平安数据中心高可用运维白皮书

2018 年 5 月

平安科技

前言

中国平安数据中心在十多年的发展过程中，遵从 ITIL、ISO9001、ISO20000、ISO27001、M&O 等多个标准，不断制定、优化数据中心的工作规范和指南，形成了一整套标准的运维体系。数据中心运维团队依据标准体系的指导，通过兢兢业业、一丝不苟的工作，保障了平安数据中心的高可用性。

平安数据中心的高可用离开不员工的辛苦工作，以及各供应商的保障支持，在此，特意向日夜奋战的员工和供应商进行特别的感谢。

为实现平安的企业社会责任，推动中国数据中心尤其是金融高可用数据中心的运维管理的提升，平安数据中心团队总结十多年的运维经验，编制了《平安数据中心高可用运维白皮书》，旨在总结和分享平安数据中心在打造高可用金融+互联网数据中心的优秀经验，与行业内各专家同仁一道为国家大数据时代建设贡献力量。

感谢中国数据中心工作组组长钟总、Uptime 北亚区董事总监胡总对本书的支持，感谢辛苦编制此书的作者。

本书若有错漏之处，恳请各位专家同行批评指正。

平安科技（深圳）有限公司数据中心 著

平安科技

序 1

2009 年，中国平安开始规划建设深圳观澜数据中心，我有幸作为这个项目的总设计师，参与了整个项目的建设，见证了中国平安紧跟国家战略步伐，大力推进中国平安信息化之路。

中国平安作为中国金融行业较早建设数据中心的企业，对数据中心的建设和运维有着深刻理解，培育造就了一批数据中心领域的专家，为平安集团步入“金融+互联网”3.0 时代、为中国数据中心行业健康发展做出了突出贡献。

数据中心全生命周期包括：需求分析、规划设计、施工安装、检测验收、运维管理。其中运维管理是数据中心生命周期中最后一个、也是历时最长的一个阶段，真可谓：三分建设，七分管理。运维管理参与设计和实施，从项目开始就将运维需求落实到设计和实施中，其工作范围涵盖数据中心全生命周期，是通过科学运维管理，实现为业务提供数据信息支持，实现企业发展目标的过程。

本书是平安人不忘初心、牢记使命、不断奋进、努力实践的结晶。内容包括数据中心运维标准化建设、组织架构、安全管理、运维实践和质量体系等。

本书凝聚了平安人对数据中心的热爱和孜孜以求的科学精神，感谢为此书出版付出辛勤劳动的编写团队，希望大家能从此书中得到启迪和帮助。

钟景华

中国数据中心工作组（CDCC）组长

2018.5

平安科技

序 2

对于数据中心的标准：Uptime Institute 发展近二十年的 Tier 的分级拓扑(Topology)标准，通过 Tier I 至 IV 的标记系统以用来表示数据中心的物理基础设施的可用性。此标准自问世以来，已被全球广泛的採用在各地数据中心的设计及建置之中。

或許当有人因业务需要说：我想要个数据中心。就有人会转过身来说：我将为你建数据中心。 但是却没有多说是否他们在谈论着同样的性能产出。 我常在一些场合里说：一个数据中心的生命周期，在设计建置阶段可短至数月也有长到一至二年，但其运营却长达十年或十几年。因此要设计及建置符合营运目标及维运需求的数据中心才是 Tier 标准的精神所在。

Uptime Institute 的每年行业调查数据均显示：有一半左右的企业 IT 组织曾在过去 12 个月期间经历过他们自有数据中心影响业务的停机，也有近三分之一的企业 IT 组织在前 12 个月内曾经历主机托管提供商的服务中断。对于这些事件大多指向：操作员的人为错误。这种说法可能涵盖了程序的错误和资源的缺乏，或欠缺管理及不善决定。而且这些责任常都是落到操作人员在未能及时救援成功的情况下。

其实大多数的情况，失败可以归因于高级管理层之决定（例如：设计妥协，预算削减，裁减工作人员，供应商选择及资源的分配），其可溯自事件发生之前的时间和空间的，譬如：什么决定导致前线操作人员没有好的准备或未受过足够的训练，因此对事件的反应作出处理不当的情况。

随着所有业务职能部门对数据需求不断的提高，如今的数据中心的 IT 和基础设施利益相关者持续面临巨大的压力，在实现价值的同时还要维护成本和效率。因此，数据中心管理和运营 Management & Operations (M&O) 的评估认证是可以提供相关指导和框架基础，也是推动实施数据中心有效的管理和运营的最佳实践。

