扫描系统测试	漏洞信息数据库应及时更新。

表 A.6（续）

检测内容	检测要求
审计系统测试	对非法的侵入尝试、操作、访问等应进行记录与分析，模拟非法入侵，相关记录与分析情况应符合设计要求。
网络管理系统测试	能够对网络资源情况进行全面信息采集和自动预警。
网络安全和管理功能复核测试	按照网络系统设计要求和安全策略，对网络安全防护和管理功能复核测试，按照安全功能组件进行测试，抽样率为30%。
网络安全防护和网络管理设备自身安全性测试	检测网络安全防护设备、网络管理设备本身没有弱点、漏洞或误配置。

附 录 B
（资料性）
巡检要求

巡检要求见表B.1。

表B.1 巡检要求

巡检项目	巡检分项	巡检分类	巡检要求
基础环境	机房	机房供配电及照明系统	1.检查市电配电柜、配电箱及UPS配电柜、配电箱外观是否有变形、脱漆或腐蚀情况，目测箱、柜内线缆是否连接牢固、有无破损，相关输入/输出回路配电图、标识是否完整，配电柜、配电箱指示灯、仪表状态是否正常； 2.检查UPS主机外观完整性，主机输入、输出端及与蓄电池柜连接是否牢固，主机前面板显示屏及指示灯的各项内容如输入电压、输出电压、电池电压、输入/输出功率以及机内工作温度是否在正常范围,UPS工作状态,UPS主机风扇是否正常工作； 3.定期测量备用发电机电池组的电压及内阻，检查空气过滤器、冷却液位、驱动皮带、排烟系统、燃油液位、机油液位、发电机组控制器及电机机房工作环境等情况，按照发电机组保养要求更换机油、机油滤芯、燃油滤芯、空气滤芯、启动电池及冷却液，定期对发电机组进行空载、带载检测； 4.对配电箱、配电柜、UPS主机及蓄电池柜外部进行除尘处理，对UPS定期放电进行保养，放电时电池应处于充满状态，并保证负载安全性，放电时UPS供电负载应不少于UPS额定负载容量的30%，放电期间注意观察UPS电池供电时间是否达到设计要求，放电保养宜每6个月进行一次； 5.通过建筑设备监控系统或机房专用监控系统检查供配电系统运行参数、运行状态，主要包括相关回路开关状态、电压、电流、频率、功率因数、有功功率、无功功率等； 6.检查机房内照明灯具、光源是否完好，灯具亮度应正常并无闪烁，照明开关面板控制正常，应急照明灯具在回路断电后应正常开启。
		机房通风、空调及环境监测系统	1.检查空调系统的各项功能及参数，主要包括新风/送风/回风温湿度、风机/风阀运行状态、供水/回水温度、水压、水阀状态； 2.检查风机、风阀、水阀的运行报警记录，分析、排查报警发生原因； 3.检查机房内温度传感器等环境监测传感器和控制面板的外观及工作状态； 4.定期清洁滤网/过滤器及室内机、室外机表面； 5.检查空调管道保温层有无破损或结露。
		机房安防设施	1.检查机房门、门锁及门禁控制器、读卡器或生物识别设备状态是否正常； 2.检查入侵报警设施，包括报警探测器、紧急按钮、声光报警器等工作状态是否正常； 3.检查机房监控摄像机图像是否清晰，录像资料检索、回放是否正常。
		机房消防设施	1.检查机房管道、桥架的防火封堵情况； 2.检查机房火灾报警探测器状态是否正常； 3.机房内人工灭火器的压力表情况，消防栓配件是否齐全，水管有无破损； 4.机房内自动灭火系统的灭火剂贮存容器、管道、阀门、与喷嘴等系统组件应无碰撞变形、损伤及锈蚀，系统喷嘴应无堵塞； 5.消防系统与配电、空调、安防等系统的联动装置、相关线路和设备状态是否正常。

表 B.1 （第 2 页/共 5 页）

巡检项目	巡检分项	巡检分类	巡检要求
基础环境	机房	机房防雷接地系统	1.检查机房各级浪涌保护器外观无明显破损，电源线、信号线、地线连接牢固，配电箱内的电源浪涌保护器的保护空气开关应处于接通状态； 2.检查机柜、配电箱接地排，机房散流网，机房等电位端子排外观应无破损，设备外壳、机柜、配电箱、防静电地板等各处接地线是否连接牢固； 3.检测机房等电位端子板、机柜/配电箱接地排、机房散流网的接地电阻应不大于1Ω。
设施设备	服务器	外观及运行状态	1.检查服务器外部清洁情况，对机箱灰尘进行清理； 2.检查各端口电源线、视频线、网络线、光纤等连接是否牢固，相应的标识/标签是否完整； 3.检查电源状态、风扇指示灯，判断各电源模块及风扇是否正常连接并处于正常工作状态； 4.检查硬盘状态指示灯，判断硬盘是否处于正常状态； 5.检查网卡指示灯判断网络连接是否正常； 6.检查健康状态指示灯,判断服务器处于正常状态、降级工作状态或部件故障状态； 7.依次检查CPU、内存、UID状态、BMC日志及各类PCI适配器、RAID适配器的状态指示灯。
		硬件性能	1.CPU使用率应不高于75%，内存使用率应不高于80%。CPU及内存使用率过高应进行硬件、进程、应用软件、端口及病毒检查，对CPU风扇运转，进程死锁、阻塞，不必要启动项，病毒木马，无用端口，网站程序后门漏洞，非法登陆等情况进行检查，根据实际情况进行硬件修复或更换、关闭超线程、撤销或回退相关进程、取消不必要启动项、关闭不常用的端口、查杀病毒修复漏洞等，内存使用率过高的应根据实际使用需要重新对iis应用程序池进行内存设置； 2.系统硬盘空间占用率不宜超过80%，磁盘队列长度均值应不大于物理磁盘数的2倍，读取响应时间宜不大于11～15ms,写入响应时间宜不大于12ms。硬盘空间占用率过高的应对垃圾文件或失效文件进行检查和清理，通过增加缓存、优化磁盘访问策略和寻址策略、优化磁盘存储数据块和访问策略、对网络流量数据发送接收速率和丢包率进行监测，提升硬盘I/O性能； 3.网络流量占满，数据传输速率下降或丢包率上升，应检查病毒或DDoS攻击情况和非法用户访问或异常进程，过多用户访问特别是大量音视频文件访问，正常业务增多致使带宽不足，应进行相应清理和加强防范，用户访问策略优化，增加宽带资源配置； 4.服务器部件温度过高，应检查机房环境或机柜散热、温控系统运行情况，检查相应部件的风扇状态及出风口阻塞情况，更换故障部件、扩充相关硬件。
	网络设备	网络设备状态	1.检查各端口电源线、网络线、光纤等连接情况，相应的标识/标签完整性； 2.检查各类指示灯，主要包括： ——系统指示灯，如发现异常应关机维修，同时启用备用设备； ——电源指示灯，如发现异常应先断开电源，根据指示灯状态依次检查电源模块及输入电源电压情况； ——风扇指示灯，如发现异常应检查风扇连接情况、对风扇进行除尘或更换检查； ——端口指示灯，如发现异常需检查相应的光纤、网线连接情况，可通过对换信

