

CECS XXX：201X

中国工程建设协会标准

数据中心基础设施等级评定标准

Standard for tier of Infrastructure of Data Centers

（征求意见稿）

××出版社

中国工程建设协会标准

数据中心基础设施等级评定标准

Standard for tier of Infrastructure of Data Centers

CECS XXX：201X

主编单位：

北

批准单位：中国工程建设标准化协会

施行日期：201×年××月××日

××出版社

201× 北 京

**前 言**

本标准是根据中国工程建设标准化协会《关于发印2014年第二批工程建设协会标准制订、修订计划的通知》（建标协字[2014］070号）的要求，由中国工程建设标准化协会信息通信专业委员会会同有关单位编制完成。

本标准在制定过程中，编制组进行了广泛的调查研究，认真总结实践经验，并参考有关国内外的标准，在广泛征求意见的基础上，最后经审查定稿。

本标准共分6章，主要技术内容有：总则、术语、基本规定、设计阶段等级评定、实施阶段等级评定、运维阶段等级评定。

本标准由中国工程建设标准化协会信息通讯专业委员会负责日常管理并负责具体内容的解释。执行过程中如有意见或建议，请寄送中国工程建设标准化协会信息通讯委员会中国数据中心工作组（地址：北京市西城区车公庄大街乙5号鸿儒大厦A座4层B-C室，邮政编码：100044,电子邮件:XXXXXXXXX）。

 本规范的主编单位、参编单位、主要起草人和主要审查人：

主编单位：中国工程建设标准化协会信息通讯委员会

参编单位：

主要起草人：

主要审查人：

**目 次**

1 总则 （5）

2 术语 （6）

3 基本规定 （10）

4 设计阶段等级评定 （11）

5 实施阶段等级评定 （11）

6 运维阶段等级评定 （13）

6.1 一般规定 （13）

6.2 组织架构 （13）

6.3 人员配备 （14）

6.4 运维人员技术要求 （15）

6.5 岗位培训与考核 （15）

6.6 管理制度 （15）

6.7 基础设施监控 （17）

6.8 基础设施维护 （19）

6.9 容量管理 （23）

6.10 应急预案与服务连续性 （24）

**1 总 则**

1.0.1 为规范数据中心基础设施的等级评定，确保电子信息系统安全、稳定、可靠地运行，做到技术先进、经济合理、安全适用、节能环保，制定本标准。

1.0.2 本标准适用于新建、改建和扩建的数据中心基础设施的等级评定。

1.0.3 数据中心基础设施的等级评定应遵循实事求是的原则。

1.0.4 数据中心基础设施的等级评定除应符合本标准外，尚应符合国家现行有关标准、规范的规定。

2 **术语**

2.0.1 数据中心 data center

为集中放置的电子信息设备提供运行环境的建筑场所，可以是一栋或几栋建筑物，也可以是一栋建筑物的一部分，包括主机房、辅助区、支持区和行政管理区等。

2.0.2 基础设施 infrastructure

数据中心内，为电子信息设备提供运行保障的设施。

2.0.3 电子信息设备 electronic information equipment

对电子信息进行采集、加工、运算、存储、传输、检索等处理的设备，包括服务器、交换机、存储设备等。

2.0.4 主机房 computer room

主要用于数据处理设备安装和运行的建筑空间，包括服务器机房、网络机房、存储机房等功能区域。

2.0.5 辅助区 auxiliary area

用于电子信息设备和软件的安装、调试、维护、运行监控和管理的场所，包括进线间、测试机房、总控中心、消防和安防控制室、拆包区、备件库、打印室、维修室等区域。

2.0.6 支持区 support area

为主机房、辅助区提供动力支持和安全保障的区域，包括变配电室、柴油发电机房、电池室、空调机房、动力站房、不间断电源系统用房、消防设施用房等。

2.0.7 行政管理区 administrative area

用于日常行政管理及客户对托管设备进行管理的场所，包括办公室、门厅、值班室、盥洗室、更衣间和用户工作室等。

2.0.8 冗余 redundancy

重复配置系统的一些或全部部件,当系统发生故障时,冗余配置的部件介入并承担故障部件的工作, 由此延长系统的平均故障间隔时间。

2.0.9 N——基本需求 N——base requirement

系统满足基本需求，没有冗余。

2.0.10 N+X冗余 N+X redundancy

系统满足基本需求外，增加了X个组件、X个单元、X个模块或X个路径。任何X个组件、单元、模块或路径的故障或维护不会导致系统运行中断。（X=1～N）

2.0.11 容错 fault tolerant

具有两套或两套以上的系统，在同一时刻，至少有一套系统在正常工作。按容错系统配置的基础设施，在经受住一次严重的突发设备故障或人为操作失误后，仍能满足电子信息设备正常运行的基本需求。