数据中心管理及运营准则应是对内部所有小组、部门、文化和实践中都适用的。其相关于人员配置、组织和培训实践、预防性维护方案、运营条件，以及计划、管理和协调实践和资源。这一切不仅是对数据中心操作团队，也应包含服务供应商和领导层所应负责的事务并为其提供了有用的信息。

今天在中国数据中心市场，欣见平安科技为平安集团发展企业数据中心运维规范的白皮书，期待其能带给平安集团的数据中心工作同仁诸多帮助。

Philip Hu 胡嘉庆

Uptime Institute 北亚区董事总监

May 2018

目录

第一章　平安数据中心高可用运维白皮书介绍 1

1.1．数据中心高可用运维白皮书目的、实用范围 1

1.2．数据中心高可用运维白皮书内容及简介 1

第二章 平安数据中心运维标准化建设 3

2.1．精细化管理理论和方法 3

2.1.1．精细化管理的概念 3

2.1.2．精细化管理在数据中心运维中的应用 3

2.2．运维 ITIL 框架 4

2.2.1．事件管理 4

2.2.2．问题管理 6

2.2.3．变更管理 6

2.3．UPTIME M&O 实践 7

2.3.1．人员组织 8

2.3.2．维护管理 9

2.3.3．培训管理 10

2.3.4．计划、协调与管理 10

2.3.5．运行状况 11

第三章 数据中心安全管理 12

3.1．信息安全管理 12

3.2．物理安全管理 13

3.2.1．物理安全配置 13

3.2.2．术语及定义 13

3.2.3．程序 14

3.2.4．人员进出登记制度 15

3.2.5．物品进出管理 17

3.2.6．消防安全管理制度 17

3.3．人员安全管理 18

3.3.1．人员安全培训 18

3.3.2．日常运维安全管理 19

第四章 人员保障与发展 21

4.1．组织架构.....21
4.2．区域和人员职责精细化分配.....22
4.3．人员培训.....25
4.3.1．新员工培训.....25
4.3.2．培训大纲.....26
4.3.3．培训实施程序.....27
4.4．人员发展.....27
4.4.1．员工例行培训.....28
4.4.2．员工专项培训.....28
4.5．供应商保障.....28
4.5.1．供应商培训及要求.....28
4.5.2．服务 SLA.....29
4.5.3．资质要求.....29
4.5.4．考核机制.....30
第五章　可靠性运维分析实践.....31
5.1．日常巡检概述.....31
5.1.1．日常巡检基本要求.....31
5.1.2．巡检频率及巡检方式.....31
5.1.3．中、低压开关柜日常巡检.....32
5.1.4．UPS 不间断电源日常巡检.....32
5.1.5．精密配电系统日常巡检.....32
5.1.6．柴发系统日常巡检.....33
5.1.7．暖通空调系统日常巡检.....34
5.1.8．消防系统日常巡检.....34
5.1.9．安防系统日常巡检.....35
5.1.10．弱电监控系统日常巡检.....35
5.2．设备预防性维护介绍.....35
5.2.1．设备预防性维护要求.....36
5.2.2．设备预防性检查、维护、操作内容.....36
5.2.3．预防性维护案例介绍.....37
5.3．预测性维护介绍.....44
5.3.1．预测性维护要求.....45
5.3.2．预测性维护项目.....45

5.4．应急演练介绍.....45
5.4.1．应急演练要求.....45
5.4.2．应急演练项目.....46
5.5．系统可用性检查.....46
5.5.1．机房基础设施月度检查.....46
5.5.2．机房基础设施场地环境检查.....46
5.5.3．机房基础设施其它信息核查.....47
5.6．生命周期管理.....47
5.6.1．中压柜生命周期规划管理.....47
5.6.2．低压柜生命周期规划管理.....47
5.6.3．变压器生命周期规划管理.....48
5.6.4．柴油发电机生命周期规划管理.....48
5.6.5．UPS 生命周期规划管理.....48
5.6.6．冷水机组生命周期规划管理.....48
5.7． 风险管理.....48
5.7.1．缩略语和定义.....49
5.7.2．风险识别.....49
5.7.3．风险管理表.....50
5.8．平安数据中心资产管理.....51
5.8.1．平安数据中心资产管理的特性.....51
5.8.2．平安数据中心资产管理制度化建设.....51
5.8.3．开发适用于自身数据中心管理需要的资产管理系统.....52
5.8.4．数据中心资产管理系统使用案例.....53
5.8.5．数据中心资产现场管理.....54
5.9．数据中心日常管理.....56
5.9.1．平安数据中心日常管理的特性.....56
5.9.2．平安数据中心日常管理制度建设.....56
5.9.3．开发适用于自身数据中心的 IDC 管理系统.....59
第六章、运维质量保障体系.....62
6.1．内部审核.....62
6.1.1．科技数据中心内部审核.....62
6.1.2．集团公司内部审核.....64
6.2．外部审核.....66