表 B.1 （第 3 页/共 5 页）

巡检项目	巡检分项	巡检分类	巡检要求
设施设备	网络设备	网络设备状态	号线缆排查，检查端口配置和连接设备。 3.对上述相关问题的处理涉及到关机、断电的，如系统没有冗余的设备、链路时，应根据当前网络状态和业务状态进行处置，当异常状态不影响业务运行，可持续监测，待业务可以中止运行时，再进行关机、断开电源等操作。
		网络设备性能	1.CPU及内存使用率监测，CPU使用率应统计每日不同时段到5秒、1分钟和5分钟的结果，5分钟的CPU平均使用率不宜超过40%，内存使用率不宜超过60%。CPU及内存使用率过高的原因可能包括以下原因： ——硬件故障，器件会大量上报中断，中断任务过多引起系统CPU占用率过高，可先断电后重启相关网络设备，根据情况检查、修复或更换设备； ——网络环境异常，包括网络震荡、网络环路及网络攻击情况，分析产生问题的原因，通过检测工具排查相关设备或接口，将相应的接口断开使设备隔离后予以处置； ——短期发生大量并发任务，对业务部署进行适当调整，如将部分用户或部分业务调整到其他网络设备； ——内存使用率过高，可检查交换机软件更新情况。 2.设备连通性检查，通过业务端口指示灯状态检查设备连通性，通过端口检查工具或指令检查端口的链路协议状态，连通性故障应检查链路及相关设备设置情况； 3.端口流量分析，采用相关管理工具或指令对网络设备端口流量进行检测，设备带宽利用率情况及超出阈值持续的时间、频次，如发现超出阈值告警或网速明显下降，宜进行遭受攻击、广播风暴等因素排查，对相关设备的端口的上限速率进行调整； 4.日志告警信息检查，采用相关管理工具或指令查看网络设备日志，查看错误及报警类事件的日志详细信息，分析原因，根据维护手册或在供应商指导下进行处理。
	存储设备	运行状态	1.检查指示灯状态，包括系统电源、网络接口、数据传输状态、电源模块等的指示灯状态； 2.检查控制器状态，包括控制器信息、控制器健康状态和运行状态； 3.检查控制器电池状态，包括控制器电池信息、电池监控状态和运行状态； 4.检查电源状态，包括电源信息、电源模块健康状态和运行状态； 5.检查风扇组、光纤连接、网线连接、硬盘的健康状态和运行状态； 6.检查软件状态，检测版本号合法性，检查软件更新和修复情况。
		业务状态	1.检查存储池状态； 2.检查存储系统备份业务状态，包括快照或克隆的状态； 3.检查磁盘RAID及逻辑单元LUN的状态，包括LUN的卷镜像状态； 4.对于远程复制的存储系统，需检查远程复制的主设备、从设备及链路状态； 5.检查文件系统状态及相关业务运行状态； 6.检查导出系统数据，包括运行数据、系统日志、硬盘日志、诊断文件等，导出告警和事件信息。
		硬件性能	1.检查磁盘空间使用情况； 2.检查存储设备及存储介质读写速率情况； 3.检查存储控制器的存储缓存的读、写缓存分配比例情况； 4.检查数据读、写命中率情况； 5.检查存储设备的电源、存储控制器电池状态；