2.0.12 静态 static state

主机房的空调系统处于正常运行状态，室内温度和露点温度达到电子信息设备的运行要求，但电子信息设备未运行。

2.0.13 动态 dynamic state

主机房的空调系统和电子信息设备处于正常运行状态，室内有相关人员在场的情况。

2.0.14 运维管理( Operation and Maintenance Management)

对数据中心基础设施进行日常运行和维护，确保各项基础设施系统安全稳定地运行。运维管理包括制定运维制度、流程和计划。执行运维的日常操作、响应和处理基础设施故障、突发事件等紧急情况。

2.0.15 生命周期（Life Cycle）

通常指数据中心从投产到经济寿命结束的全过程。但也包括将投产前的规划期、设计期、建设期、试运行期作为生命周期一部分，做阶段考量。

2.0.16 预防性维护（Preventive Maintenance）

按照基础实施各系统的使用规定，设置预定的时间间隔或按既定的准则实施的维护和保养。

2.0.17 风险评估（Risk Assessment）

针对运行的设备所面临的威胁、存在的弱点、造成的影响，以及三者综合作用所带来风险的可能性的评估，同时确定风险是否可容许的全过程。

2.0.18 容量管理（Capacity Management）

对于基础设施在空间、电力承载能力、制冷能力等方面的评估，以满足IT 数据存储和处理的需要容量。为了实现其目标，容量管理需要与业务及IT 战略流程保持密切的联系。

2.0.19 资产管理（Asset Management）

对于数据中心基础设施中每个资产建立独有的标识，并详细进行资产描述、制造商、型号、安装日期、保修期等信息的记录管理。

**3 基本规定**

3.0.1 数据中心应划分为A、B、C三级，分级原则应按现行国家标准《数据中心设计规范》GB50174的要求执行。

3.0.2 数据中心等级评定应分为设计阶段、施工阶段和运维阶段，各阶段的等级评定宜与项目同期进行。

3.0.3 数据中心设计阶段的评定要求除应符合本标准的规定外，尚应符合现行国家标准《数据中心设计规范》GB50174的有关规定。

3.0.4 数据中心实施阶段的评定要求除应符合本标准的规定外，尚应符合现行国家标准《数据中心基础设施施工及验收规范》GB50462的有关规定。

3.0.5 数据中心运行和维护阶段的评定要求除应符合本标准的规定外，尚应符合现行协会标准《数据中心基础设施运维标准》CECSXXXX的有关规定。

**4 设计阶段等级评定**

4.0.1 设计阶段等级评定的主要内容应包括数据中心选址。

4.0.2 数据中心设计阶段的等级应根据设计文件进行评审和确定，宜从规划和方案设计阶段开始，应以施工图为最终评审文件。

4.0.3 A级数据中心设计阶段等级评定应按照表4.0.3-1执行，B级数据中心设计阶段等级评定应按照表4.0.3-2执行，C级数据中心设计阶段等级评定应按照表4.0.3-3执行。

**5 实施阶段等级评定**

5.0.1 数据中心实施阶段等级评定宜在完成设计阶段等级评定后进行，也可按照设计阶段等级评定的方法评审相关设计文件后进行实施阶段等级评定。

**5.0.1 条文说明：**如数据中心已经取得设计等级认证的，则可直接进入实施等级认证下一项流程；如数据中心未取得设计等级认证，则需先按照设计等级评定方法的要求评审相关设计图纸等资料确保其符合相对应的设计等级技术要求。

5.0.2 数据中心实施阶段等级评定应符合下列要求：

1 工程施工应符合设计要求；

2 工程施工质量应符合国家及地方相关质量要求；

3 各项检测应达到设计和检测标准的要求。

5.0.3 根据数据中心等级评定技术要求，验证现场各系统有效性，并保障实施结果不低于技术要求的规定；关键条款必须100%验证并合格，非关键条款100%验证，且不合格项不得多于10项。