6.2.1．M&O 换证审核 66
6.2.2．ISO9001 审核 67
6.2.3．ISO27001 审核 69
6.2.4．ISO20000 审核 69

第一章 平安数据中心高可用运维白皮书介绍

1.1．数据中心高可用运维白皮书目的、实用范围

随着平安集团步入“金融+互联网”的 3.0 时代，平安确立了未来十年深化 “金融+科技” 、探索“金融+生态”的战略规划，以“国际领先的科技型个人金融生活服务集团”为目标，将创新科技聚焦于大金融资产、大医疗健康两大产业，采用区块链、云计算、人工智能、安全四大核心技术，并深度应用于“金融服务、医疗健康、汽车服务、房产服务、智慧城市”五大生态圈，至 2017 年末，集团互联网用户达到 4.36 亿，为了更好深化科技创新在客户经营中的应用，提升客户体验，对数据中心的规模和要求越来越高。

随着互联网+金融的不断发展，平安数据中心从原先的两地三中心，逐渐发展为多地多中心的模式，以北、上、深为中心，覆盖全国的数据中心集群。平安数据中心在建设方面，基于 GB50174《电子信息系统机房设计规范》A 级标准，参考 Tier Ⅳ国际标准，选用国际领先的、高可用的设备，为数据中心的高可用性打下了良好的基础。随着数据中心经过十多年的发展，累积了大量的规划、设计、运维知识和经验。

数据中心运维是一个不断变化、实践性很强的工作，平安数据中心运维从第一层次的规范化运维，到第二层次的精细化运维，再到第三层次的个性化运维，运维团队不断的挑战自我、提升自我，逐渐形成了自我特色的运维模式，在保障高可用性的前提下，探索节能智能，不断降低数据中心的运行 PUE，提高运维的效率。

平安数据中心高可用运维白皮书旨在分享平安数据中心如何打造一个标准化、精细化的运维体系，提高运维人员的专业知识和运维能力，实现数据中心的高可用性。

本白皮书对相关的认证标准进行解读，比如 ISO9001、M&O，结合实践经验，提供这些标准在运维过程中的实际落地方法，为行业内需要通过此类认证的用户提供指导。

本白皮书可供金融数据中心、通讯数据中心、网络运营商数据中心及企业数据中心的管理者，参与数据中心基础设施运维的人员参考和借鉴。

1.2．数据中心高可用运维白皮书内容及简介

本白皮书涵盖了以下章节和内容：

- 平安数据中心高可用数据中心运维白皮书介绍

  介绍了本白皮书编写的契机以及目的，总结多年的运维经验，为企业内部后续的数据中心体量增长提供高可靠的运维保障，也可供同行业的公司和个人进行参考，旨在建立满足自己实际业务需要的运维保障体系。

- 运维标准化建设

本章从运维的标准化出发，介绍了精细化管理的理论，以及在数据中心运维过程中的具体实践。

介绍了 ITIL 框架的基本信息，本书具体对事件管理、问题管理、变更管理方面进行详细的阐述。

介绍了 Uptime M&O 的背景以及其在数据中心运维的重要性，M&O 运维认证的五大方面，主要包括：人员与组织；保养与维护；人员培训；规划、协调与管理；运行状况管理。