表 B.1 （第 4 页/共 5 页）

巡检项目	巡检分项	巡检分类	巡检要求
设施设备	存储设备	硬件性能	6.检查磁带驱动器使用情况，及时清洗磁头。
	桌面及其他硬件	桌面及其他硬件	1.定期检查工作站、瘦客户机电源及风扇状态； 2.定期检查桌面及相关硬件电源、通信及控制线路情况； 3.检查台式机工作站、瘦客户机是否正常开机启动，所有用户终端是否能正常登录； 4.检查工作站、瘦客户机CPU、内存及工作站硬盘等资源占用情况； 5.检查输入输出设备响应延时是否正常； 6.检查显示设备的图像亮度、对比度、色彩、分辨率及播放设备音量、音质是否符合要求，大型监视墙显示切换、控制功能是否正常； 7.检查打印机打印、扫描等功能是否正常，并检查打印耗材是否及时更换，定期清洁打印机进退纸通道，对机械部位及时清洗、润滑，并修复、更换磨损部件； 8.检查工作站运行日志是否存在异常错误、警告事件或非法登录情况。检查应用软件系统日志中移动终端的访问是否经过用户身份验证； 9.定期对工作站进行操作系统及应用软件补丁更新； 10.检查工作站防病毒软件配置情况，并定期查杀病毒； 11.定期对工作站运行数据进行备份。
软件	系统软件	系统软件	1.系统更新巡检：通过系统自动更新工具检查系统更新情况； 2.系统日志巡检：通过系统日志管理工具检查系统相关事件，检查系统运行状态，主要包括系统补丁及应用程序安装事件，系统开机、启动或重启、用户登录访问事件，系统错误、警告事件； 3.系统备份巡检：检查系统文件备份情况与既定备份策略的符合情况； 4.定期清理系统注册表，用磁盘清理工具清理系统缓存文件、垃圾文件。
	应用软件及接口	应用软件及接口	1.系统性能监测：通过性能监测工具对系统的CPU、内存、磁盘、网络等资源使用情况进行监测和分析，识别系统性能瓶颈，如响应速度慢、资源利用率高等问题，采取相应措施进行优化； 2.应用软件日志分析：通过日志分析工具对系统日志进行分析，查找系统错误、警告等信息，识别系统故障和安全问题，及时进行修复和加固； 3.应用软件功能检测：对集成平台中的各个应用软件进行功能检测，主要包括系统功能、数据、接口情况等； 4.定期进行数据备份和恢复测试并及时恢复系统数据； 5.版本管理：对系统应用软件进行版本管理，软件版本应符合系统需求并运行稳定，及时安装相应的软件补丁； 6.系统数据清理：清理系统过期、失效的数据和文件； 7.检查系统接口：检查系统硬件接口线缆连接情况，数据转换、通信情况。软件接口对数据验证及程序调用请求情况等； 8.安全检测：对集成平台进行安全检测。
	数据库	配置环境	1.检测数据库网络连接状态，如监听器状态、网络连通情况、客户端和服务器连通情况等； 2.检测操作系统资源利用率，如CPU占用率、内存使用率及磁盘I/O速率等； 3.检查磁盘空间使用情况，如剩余空间不足，删除不必要的文件或申请添加磁盘； 4.检查服务器时间。

表 B.1 （第 5 页/共 5 页）

巡检项目	巡检分项	巡检分类	巡检要求
软件	数据库	基本状态	1.检查所有数据库实例状态以及与数据库相关的后台进程； 2.检查表空间基本信息，包括表空间大小、剩余空间大小、表空间使用率等； 3.检查表空间与数据文件关系，包括数据文件信息、数据文件创建时机、保存路径、数据文件大小及个数、表空间与数据文件对应关系等； 4.检查数据库参数及参数设置对应的配置文件； 5.检查内存池，包括内存结构地址、是否是共享内存池、初始大小、当前总大小、数据占用大小等； 6.检查数据库日志告警及错误处理信息。
		备份信息	1.检查数据库备份日志信息； 2.检查定时备份任务； 3.检查定时删除备份任务，检查备份目录中的过期备份； 4.检查备份空间，查看备份文件存放目录、备份所在目录大小、备份目录所在根目录磁盘剩余空间大小等。
		安全性设置	1.查看用户信息，包括用户名、用户密码、索引表空间、默认表空间、数据文件等； 2.检查系统安全日志文件中登录成功或失败的用户日志信息； 3.检查数据库密码策略，定期修改密码； 4.检查数据库默认用户密码； 5.检查用户权限信息，包括用户名、权限、类型等； 6. 检查数据库默认端口使用情况。
系统安全性	安全防护软件/硬件	安全防护软件/硬件	1.检查安全防护硬件设备状态及接口信息，包括设备电源、 CPU 、内存、磁盘状态及网口、串口的通信状态等； 2.检查安全防护软/硬件的系统日志，检查安全防护系统的异常运行情况，通过安全防护系统分析报告对信息系统入侵、非法访问、数据丢失或破坏等事件，提出系统修复或优化意见； 3.定期检查、更新安全防护软/硬件的安全策略或规则库，及时清理规则库过期、失效的内容； 4.对安全防护软/硬件的操作日志进行检查、审计，检查非法登录、操作等情况。
	系统安全机制	系统安全机制	1.定期核查信息系统安全管理制度执行情况，分析相应的安全事件原因和处置情况，提出改进措施； 2.对系统需要加密的文件、数据及信息，定期核查数据存储、调用、传输过程中加密解密的有效性； 3.定期检查系统访问用户的账户、用户类型、用户权限及用户身份认证设置情况，核查账户、密码的有效性； 4.检查软、硬件及数据库的操作日志，检查非法访问情况。配置堡垒机的系统，应核查、审计运维人员登录堡垒机及相关运维操作是否符合安全管理制度要求。