**5.0.3 条文说明：**实施验证阶段验证方须收集有效证据，或采取有效手段，证明各系统的有效性。如可采取模拟故障的方法来验证某一个区域或部位系统的有效性，例如：技术要求电源是冗余的，则可分别采用其中一路拉闸的方法来验证其有效性。同时，需有对应系统的操作方法或流程。对于项目中同一类验证项目验证点n≤4的，需100%覆盖验证，4<n≤20的，按不低于50%验证且不少于4处，n>20时，可按不低于10处进行验证。

5.0.4 对于整体设计分步实施的项目，实施等级评定只对所申请并已实施完成的部分有效；

5.0.5 当设计审核及测试验证存在不符合项时，应在规定期限内完成整改，对整改结果以必要的方式进行验证，整改验证通过，按照实际等级给出评价结论。若未能按期完成整改的或整改不通过的，按评定结论不符合处理。

5.0.6 实施阶段等级评定应按照表5.0.6执行，评定结论应与检查结果相符，实施阶段等级评定结论有效期为3年。

**6 运维阶段等级评定**

**6.1 一般规定**

6.1.1 运维阶段等级评定的主要内容应包括数据中心运维组织架构与员工职责分配、管理制度与流程建设、基础设施监测、基础设施的维护、容量规划与演练、资产管理、外包管理、验收投产管理。

6.1.1条文说明：数据中心运维组织架构与员工职责的分配是构建和保障数据中心运行的基础。

6.1.2 运维阶段等级评定可分为投产前和投产后两个阶段。投产后可对一个运行周期（四个自然季节）进行综合评定，也可用于定级后复查（包括等级的升、降级）。

6.1.2条文说明

**6.2 组织架构**

6.2.1 运维团队应有清晰的组织架构，对各岗位应有明确的职责分工和分界，当架构和岗位调整时，其职责应做相应的权责匹配和更新。

**6.2.1条文说明：**数据中心运行离不开制度和流程的保障，应按照组织架构编制和设定明确的工作职责和管理规定，建立和落实团队、岗位和人员管理制度。制定与人力资源相关管理制度，如：员工行为规范、考勤管理制度、人员管理考核制度、员工内部调动/辞职/离职/劳动合同管理规定、保密协议等。

6.2.2 根据工作内容，数据中心应设置客户服务、运维巡检、技术管理、综合管理等部门。

6.2.2 条文说明：根据数据中心的规模、管理体制的差异，部门的设置数量与名称可做相应的调整。

6.2.3 客户服务部门应受理内外部的服务请求，做好流转、监督和回复，进行服务质量的跟踪。

6.2.4 运维巡检部门应对基础设施进行巡检，担任值班工作，第一时间发现故障或问题，及时报告和处理。

6.2.5 技术管理部门应对基础设施提供运维技术支持，解决技术问题，承担数据中心基础设施的安装、调试和维护。其人员组成应包括电气、暖通、弱电、消防等技术人员。

6.2.6 综合管理部门应担负数据中心的行政和后勤保障。

**6.3 人员配备**

6.3.1 按照基础实施的专业设置配备相应的岗位，配备专业的技术人员，人员的配备可在编，也可采取外包方式。

数据中心基础设施运维人员的配备应根据运维管理目标或SLA 来确定。高等级的数据中心，可按照7X24小时 的运行要求配置运维人员。

高等级以及具有一定规模的数据中心，每个班组应配备具有电力、暖通、弱电专业能力的运维人员，以达到“即时应急响应”的工作状态。等级相对低的数据中心，按需配备相应专业人员，达到“即时报警”的工作状态。

数据中心基础设施运维管理团队的关键管理人员或关键岗位人员在正常运维工作开展中应采用A、B 角色配置，日常工作中应具备角关键岗位应有人员备份和储备。

**6.4 运维人员技术要求**

对需要持证以及专业技能要求的岗位，上岗人员应具备国家要求的相应资格证书。应在运维管理程序中明确规定资质等级与操作权限的一致性。数据中心应建立良好的循环机制，人员可进行岗位轮换和交叉培训，使所有人员掌握全面的基础知识。