- 数据中心安全管理

金融数据中心往往比其他数据中心对安全性、可管控性要求更高，本章从信息安全、物理安全、人员安全三个方面进行阐述。

- 人员保障与发展

本章介绍了平安数据中心为满足高可靠性所建立的组织架构体系，以及各个岗位的职责和分工。

介绍了用来满足本职工作的培训和模拟演练的培训课程设置，以及各种培训和演练的考核制度。

介绍了供应商的保障，对供应商服务人员的资质要求，SLA 要求，考核体系。

- 可靠性运维分析实践

介绍了数据中心基础设施各种设备的日常巡检频率、内容和要求。

在设备预防性维护方面，介绍了包括配电系统中 8 项设施的维护、暖通系统中 4 项设施的维护、弱电系统中 3 项设施的维护方法。

预测性维护方面，本白皮书介绍了预测性维护的目的和意义，列举了数据中心基础设施需要的预测性维护项目。

系统可靠性验证方面，介绍了数据中心可靠性验证的必要性和目的，并列举验证的类型和方法。

生命周期管理，介绍了基于数据中心的使用寿命而对高压配电柜、UPS、电池、精密空调、冷水机组制定的升级、年检、大修、改造、淘汰的规程。

介绍了数据中心的可用性检查，权威的第三方系统功能验证等。

介绍了风险管理、资产管理、现场管理方面的内容。

- 运维质量保障体系

本章介绍了检验数据中心运维质量的方式，ISO9001 质量体系检验，平安内部的安全部门审计，平安数据中心内部不同分组的互相审计，M&O 的认证审核等。

第二章 平安数据中心运维标准化建设

数据中心运维工作涉及两大方面：一是确保数据中心的稳定性而对数据中心各个环节进行维护；二是当数据中心内出现问题时，能够及时定位并且解决，以缩短故障时间。

围绕以上两个方面，平安数据中心的运维标准化建设，采用精细化管理的方法，总结自己的经验教训，将国际领先的 ISO 管理体系，ITIL 流程体系，M&O 运维标准合理的融合起来，形成具有独特的运维体系。

2.1．精细化管理理论和方法

2.1.1．精细化管理的概念

精细化管理是一种理念，一种文化。它是社会分工精细化、以及服务质量精细化对现代管理的必然要求。现代管理学认为，科学化管理有三个层次：第一个层次是规范化，第二层次是精细化，第三个层次是个性化。

2.1.2．精细化管理在数据中心运维中的应用

数据中心运维精细化管理，实际是一个为保障数据中心高可用性为目标分解细化和责任落实的过程，是高可用性这个目标能有效地贯彻到每个环节并发挥作用的过程，同时也是提升团队整体执行力的一个重要途径。

精细化运维是一个全员参与的过程，每一位员工既是精细化运维的对象、载体和参与者，也是精细化运维的主体和实施者。

如何实施精细化管理，平安数据中心将运维人员岗位分工进行精细化，职责分工进行精细化，运维平台进行精细化设置，设备维护保养流程进行精细化，客户服务进行精细化，以“精、准、细、严”为基本原则，通过提升改造员工素质技能，加强内部控制，强化精细化管理，从整体上提升数据中心的稳定和安全性。

“精”是精益求精，追求更好，是一种态度，将数据中心的管理和日常工作做到极致，按照数据中心高可用的要求，追求设施运行的最佳状态。

“准”是准确、准时，代表了运维的规范、认真的规则意识。信息要保持准确性，包括现场设备物理信息准确性，标示标签的准确性，设备数据的准确性，时钟的准确性，监控平台设备数据、状态的准确性，仪器仪表的准确性，流程的准确性，手册的准确性，这些信息是运维过程中风险识别、故障判断、故障处理的必要参考，信息的准确度直接关系到设备的最佳运行状态，以及故障能否及时处理，避免人为引起的二次故障。数据中心设备的日常维护事项众多，维护变更的安排是基于全面的风险评估后制定的，每一

项维护应该在规定的时间内，准时进行，避免在不当的时间内处理不当的事情。

“细”是细致、细微。运维中人员责任分工要细，各司其职，保障运维中各项工作落实到位；制度、规范要细，是质量考核的标准；标准的维护手册、标准的操作手册、标准的应急手册要细，确保在最不利的情况下，按照手册一步一步执行是安全可靠的；

“严”是严格、严谨，体现在对运维各个环节的执行和过程的控制。对数据中心运维的各项规章制度严格落实，控制质量。数据中心运维过程中，宁可失之于严，不可失之于宽。

平安数据中心运维团队严格按照精细化管理的要求，建设自有的运维标准，不断去检视流程、制度、规范、人员，挖掘潜在的能力，保障数据中心的高可用性。

2.2．运维 ITIL 框架

平安数据中心参考 ITIL 的流程，根据多年运维的实际情况，对模块进行精选，对应用最广的事件管理、问题管理、变更管理、服务请求管理、资产管理、安全管理进行描述，其中针对金融数据中心对安全的重要性，安全管理放在本白皮书的第三章进行单独说明，资产管理放在第五章内进行说明，本章只描述事件管理、问题管理、变更管理在平安数据中心运维工作中的应用。

平安数据中心对事件管理、问题管理、变更管理均在自有 Service Bot 系统中进行。Service Bot 系统中记录事件、服务请求、问题和变更的编号、上报人、上报时间、处理组、处理人、事件类型、事件来源、处理优先级、详细描述、事件原因分析、处理方案、处理过程等信息。

管理单中可以对事件、父事件、问题单、请求单、变更单五个信息相互关联。方便事件的升级和跟踪。

系统中将一个事件、问题和变更实施闭环管理，分为新建、分派、处理中、等待、已解决、已关闭 6 个状态，跟踪记录处理目标 SLA(服务等级协议)信息，关闭经上报人审核完成后给予满意度评价。