附 录 C
（资料性）
故障维修

故障维修见表C.1。

表C.1 故障维修表

维修项目	维修分项	故障分类	维修要求
基础环境	机房供配电及照明系统	过载、短路	1.逐级测量相应回路火线、零线间电阻及火线、零线的对地电阻，排查线路是否接错或线缆绝缘是否失效； 2.对于过载的故障，需检查回路中接入的负载情况。
		断路	检查火线、零线的对地电压，对回路中的设备逐级排查，判断故障点，对电缆的断点重新接驳后，做好绝缘措施。
		漏电	断开回路中所有电源和负载进行排查，采用绝缘电阻测试仪依次检测火线、零线、地线之间的绝缘电阻及负载设备电源输入端对地绝缘电阻，应不低于0.5MΩ 。
		UPS故障	切换UPS到旁路状态，检查UPS整流电路、逆变器、蓄电池、保护电路等部件，逐步分析排除故障。
		照明故障	照明灯具、开关故障应检查相关配电系统，并断电检查相应的照明回路，灯具、开关处连线是否松脱，如灯具和开关设备故障，按情况进行修复或更换。
		配电系统远程控制故障	远程控制功能失效情况应检查相应的通讯及控制设备是否处于正常状态，并检查相关控制节点的线路是否存在故障。
	机房通风、空调及环境监测系统	温度、湿度异常	应检查温湿度设置情况，空调压缩机、冷凝器、加热器、加湿器、风机、风阀、滤网的状态，空调风管、空调制冷剂是否存在泄漏等，对故障部件予以更换、修复或清理，及时补充制冷剂。
		空气质量异常	监测到机房一氧化碳、二氧化碳或粉尘浓度上升而无法正常调节情况，检查机房新风、排风的风机、风阀、滤网的状态，对故障部件予以更换、修复或清理，同时检查空调风管是否存在泄漏。
		其他故障	1.检查空调控制面板是否故障，控制面板连接线路是否松脱、短路； 2.检查温湿度传感器、空气质量传感器是否正常工作，传感器线路是否正常连接，对故障传感器进行更换； 3.检查空调室内机是否发生凝水、溢水，空调排水管是否堵塞。
	机房安防设施	机房门禁系统故障	机房门禁系统故障包括门、门栓、门锁破损，门禁识别、开锁功能失效等，应排查故障设备和系统连接线路，更换故障设备。
		报警系统故障	报警系统故障包括探测器、紧急按钮误报警、失效或无法复位、警情发生时声光报警器无法启动等，对于误报警的情况，需排查是否存在导致误报的外部原因，排除外部因素后再检查设备故障。报警系统故障排查应将探测器、按钮相应的防区进行旁路，再检查相应设备和报警线路。
		摄像机故障	摄像机故障包括无图像或图像失真、模糊，应排查摄像机、电源及传输线路是否存在故障，对故障设备予以修复或更换。

表 C.1（第 2 页/共 5 页）

维修项目	维修分项	故障分类	维修要求
基础环境	机房安防设施	存储录像资料损坏	存储录像资料丢失或无法检索、回放，应检查检索的资料是否已超过存储期限，是否有人为操作导致录像资料丢失或未录像，存储硬盘是否损坏。
	机房消防设施	灭火器失效	对过期失效的灭火器予以更换，对消防栓设施有破损的予以修复。
		消防报警探测器误报、失效	应首先排查导致误报的外部因素，如环境潮湿、粉尘的影响，排除外部因素后，再对的设备和线路进行检测，修复或更换故障设备。
		自动灭火系统故障	如发生渗水、漏气等情况，应检查相应管道及阀门是否正常。如发生火灾后系统无法启动情况，应检查系统控制模块、阀门、管道过滤器或喷口，对故障部件予以修复、更换。
		消防联动安防、配电、空调等设施故障	应检查联动模块及相应线路，排除联动设备自身故障，检查相关系统联动控制、通讯端口是否正常。
	防雷接地设施	防雷接地设施故障	1.检查各级浪涌保护器及其接地线，及时予以更换； 2.配电箱中电源浪涌保护器的保护空气开关断开时，应检查电源浪涌保护器是否短路失效，及时更换失效的浪涌保护器。
硬件设备	服务器	启动、加电故障	启动、加电故障包括主机不能加电、开机无显示/开机报警、启动死机/报错、反复重启、BIOS异常、开机噪音大、登录失败/报错等： 1.依次检查服务器供电电压、电源线连接状态，服务器电源模块状态； 2.进行CPU、主板、硬盘等元器件的温度检查，检查相关部件风扇状态； 3.CPU、内存、系统硬盘等部件进行重新拔插和检查，监测相关部件工作情况，多内存服务器检查内存规格一致性和兼容性； 4.检查BIOS设置,主要包括启动顺序、启动磁盘的参数等，必要时恢复BIOS的出厂设置； 5.检查操作系统文件损坏情况及病毒入侵和非法访问情况并进行相应维护。
		驱动器类故障	驱动器类故障除可能造成服务器无法启动外，还包括硬盘/光驱无法识别、程序运行出错、硬盘对格式化操作无法完成、硬盘/光驱出现异响、噪声等： 1.检查硬盘、光驱外观是否变形、变色及断裂缺损； 2.检查硬盘、光驱加电后指示灯闪烁情况，硬盘连接线状态，跳线状态； 3.检查硬盘、光驱BIOS设置情况； 4.检查硬盘坏道及其它故障，宜采用硬盘检测程序进行检查。
		软件安装故障	软件安装故障主要包括操作系统或应用软件安装发生报错、重启、死机等，以及软件无法安装或无法卸载： 1.服务器各部件连接线状况，连接插头、插座的接针变形、缺失、短路等现象； 2.检查电源、主板和内存状态，硬盘、光驱的异响、噪声情况； 3.检查CPU、硬盘、显卡等温度，风扇状态； 4.检查BIOS设置，必要时恢复出厂设置； 5.在软件安装最小系统下进行测试，故障消失则将最小系统外的设备逐一接上，排查故障部件；