**6.5 岗位培训与考核**

 对数据中心员工应进行完整及严格的培训，培训内容应包括数据中心基础设施的所有系统的工作原理、操作流程、应急预案、以及管理制度等，培训的结果与年度绩效考核相关联。

**6.6 管理制度与流程建设**

**6.6.1**运行服务管理制度应包括服务体系、服务承诺协议SLA（根据数据中心的服务模式而定）、服务台管理、机房（重要区域）管理、运维值班、巡检、操作管理、资产管理等制度。建立服务台、事件处理、变更、问题管理的流程。

**6.6.2** 数据中心的运行应建立相应安全管理制度，安全管理制度应包括以下的内容，并应符合表6.6.2的要求。

1 数据中心应建立和落实物理环境安全管理制度，明确安全区域、规范区域访问管理，减少未授权访问所造成的风险。

2 数据中心应与录用的人员签署保密协议，制定安全与服务管理安全责任和与之相配套的安全责任管理细则。

3 数据中心应建立安全事件处理、重大事件上报（通报）流程的管理。

表6.6.2 安全管理制度一览表

|  |  |  |  |
| --- | --- | --- | --- |
| 安全管理 |  | 内容 | 符合度 |
| 1 | 安全与服务管理安全责任管理办法 |  |
| 2 | 安全与服务管理责任细则 |  |
| 3 | 安全组织架构与责任 |  |
| 4 | 第三方安全与审计管理 |  |
| 5 | 安全风险评估管理 |  |
| 6 | 外部服务管理 |  |
| 7 | 安全事件处理 |  |
| 8 | 问题管理 |  |
| 9 | 重大事件上报管理 |  |
| 10 | 内部审计管理 |  |

**6.6.3** 数据中心应建立服务体系和管理流程，服务体系和管理流程应符合表6.6.3的要求。

表6.6.3 服务体系和管理流程一览表

|  |  |  |  |
| --- | --- | --- | --- |
| 服务体系管理流程 |  | 内容 | 符合度 |
| 1 | 服务体系 |  |
| 2 | 服务的组织架构与人员配备 |  |
| 3 | 服务台的建设 |  |
| 4 | 事件管理流程 |  |
| 5 | 变更管理流程 |  |
| 6 | CMDB管理与维护 |  |
| 7 | 问题管理流程 |  |
| 8 | 资产管理与维护 |  |
| 9 | 供应商管理 |  |
| 10 | 巡检 |  |
| 11 | 动环监控 |  |
| 12 |  |  |

**6.7 基础设施监控**

数据中心应具备机房环境监控系统，对基础设施设备、机房环境状况、安防系统状况进行7X24 小时实时监测，监测记录保存时间应满足故障诊断、事后审计的需要。数据中心应对基础设施的运行提供实时的监测能力。

**1、建立数据中心应搭建基础设施管理系统（平台）**

对C级的数据中心至少搭建基础设施的动环监控系统。对A/B级数据中心应搭建基础设施管理系统（DCIM或DCOM），通过技术的手段实现基础实施的运行监控。

2、针对于不同的数据中心管理目标，对于A/B/C等级数据中心要求运维人员做到全年7x24 小时的值守。对C级数据中心可将24小时的监控与楼宇消控中心统一管理。每一班需要有至少一名值班长（资深人员），具备对于现场紧急情况进行快速处置的能力。

3、对具有分中心中心或多中心的数据中心，主中心应能远程访问分中心动环和安防系统，平行多中心运行的数据中心应建立互为监控的机制和互备的监控功能，实施远程监控。

|  |  |  |  |
| --- | --- | --- | --- |
| 等级 | 人员配备 | 人员要求 | 符合度 |
| A | 7\*24小时值守，应能随时联系并召集相关系统维护人员、供应商维护人员 | 至少配备一名值班长和覆盖电力、暖通和弱电专业人员， |  |
| B | 7\*24小时值守，应能随时联系并召集相关系统维护人员、供应商维护人员 | 至少配备覆盖电力、暖通和弱电专业人员， |  |
| C | 7\*24小时值守（可与消控中心联合），应能随时联系并召集相关系统维护人员、供应商维护人员 |  |  |