表 C.1（第 3 页/共 5 页）

维修项目	维修分项	故障分类	维修要求
硬件设备	服务器	软件安装故障	6.应用软件安装故障，暂时关闭BIOS防写开关，同时关闭系统BootEasy功能及防病毒功能； 7.软件原因或病毒入侵引起的安装故障，可参考软件手册相关要求进行修复。
		程序运行故障	程序运行故障包括系统运行中出现蓝屏或死机、系统运行速度变慢、应用程序不能正常使用、程序运行导致硬件功能失效等： 1.查看应用软件手册并咨询软件供应商，进行服务器当前硬件配置符合性检测； 2.设备管理器中检查硬件状态，更新相关硬件驱动程序； 3.检查并整理硬盘空间，临时文件和非必要文件进行相应处理； 4.软件冲突、兼容或病毒引起的故障，可参考软件手册相关要求进行修复。
		显示故障	显示故障包括开机无画面、显示偏色、抖动、花屏等： 1.检查显示设备与服务器显卡连接线及端口状态； 2.检查服务器显卡温度及显卡风扇状态； 3.显卡重新插拔或更换显卡； 4.检查显示设备，并进行相应修复。
		网络通讯故障	网络通讯故障包括服务器连不通网络、网络传输速度慢、数据传输错误、网络应用出错或死机、某项应用不能使用网络、网络设备安装异常等： 1.检查网卡指示灯状态，更换网卡； 2.检查主板与网卡上元器件的变形、变色情况； 3.加电后网卡及其它设备异味、温度过高等情况，更换相关部件； 3.检查服务器CPU、内存等资源占用情况以及网络链路状态； 4.检查网络设备及相关配置情况，并进行相应修复。
	网络设备	物理层	物理层故障包括网络设备硬件故障及物理线路故障，具体有网络电缆或光纤线缆的物理损坏或松动、线路中间传输/转换设备故障、网络设备主板、端口模块或电源故障等，可通过网络设备指示灯、线缆测试工具及硬件检测工具进行排查处理。
		数据链路层	数据链路层故障包括数据帧丢失或错发、流量监控异常、链路层地址设置及链路协议建立问题、同步通讯时钟问题等，数据链路层故障应通过相关指令检查MAC地址与IP地址的映射。
		网络层	网络层故障包括路由及IP地址设置错误、子网掩码设置错误、IP和DNS不正确绑定等，可通过连通性测试或路由检测命令来排查。
		传输层	传输层故障主要包括数据包重发、通信拥塞、路由器或防火墙访问列表配置有误等，可通过协议分析器等工具对数据通信进行分析。
		应用层	应用层故障主要是服务器、操作系统、应用程序等软硬件资源的问题或异常造成，可通过操作系统、应用程序自身检测功能或其它软、硬件检测工具对相关问题进行排查。
	存储设备	硬件故障	1.检查控制器或服务器、硬盘模块、接口模块、风扇模块、电源模块等硬件类状态是否故障告警；

表C.1（第4页/共5页）

维修项目	维修分项	故障分类	维修要求
	存储设备	硬件故障	2.在存储设备侧查看相应模块的告警指示灯。
		链路故障	1.排查相关设备光纤、网线连接是否松动或被损坏； 2.排查光模块是否出现故障或光模块类型是否匹配； 3.对于采用FC-SAN架构的存储系统，应检查FC主机端口、服务器HBA卡、存储设备交换机端口的速率是否匹配； 4.排查是否iSCSI主机端口IP地址或服务器业务网口IP地址是否配置错误。
	桌面及其他硬件	工作站、瘦客户机等设备开机、启动异常	检查系统电源、主板等部件，同时检查工作站的BIOS设置情况，对故障部件予以修复更换。
		用户登录异常	1.检查系统网络状态； 2.依据系统提示检查应用程序补丁安装情况； 3.检查相关运行数据丢失情况及用户权限更新情况。
		输入输出设备响应异常	1.检查相关设备硬件故障情况； 2.检查相关设备驱动程序更新情况。
		系统显示画面或控制异常	1.检查显示设备相关线缆连接情况； 2.检查显示设备画面调节控制功能； 3.显示屏幕局部偏色等情况，应检查设备附近的电磁干扰情况； 4.对显示设备的故障主板、电源等部件进行修复或更换。
		打印机异常	1.打印机无响应，检查打印机电源及通讯接口，并检查打印机的工作状态如缺纸、卡纸等情况，必要进行设备重启； 2.打印异常情况如模糊、乱码等现象，应检查打印机喷头及传动部件，对相关部件进行清洗、润滑或更换处理。
		专用终端故障	依据行业终端功能、性能要求，在设备供应商支持下进行设备修复或更换。
软件	系统软件	系统无法启动或出现死机、蓝屏	1.排查服务器等硬件原因； 2.启动故障，检查近期安装的系统更新，使用系统恢复工具回滚、删除近期系统更新或返回最近一次正确的系统配置； 3.磁盘引导分区损坏或系统文件损坏，检查并修复引导分区或系统文件，或用缓存副本替换损坏的文件； 4.运行中死机、蓝屏故障，检查近期安装的软件，删除与操作系统冲突的相关软件； 5.在系统数据备份后，采用系统安装介质对操作系统重新安装，重装系统宜在设备供应商支持下进行。
		系统安装应用程序错误或应用程序无法运行	1.检查系统对应用程序安装权限开启情况； 2.检查动态连接库文件损坏和丢失情况，采用修复工具进行修复； 3.检查系统版本与应用程序版本的兼容性，更换有冲突的应用程序版本； 4.应用程序接口调用失败，检查访问权限及相关文件，根据系统显示的错误代码进行相应处理。
		系统运行缓慢	1.检查系统虚拟内存设置情况； 2.检查系统开机启动项优化情况；

表 C.1（第 5 页/共 5 页）

维修项目	维修分项	故障分类	维修要求
软件	系统软件	系统运行缓慢	3.检查系统注册表及过期失效文件清理情况。
		病毒攻击	进行病毒查杀，参考软件手册及防病毒相关要求进行处理。
	应用软件及接口	系统登录失败	故障原因主要包括用户身份验证错误、相关账户权限失效、客户端工作站故障或访问请求冲突等，应分析系统日志近期登录情况，对相关失效的账户权限进行恢复。
		平台显示设备不在线	系统显示被管理、控制的设备不在线，应检查前端设备状况，系统对设备检索设置情况、系统网关等硬件故障，根据对系统设置情况及接口状态进行处理。
		应用程序错误或功能失效	常见问题主要有配置文件错误、数据丢失或损坏、软件接口调用异常、相关硬件通信故障等，应根据应用软件的故障指示或代码，对服务器端、客户端及接口设备、通信链路进行故障排查及处理。
		系统响应缓慢或停滞	常见问题主要包括程序bug导致死循环、并行任务或访问请求过多导致系统硬件资源占用率过高等。应暂停出现问题的程序，或暂时关闭不重要的功能模块，调整系统用户最大访问数量的设置，并根据用户权限优先级的设置以保证主要用户请求。如故障频繁发生，宜对软硬件配置进行升级。
		系统受到攻击或发现病毒	进行病毒查杀，参考相关要求进行处理。
	数据库	事务故障	事务故障可通过事务重做、事务撤销恢复。
		系统故障	1.检查数据库系统版本，不使用新发布的测试版本作为生产环境； 2.检查数据库系统的修补程序，安装修补程序前做好数据库测试和备份工作； 3.检查数据库系统主机是否存在硬件故障，检查数据库软件是否异常； 4.检查系统日志文件，查看系统故障原因和故障前系统运行状态。
		介质故障	检查数据库系统存储的介质是否被损坏。
		数据库连接异常	检查网络情况、数据库状态、检查数据库运行日志、检查数据库登录情况、检查是否杀毒软件导致数据库异常。
系统安全	-	设备启动故障	检查设备电源供电情况，设备电源模块和部件，对故障部件进行修复或更换。
		设备连接或登录故障	检查安全设备网络端口连接状态，IP地址及路由设置情况，相关应用端口开放情况，相应的用户的授权情况。
		设备功能故障	安全设备的检测、防护、审计、扫描功能故障，应检查相关应用端口开放情况，相应软件补丁安装情况，安全策略或规则库更新情况以及规则冲突情况。

附 录 D
（资料性）
巡检记录

供配电、照明系统巡检记录表见表D.1,通风、空调及环境监测系统巡检记录表见表D.2,机房安全防范/消防系统巡检记录表见表D.3,机房防雷接地巡检记录表见表D.4,服务器巡检记录表见表D.5,网络设备(交换机)巡检记录表见表D.6,系统存储设备巡检记录表见表D.7,桌面及其他硬件巡检记录表见表D.8,软件巡检记录表见表D.9,数据库巡检记录表见表D.10,安全防护系统巡检记录表见表D.11。

表D.1 供配电、照明系统巡检记录表

项目名称				
机房位置				
巡检项目	巡检内容	正常	异常	备注
配电柜/配电箱	外观及线路连接	☒	☒	
	输入电压	☒	☒	
	输出电压	☒	☒	
	配电回路图及标识完整性	☒	☒	
UPS主机及电池组	外观及线路连接	☒	☒	
	输入电压	☒	☒	
	输出电压	☒	☒	
	电池电压	☒	☒	
	面板/指示灯显示状态	☒	☒	
备用发电机及电池组	外观及控制器连接	☒	☒	
	电池电压及内阻	☒	☒	
	冷却液位	☒	☒	
	燃油液位	☒	☒	
	驱动皮带	☒	☒	
	排烟设备	☒	☒	
	空载启停测试	☒	☒	
	带载启停测试	☒	☒	
机房照明	灯具状态	☒	☒	
	控制面板状态	☒	☒	
配电/照明监控软件	系统登录、操作情况	☒	☒	
	配电/照明各回路状态	☒	☒	
系统保养情况说明				
异常问题及处理情况说明				
注：系统保养包括设备除尘、UPS定期充放电、发电机组机油及滤芯更换等。供配电、照明系统检查项为指导性要求，运维需方、供方可根据项目实际情况及需求予以调整。				

表D.2 通风、空调及环境系统巡检记录表

项目名称				
机房位置				
巡检项目	巡检内容	正常	异常	备注
空调、通风及环境监控软件	系统登录、操作情况	☒	☒	
	新风/送风/回风温度	☒	☒	
	新风/送风/回风湿度	☒	☒	
	风机/风阀运行状态	☒	☒	
	水阀状态及水压	☒	☒	
	供水/回水温度	☒	☒	
	系统运行报警记录	☒	☒	
室内实际控制状态	室内温度	☒	☒	
	室内湿度	☒	☒	
	空气质量	☒	☒	
其他	控制面板状态	☒	☒	
	环境监测传感器状态	☒	☒	
系统保养情况说明				
异常问题及处理情况说明				
注：系统保养包括清洁滤网/过滤器及室内机、室外机表面，空调室外机加氟等。通风、空调及环境系统检查项为指导性要求，运维需方、供方可根据项目实际情况及需求予以调整。				

表D.3 机房安全防范/消防系统巡检记录表

项目名称				
机房位置				
巡检项目	巡检内容	正常	异常	备注
安防管理软件	安防设备是否在线	☒	☒	
	系统日志报警/异常事件	☒	☒	
门禁系统	出入识别及开门	☒	☒	
	机房门的闭门器状态	☒	☒	
报警系统	触发防区报警状态	☒	☒	
	声光报警器状态	☒	☒	
视频监控系统	图像检查	☒	☒	
	录像检索、回放	☒	☒	
	图像保存时长	☒	☒	
消防设施	管道防火封堵	☒	☒	
	灭火器状态	☒	☒	
	消防栓状态	☒	☒	
	火灾报警器状态	☒	☒	
	自动灭火系统	☒	☒	
系统保养情况说明				
异常问题及处理情况说明				
注：系统保养包括摄像机防护罩除尘、报警探测器除尘、闭门器除尘/除垢及注油等。机房安全防范/消防系统检查项为指导性要求，运维需方、供方可根据项目实际情况及需求予以调整。				

表D.4 机房防雷接地巡检记录表

项目名称				
机房位置				
巡检项目	巡检内容	正常	异常	备注
防雷器检查	电源防雷器	☒	☒	
	信号防雷器	☒	☒	
各接地端子检查/检测	机房等电位端子箱	☒	☒	
	机房散流网	☒	☒	
	配电柜/配电箱	☒	☒	
	空调室内机	☒	☒	
	防静电地板	☒	☒	
	机柜接地端子排	☒	☒	
	机柜柜体/柜门	☒	☒	
	机柜内主要设备	☒	☒	
异常问题及处理情况说明				
注：检测接地电阻应符合相关专业规范及设计要求。机房防雷接地检查项为指导性要求，运维需方、供方可根据项目实际情况及需求予以调整。				