4、24小时监控并记录基础设施、消防、安防等系统的运行，定时安排对基础设施进行现场的巡视，基础设施故障时记录和通知相关人员处理，做好交接班。监控内容有（但不局限于）：

|  |  |
| --- | --- |
| 监控和巡视对象 | 监控内容 |
| 空调系统（精密空调系统、新风系统） | 空调系统的运行、环境温度、环境湿度、出风温度、回风温度，告警情况等 |
| 电力系统（供配电系统、UPS系统、发电机系统、防雷接地系统、） | 供配电系统：电流、电压、功率因数、有功功率、无功功率、谐波等 |
| 发电机：启停情况、电流、电压、负载率、控制系统供电情况等 |
| UPS:输入电流电压、输出电流电压、频率、负载率、温度、报警情况、电池充电/放电电压等 |
| 电源使用效率：PUE值（通过监控软件监测或计算得出） |
| 防雷接地系统：浪涌保护器、避雷器状态等 |
| 安防系统（消防系统、视频监控系统和门禁系统） | 消防系统：消防控制系统状态、气体灭火钢瓶压力、灭火器有效期检查 |
| 视频监控系统: 告警情况、监控录像等 |
| 门禁系统：门禁状态、告警情况 |

5、编制监测的日报、周报、月报和年报。

**6.8基础设施维护**

数据中心基础设施的维护评测基点如下：

**6.8.1基础设施的预防性检查**

 基础设施预防性检查是数据中心日常运行必不可少的项目，预防性检查的内容如下：

|  |  |  |
| --- | --- | --- |
| 服务对象 | 性能检查内容 | 脆弱性检查内容 |
| 空调系统 | 精密空调 | 高压压力、低压压力（风冷系统），冷冻水压力、温度，冷却水压力、温度（水冷系统），风机运行情况，灰尘情况等 | 机房热点情况、室内机漏水检查、室外风机运转情况、加湿罐阳极棒检查、过滤网检查等 |
| 新风系统 | 风机运行情况、风速，预处理系统工作状态，上下水情况等 | 过滤网检查、风压差检查 |
| 电力系统 | 配电系统 | 接地电阻、零序电流、器件发热情况等 | 导线、器件发热情况，防浪涌器件情况等 |
| 发电机 | 转速、发热情况等 | 油位，吸气、排烟通道等 |
| UPS系统 | 器件发热情况、电池情况（外观、非免维护电池检查液位、接线柱）、检查通风情况（风扇、入气口、出气口）等 | 器件、导线发热情况，电池放电时间、通风情况等 |
| 防雷接地系统 | 接地电阻测试 | 引下线检查、接地汇接排检查 |
| 安防系统 | 消防系统 | 钢瓶压力、有效期、探头污染等 | 启动瓶、管道开关、气体压力等 |
| 视频监控系统 | 画面清晰度（不同照度情况下）、录像硬盘（磁带）容量、云台运行等 | 监控系统运行状态、监控死角问题等 |
| 门禁系统 | 服务器、控制器、读卡器、门磁等工作状态 | 门禁系统与消防系统和视频监控系统的联动检查（如果有此功能），异常情况报警检查 |
| 综合布线系统 | 光纤、铜缆链路测试，性能测试等 | 线缆两端应贴有识别标签，标志要与实际拓扑图完全一致 |

**6.8.2数据中心基础设施日常维护**

 数据中心基础设施的日常维护有；

| 服务对象 | 基础类操作 | 测试类操作 | 数据类操作 |
| --- | --- | --- | --- |
| 空调系统 | 精密空调 | 启停机、清洗更换滤网、清洗更换加湿系统、清洁冷凝器等 | 漏水报警测试、周期性主备切换/应急演练等 | 运行日志备份，报警记录备份、清除等 |
| 新风系统 | 启停机、清洗更换滤网等 | 消防联动测试 | 运行记录备份（如果有） |
| 电力系统 | 配电系统 | 除尘、合闸、分闸等 | 互投测试等 | 运行记录备份 |
| 发电机 | 更换三滤、机油、清洁、防冻液等 | 空载测试、带载测试、切换演练等 | 运行日志备份，报警记录备份、清除等 |
| UPS系统 | 旁路、清洁等 | 旁路测试、电池放电测试、周期性主备切换/应急演练等 | 运行日志备份，报警记录备份、清除等 |
| 防雷接地系统 | 接地端子、汇流排紧固，浪涌、防雷保护器复原等 | 接地电阻测试 |  |
| 安防系统 | 消防系统 | 探头检测等 | 启动测试、探头测试等 | 报警记录备份、清除 |
| 视频监控系统 | 视频监控头清洁，云台保养 | 器件灵敏度、画面清晰度（不同照度情况下）、云台运行等 | 出入记录导出、备份，监控图像记录备份、清除，报警记录备份、清除等 |
| 门禁系统 | 门禁授权等 | 门禁系统与消防系统和视频监控系统的联动检查测试（如果有此功能），掉电测试 | 运行日志备份，报警记录备份、清除等 |
| 综合布线系统 | 线路跳接等 | 链路测试、性能测试 | 布线系统拓扑图数据更新 |

**6.9 容量管理**

6.9.1 数据中心运行过程中应进行容量管理，容量管理应包括空间管理、能力管理、能效管理和人力成本管理。

**6.9.1条文说明：**容量管理是衡量和评估一个数据中心运行管理能力重要指标。

6.9.2空间管理应综合平衡电子信息设备布置空间、基础设施安装空间、管线安装空间，并应设置运行维护、设备运输和安全疏散通道。

6.9.3能力管理应确保互联网接入容量、电力、水、燃气和等能源供应，并确保综合布线信息点容量、供配电和空调等容量满足运行要求。

6.9.4能效管理应对数据中心的电和水的使用情况进行计量和累计，计算出年平均电能使用的能效（PUE）和水使用的能效（WUE）。

6.9.5人力成本管理应对计算数据中心人力资源投入成本，并提高劳动生产率。

6.9.5数据中心基础设施运维部门应全面了解并记录数据中心的容量数据，统计和分析运行的规律和趋势，提出不断优化运行方案。当基础设施不能满足IT 增长的需求时，应提前制定并上报扩容或者新建数据中心的计划。

**6.10 应急预案与服务连续性**

数据中心应将应急预案和灾难恢复管理纳入业务连续性管理框架。建立应急管理组织架构，明确应急预案和灾难恢复管理机制和流程。数据中心应急预案与服务连续性评测基点如下：

**6.10.1 风险分析与评估**

数据中心应统筹规划基础设施的连续性计划和灾难恢复工作，通过风险分析识别和评估业务运营中断所造成的影响和损失，明确业务连续性管理重点，明确灾难恢复策略、预案并及时更新。根据业务重要程度实现差异化管理，确定恢复优先顺序和恢复等级。对于每个数据中心应当至少每三年开展一次全面运行风险影响分析，并形成运行风险影响分析报告。

**6.10.2 应急等级划分**

针对不同等级的灾难事件分别制定应急处理流程，明确紧急情况发生时的紧急处理流程和业务恢复机制等。根据系统的重要程度和场景，建立不同等级的灾难备份环境（包括建立同城或异地备份），从而提高数据中心对较大规模灾难事件的抵御能力。

**10.6.3 确定RTO和RPO**

应当综合分析数据中心业务运营中断可能产生的损失与业务恢复成本，结合业务服务时效性、服务周期等运行特点，确定重要业务恢复时间目标（业务RTO）、业务恢复点目标（业务RPO）。原则上重要业务恢复时间目标不得大于4小时，重要业务恢复点目标不得大于半小时。

**6.10.3 建立业务连续性计划和灾难恢复预案**

应依据数据中心业务发展的总体目标、经营规模以及风险控制的基本策略，制定相应的应急预案，制定应急演练计划，业务连续性计划和应急恢复预案应包括但不限于以下内容：

连续性计划和灾难恢复指挥小组和工作小组人员组成及联系方式、汇报路线和沟通协调机制、灾难恢复资源分配、基础设施与信息系统的恢复优先次序、灾难恢复与回切流程及时效性要求、应急操作流程、对外沟通机制、最终用户操作指导及第三方技术支持和应急响应服务等内容。