表D.5 服务器巡检记录表

项目名称				
服务器品牌		服务器型号		
服务器系列号		服务器IP地址		
操作系统版本		数据库版本		
CPU型号规格		CPU数量		
内存型号规格		内存数量		
硬盘型号规格		硬盘数量		
RAID配置		RAID控制器缓存		
巡检项目	巡检内容	正常	异常	备注
外观及运行状态	线缆连接及标签	☒	☒	
	健康状态	☒	☒	
	硬盘状态	☒	☒	
	电源、风扇状态	☒	☒	
	网卡状态	☒	☒	
	BMC日志	☒	☒	
	适配器状态	☒	☒	
硬件性能	CPU平均利用率	☒	☒	
	CPU温度	☒	☒	
	内存平均利用率	☒	☒	
	硬盘空间占用率	☒	☒	
	读取/写入响应时间	☒	☒	
	网络连接状态	☒	☒	
异常问题及处理情况说明				
注：CPU及内存平均利用率要求检测3次，每次5分钟，3次平均的利用率应符合要求。服务器检查项为指导性要求，运维需方、供方可根据项目实际情况及需求予以调整。				

表D.6 网络设备（交换机）巡检记录表

项目名称				
机房位置				
巡检项目	巡检内容	正常	异常	备注
网络设备运行状态	线缆连接及标签	☒	☒	
	系统健康状态	☒	☒	
	电源状态	☒	☒	
	风扇状态	☒	☒	
	端口状态	☒	☒	
硬件性能	CPU利用率	☒	☒	
	内存利用率	☒	☒	
	网络连通性	☒	☒	
	网络端口流量分析	☒	☒	
	日志告警信息	☒	☒	
异常问题及处理情况说明				
注：每次巡检网络核心层、汇聚层设备应100%检查，接入层设备每次巡检不少于总数的10%且不少于10台（个）。网络设备（交换机）检查项为指导性要求，运维需方、供方可根据项目实际情况及需求予以调整。				

表D.7 系统存储设备巡检记录表

项目名称				
设备品牌		设备型号		
设备系列号		设备IP地址		
硬盘类别		硬盘型号规格		
RAID级别		硬盘数量		
巡检项目	巡检内容	正常	异常	备注
外观及运行状态	线缆连接及标签	☒	☒	
	电源、风扇状态	☒	☒	
	各端口状态	☒	☒	
	硬盘状态	☒	☒	
	存储日志	☒	☒	
硬件性能	硬盘空间使用率	☒	☒	
	存储读取/写入速率	☒	☒	
	检查存储缓存命中率	☒	☒	
业务状态	检查存储Lun使用率	☒	☒	
	检查存储热备盘	☒	☒	
	远程复制设备及链路	☒	☒	
异常问题及处理情况说明				
注：系统存储设备检查项为指导性要求，运维需方、供方可根据项目实际情况及需求予以调整。				

表D.8 桌面及其他硬件巡检记录表

项目名称				
设备品牌		设备型号		
设备系列号		设备IP地址		
巡检项目	巡检内容	正常	异常	备注
硬件性能及运行状态	电源、风扇状态	☒	☒	
	供电线路	☒	☒	
	通信/控制线路	☒	☒	
	终端CPU、内存利用率	☒	☒	
	终端硬盘占用率	☒	☒	
	显示屏亮度、对比度、色彩及分辨率	☒	☒	
	播放设备音量、音质	☒	☒	
	监视墙显示切换、控制	☒	☒	
	打印设备功能	☒	☒	
业务状态	终端开机启动、登录	☒	☒	
	输入/输出设备响应延时	☒	☒	
	软件版本更新	☒	☒	
	病毒查杀	☒	☒	
	工作站数据备份	☒	☒	
异常问题及处理情况说明				
注：桌面及其他硬件检查项为指导性要求，运维需方、供方可根据项目实际情况及需求予以调整。				

表D.9 软件巡检记录表

<table>
<tr><td>项目名称</td><td colspan="5"></td></tr>
<tr><td>软件品牌/型号</td><td colspan="2"></td><td>软件版本号</td><td colspan="2"></td></tr>
<tr><td>软件安装主机名称</td><td colspan="2"></td><td>软件安装主机IP地址</td><td colspan="2"></td></tr>
<tr><td>巡检项目</td><td colspan="2">巡检内容</td><td>正常</td><td>异常</td><td>备注</td></tr>
<tr><td rowspan="4">系统软件</td><td colspan="2">系统日志</td><td>☒</td><td>☒</td><td></td></tr>
<tr><td colspan="2">系统更新</td><td>☒</td><td>☒</td><td></td></tr>
<tr><td colspan="2">系统备份</td><td>☒</td><td>☒</td><td></td></tr>
<tr><td colspan="2">系统注册表清理</td><td>☒</td><td>☒</td><td></td></tr>
<tr><td rowspan="9">应用软件及接口</td><td colspan="2">软件运行日志</td><td>☒</td><td>☒</td><td></td></tr>
<tr><td colspan="2">软件功能检测</td><td>☒</td><td>☒</td><td></td></tr>
<tr><td colspan="2">软件版本更新</td><td>☒</td><td>☒</td><td></td></tr>
<tr><td colspan="2">软件运行数据备份</td><td>☒</td><td>☒</td><td></td></tr>
<tr><td colspan="2">过期、失效数据清理</td><td>☒</td><td>☒</td><td></td></tr>
<tr><td colspan="2">软件安全性检测</td><td>☒</td><td>☒</td><td></td></tr>
<tr><td colspan="2">系统硬件接口连接</td><td>☒</td><td>☒</td><td></td></tr>
<tr><td colspan="2">软、硬件接口状态</td><td>☒</td><td>☒</td><td></td></tr>
<tr><td colspan="6">异常问题及处理情况说明</td></tr>
<tr><td colspan="6"></td></tr>
<tr><td colspan="6">注：应用软件宜根据系统具体功能及性能参数对巡检要求予以调整完善。软件检查项为指导性要求，运维需方、供方可根据项目实际情况及需求予以调整。</td></tr>
</table>