**6.10.4 应急预案需要的资源与培训**

数据中心为应急预案和灾难恢复提供充分的资源保障，包括基础设施、网络通信、运维及技术支持人力资源。每年必须开展应急预案、操作流程的技术培训等。

**6.10.5 建立应急预案和灾难恢复有效性测试验证机制**

针对应急和灾难恢复的预案、流程进行测试验证，验证的内容包括支持应急计划和灾难恢复系统的硬件环境、系统环境、业务功能、业务数据等验证。

**6.10.6 应急计划和灾难恢复演练**

数据中心每年应实施相关系统专项应急演练，每年至少进行一次重要信息系统全面应急切换演练，以真实业务接管为目标，验证应急系统有效接管生产系统及安全回切的能力。

**6.10.7 应急演练报告**

进行应急计划和灾难演练时，按要求向监管机构提交全面灾备切换和真实业务接管演练报告。因灾难事件启动灾难恢复或将灾备中心回切至生产中心后，应及时向监管机构报告，报告内容包括但不限于：灾难事件发生时间、影响范围和程度，事件起因、应急处置措施、灾难恢复实施情况和结果、回切方案。

|  |
| --- |
| 应急与恢复 |
| 　 | 　测试基点 | 符合度 |
| 1 | 应急领导小组，工作职责、工作小组 | 　 |
| 2 | 应急计划和相关系统的应急预案 | 　 |
| 3 | 应急演练记录 | 　 |
| 4 | 应急领导小组工作例会记录 | 　 |
| 5 | 应急领导小组专项会议记录 | 　 |
|  | 每年至少进行一次重要信息系统专项应急演练，三年全覆盖演练 |  |
|  |  |  |

**6.10.8 资产管理**

资产管理是保障数据中心运行的重要组成部分，数据中心的资产管理评测基点如下：

1、数据中心运行应建立基础设施的全生命周期管理，生命周期管理是指从数据中心规划、设计、建设到运维直至停用“报废”的全过程。

2、实施基础实施运行的风险评估，制定设备维护、升级或更换的计划，及时报告给运维管理部门。对于冗余设备宜设立轮换运行机制，以延长整体设备的生命周期。

3、数据中心应建立资产管理系统，可以是独立的系统，也可以建立在数据中心基础设施管理（DCIM DCOM）平台中，完整及实时更新的资产数据库。数据库应包括所有关键基础设施设备的清单，还应记录设备设施的运行情况、事件情况、变更情况、维护保养频次等信息。资产数据库应最少包括以下信息：

资 产 ID： 每个资产的唯一标识号

分类： 系统分类、设备分类

描 述： 资产的文字说明

制 造： 资产的制造厂家

型 号： 制造厂家的产品型号

规 格： 资产的规格或者标称值、配置

位 置： 位置ID（房间或区域）

购 买 人： 资产维护的负责人

序 列 号： 制造厂家的序列号

安装日期： 资产的投产日期

保修期限： 保修到期的日期

保修单位：保修单位名称、维护工程师、联系电话等

更 换： 预计的资产更换日期

维护频次： 年检、季检、月检等

维修信息：每次的维护记录（维护（修）时间、维护内容、跟换的部件、版本号（系统升级时）等）

报废：报废原因、报废申请和审批、报废处置

**6.10.9** 供应商管理。

 数据中心服务外包一般有以下两种形式:

(一)基础设施类:外包服务商提供数据中心机房、配套设施的租赁和相应的运维服务。

(二)运营维护类:外包服务商向建设方的数据中心提供信息系统或基础设施的日常运行、维护等服务。

数据中心服务外包管理评测基点如下：

**（1）数据中心外包服务的责任**

数据中心主管部门应对外包外包服务担负最终管理责任，应推动和完善外包风险管理体系建设，确保数据中心的运行有效应对外包风险。

数据中心应制定数据中心服务外包管理制度、流程，建立全面

的风险控制机制。

**（2） 服务商选择**

在选择数据中心外包服务商时，应充分审查、评估外包服务商的资质、专业能力和服务方案，对外包服务商进行风险评估，考查其服务能力是否足以承担相应的责任。评估包括:外包服务商的企业信誉及财务稳定性，外包服务商的信息安全和信息科技服务管理体系，行业服务经验等。提供数据中心基础设施外包服务的服务商，其运行环境应符合行业要求，并具有完备的安全管理规范。

**（3） 服务合同管理**

应与数据中心外包服务商签订书面合同，在合同中明确重要事项，包括但不限于双方的权利和义务、外包服务水平、服务的可靠性、服务的可用性、信息安全控制、服务持续性计划、审计、合规性要求、违约赔偿，以及服务SLA等。

**（4） 服务管理**

数据中心应加强外包服务活动的安全管理，设置相应的团队监督、检查、考核外包服务商的服务，服务管理的内容包括但不限于：

1、将外包服务安全管理纳入数据中心的整体安全策略，保障业务、管理和客户敏感数据信息安全。

2、按照"必需知道"和"最小授权"原则，严格控制外包服务商信息访问的权限，签订安全保密协议，要求外包服务商不得外泄露所接触的信息。

3、要求外包服务商保留操作痕迹、记录完整的日志，相关内容和保存期限应满足事件分析、安全取证、独立审计和监督检查需要。

4、要求外包服务商遵守建设方有关信息科技风险管理制度和流程。

5、建设方应要求外包服务商每年至少开展一次信息安全风险评估并提交评估报告。

6、制定数据中心外包服务应急计划，制订供应商替换方案，以应对外包服务商破产、不可抗力或其它潜在问题导致服务中断或服务水平下降的情形，支持数据中心连续、可靠运行。

7、建立外包服务考核、评价机制，定期对外包服务活动和外包服务商的服务能力进行审核和评估，确保获得持续、稳定的外包服务。

**6.10.10 投产验收管理**

投产验收管理是数据中心由建设转为运行必经的过程，交付运营前全系统验证是否完备对后期的运营至关重要。投产验收管理评测基点如下：

1、数据中心建设可研、立项、环评、投资以及报审报批材料；

2、建筑规划报审、设计方案、施工图（含图审）、工程量清单、预算、防雷接地、消防设计报审等材料；

3、施工计划、进度、施工变更（含签证）、施工过程监理；

4、单项测试验收、系统联调、第三方检测、监管部门强制验收（消防、防雷）、竣工验收报告、决算审计等；

5、建设中设备采购合同、各基础设施设备的随机资料、操作和维护手册等、设备供应商信息、出入库等文档管理。

6、投产前组织架构是否健全，各岗位人员是否到位；

7、岗位培训是否完成；

8、制度和流程是否建立；

9、各系统运行是否完成规定的试运行期，是否进入正常状态；

10、投产前应急预案是否通过演练，文档是否齐全。

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **项目** | **内容** | **符合度** |
| 1 | 组织架构 | 部门设置 |  |
| 人员 | 岗位设置 | 　 |
| 2 | A/B角制度 | 是否有A/B角配置。 | 　 |
| 3 | 人员离岗管理 | 调离人员在离岗前是否有完善的离岗交接手续，有关人员签字齐全，交接资料妥善保管。 | 　 |
| 4 | 培训 | 是否组织在岗人员，特别是技术骨干人员参加业务或技能的培训，以便更好完成本职工作。 | 　 |
| 5 | 岗位设置 | 需要持证上岗以及专业技能的要求与执行情况 | 　 |

|  |  |  |  |
| --- | --- | --- | --- |
| 组织架构 |  | 内容 | 符合度 |
| 1 | 组织架构及工作职能 |  |
| 2 | 内设团队工作职责 |  |
| 3 | 岗位职责 |  |
| 4 | 岗位AB角管理 |  |
| 5 | 职责分离 |  |
| 6 | 保密协议 |  |
| 7 | 员工职位管理办法 |  |
| 8 | 职位聘任协议 |  |
| 9 | 员工内部调动/辞职/离职/劳动合同 |  |
| 10 | 员工教育培训管理 |  |
| 11 | 员工考勤管理 |  |
| 12 | 第三方（含外包）管理 |  |

|  |  |  |  |
| --- | --- | --- | --- |
| 物理安全访问控制 |  | 内容 | 符合度 |
| 1 | 数据中心安全防控策略 |  |
| 2 | 物理安全边界与物理入口控制 |  |
| 3 | 公共访问和交接区域管理 |  |
| 4 | 办公场所和辅助设施保护管理 |  |
| 5 | 防止外部和环境威胁 |  |
| 6 | 门禁管理 |  |
| 7 | 值班管理 |  |
|  |  |  |

在不同工况及不同外界气候条件下的电力使用效率PUE 的变化情况，对采用冷水机组的空调系统应全面了解并记录数据中心在不同工况及不同外界气候条件下的水使用效率WUE 的变化情况，