表D.10 数据库巡检记录表

项目名称				
主机名称		CPU配置		
内存配置		硬盘配置		
操作系统版本		数据库名称及版本		
数据库端口号		相关业务系统		
巡检项目	巡检内容	正常	异常	备注
配置环境	CPU、内存占用率	☒	☒	
	磁盘空间占用率	☒	☒	
	系统网络连接	☒	☒	
	服务器时间	☒	☒	
基本状态	数据库实例及服务进程	☒	☒	
	数据库参数	☒	☒	
	表空间状态	☒	☒	
	控制文件状态	☒	☒	
	数据文件状态	☒	☒	
	内存池检查	☒	☒	
	数据库日志告警及错误处理信息	☒	☒	
备份信息	数据库备份日志	☒	☒	
	备份文件目录	☒	☒	
	备份磁盘空间	☒	☒	
	定时备份及过期备份删除	☒	☒	
安全性设置	用户信息设置及口令修改	☒	☒	
	安全日志	☒	☒	
	密码策略及密码定期修改	☒	☒	
	数据库端口状态	☒	☒	
异常问题及处理情况说明				

注1：CPU、内存、硬盘配置应分别注明相应的规格、数量。

注2：表空间状态包括表空间大小、剩余空间大小、表空间使用率、临时表空间使用情况等。

注3：控制文件状态包括控制文件个数、名称、位置等。

注4：数据文件状态包括数据文件信息、数据文件创建时机、保存路径、数据文件大小及个数、表空间与数据文件对应关系等。

注5：内存池检查包括内存结构地址、是否是共享内存池、初始大小、当前总大小、数据占用大小等。

注6：数据库检查项为指导性要求，运维需方、供方可根据项目实际情况及需求予以调整。

表D.11 安全防护系统巡检记录

<table>
<tr><td>项目名称</td><td colspan="5"></td></tr>
<tr><td>硬件/软件名称</td><td colspan="2"></td><td>硬件/软件品牌、型号</td><td colspan="2"></td></tr>
<tr><td>软件版本号</td><td colspan="2"></td><td>硬件设备IP地址</td><td colspan="2"></td></tr>
<tr><td>巡检项目</td><td colspan="2">巡检内容</td><td>正常</td><td>异常</td><td>备注</td></tr>
<tr><td rowspan="4">安全防护硬件状态</td><td colspan="2">电源状态</td><td>☒</td><td>☒</td><td></td></tr>
<tr><td colspan="2">CPU、内存状态</td><td>☒</td><td>☒</td><td></td></tr>
<tr><td colspan="2">磁盘状态</td><td>☒</td><td>☒</td><td></td></tr>
<tr><td colspan="2">网口/串口通信</td><td>☒</td><td>☒</td><td></td></tr>
<tr><td rowspan="4">安全防护软件状态</td><td colspan="2">系统运行日志</td><td>☒</td><td>☒</td><td></td></tr>
<tr><td colspan="2">系统操作日志</td><td>☒</td><td>☒</td><td></td></tr>
<tr><td colspan="2">安全策略/规则库</td><td>☒</td><td>☒</td><td></td></tr>
<tr><td colspan="2">规则库清理</td><td>☒</td><td>☒</td><td></td></tr>
<tr><td rowspan="2">其他</td><td colspan="2">数据加密</td><td>☒</td><td>☒</td><td></td></tr>
<tr><td colspan="2">安全系统用户信息</td><td>☒</td><td>☒</td><td></td></tr>
<tr><td colspan="6">异常问题及处理情况说明</td></tr>
<tr><td colspan="6"></td></tr>
<tr><td colspan="6">注1：运维供方宜根据系统具体防护对象、防护功能及软、硬件性能参数对巡检要求予以调整完善。
注2：系统运行日志检查，应对防护对象存在入侵、非法访问、数据丢失或破坏等事件进行分析并提出修复或优化意见。
注3：数据加密检查，应核查数据存储、调用、传输过程中加密解密的有效性。
注4：安全防护系统检查项为指导性要求，运维需方、供方可根据项目实际情况及需求予以调整。</td></tr>
</table>

附 录 E
（资料性）
数据库备份

数据库备份记录表见表E.1,数据库备份恢复测试表见表E.2。

表E.1 数据库备份记录表

项目名称			
操作系统版本		数据库名称及版本	
数据库端口号		相关业务系统	
备份频率		备份时间	
备份策略/方式	☒手动备份 ☒自动备份		
	☒完全备份 ☒增量备份 ☒差异备份		
	☒本地备份 ☒远程备份		
	☒在线备份 ☒离线备份		
备份工具			
备份介质			
备份文件路径			
备份文件名			
备份过程简述			
备份执行人		检查人	

表E.2 数据库备份恢复测试表

<table>
<tr><td>项目名称</td><td colspan="3"></td></tr>
<tr><td>操作系统版本</td><td></td><td>数据库名称及版本</td><td></td></tr>
<tr><td>数据库端口号</td><td></td><td>相关业务系统</td><td></td></tr>
<tr><td>测试主机</td><td></td><td>测试主机IP地址</td><td></td></tr>
<tr><td>备份介质编号</td><td colspan="3"></td></tr>
<tr><td>备份文件名</td><td colspan="3"></td></tr>
<tr><td>备份文件路径</td><td colspan="3"></td></tr>
<tr><td>数据恢复路径</td><td colspan="3"></td></tr>
<tr><td colspan="4">备份恢复测试步骤简述</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td colspan="4">备份恢复测试问题说明</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td>测试结果</td><td colspan="3">☒数据恢复成功 ☒数据恢复不成功</td></tr>
<tr><td>测试执行人</td><td></td><td>测试时间</td><td></td></tr>
<tr><td colspan="4">注：对于定期自动备份的数据，应按备份方案定期进行数据恢复测试，对手动备份的数据，应在手动备份完成后立即进行恢复测试。</td></tr>
</table>