2.2.1．事件管理

数据中心事件管理的目标就是在出现事件时，通过内部的事件管理流程，采用既定的措施，尽可能的快速恢复系统的正常运行，避免造成业务中断。

事件管理的要素包括事件上报记录、事件级别定义、事件处理过程、事件升级机制、事件响应机制、事件状态，平安数据中心通过制定事件管理流程，在 Service Bot 系统中跟踪记录事件的整个过程。

2.2.1.1．事件定义

(1) 报警：定义报警的概念和范围。

(2) 故障：定义数据中心中故障的概念和范围。

(3) 一级故障：参考运行 SLA 要求，直接影响业务运行可靠性的故障定义为一级故障。

(4) 二级故障：基础设施设备中单个关键设备故障。需定义清楚关键设备。

(5) 三级故障：指对机房内设备的正常运行形成安全隐患但未造成实际影响的事件。

(6) UIOC：机房设备软硬件运行异常导致应用层面发生严重故障，为解决相应故障所启动的重大事件管理流程。

2.2.1.2．事件发现

基础设施运维人员通过例行巡检、远程监控、手机短信、拨号报警等方式了解到基础设施、机房设备或运行环境的报警信息，第一时间赶赴现场了解报警情况，获得报警的完整信息。如属基础设施或运行环境故障，应第一时间通知当班基础设施工程师，工程师根据具体情况判断是一级故障、二级故障或三级故障。

2.2.1.3．故障分级上报制度

- 当班基础设施工程师判断为三级故障，由基础设施工程师协调技工岗人员或相关服务商对故障进行排除与跟进。
- 如为二级以上故障，当班基础设施工程师于 2 分钟之内通知相应的小组负责人，小组负责人根据故障情况安排处理措施，并就故障排除进展适时通报管理者代表。
- 如为一级故障，小组负责人应于 2 分钟之内通知管理者代表，管理者代表 2 分钟之内通知中心经理，并每隔 2 小时汇报故障排除进展，中心经理根据故障具体情况通报公司相关领导，并确定是否启动 UIOC。

2.2.1.4．故障处理

- 基础设施工程师负责制，负责响应故障、判断故障、通报故障，协调资源对故障进行处理。
- 如为三级故障，则协调内部人员共同对故障进行处理，如果需要供应商紧急处理，应在 30 分钟内通知服务商人员安排维修，同时将故障处理过程向小组负责人汇报。
- 如为二级以上故障，应第一时间到达现场并通知小组负责人，如果需要供应商紧急处理，应在 10 分钟内通知厂家维护人员赶赴现场排除故障，如故障不能顺利排除，应敦促厂家启动紧急应对措施（如提供备机等），尽快排除故障。故障排除进展每隔 2 小时内通报小组负责人和管理者代表。如为一级故障，管理者代表汇报给中心经理。
- 所有故障处理完毕后，均应在在相关管理系统中填报故障事件，并记录故障处理全过程。

2.2.2．问题管理

问题是导致一个事件或者多个事件的根本原因，问题管理就是找到这些事件产生的根本原因，通过实施主动问题管理，在事件发生之前将问题发现并解决，从而减少事件发生的数量。问题管理往往时间周期比较长，需要诊断根源，制定恰当的解决方案，从根本上解决。

问题一般由风险或者事件转化而来，管理中，需要和风险、事件相关联，问题的定级可以参考后续平安数据中心风险的定级，问题的分类与上述的事件分类相似。

2.2.3．变更管理

变更管理的目的，是确保以受控的方式去评估、批准、实施和评审所有变更，确保标准方法和过程得到使用，阻止未授权的变更发生，使得变更风险可以降至最低，同时将变更相关突发事件的影响减到最小，并且确保所有变更都必须可跟踪和可追溯。

变更管理的要素包括变更的分类、变更管理的流程、变更管理的角色定义、变更的发起、变更的审批、变更的执行和关闭，变更的常规政策和预授权政策等。

2.2.3.1．变更管理解释

变更管理：在对基础设施进行日常运行、维护中所涉及具有一定风险性操作过程的管理描述。

变更管理的目标旨在通过规范化、标准化、流程化的管理方式，规避在变更实施中的风险项。变更管理范围涉及年度例行变更，事件类变更，数据中心系统架构的更改，设备状态、参数、配置等方面的变更。

2.2.3.2．变更的分类

平安数据中心基础设施运维，按照变更的影响程度，分为一级变更，二级变更，三级变更。

- 一级变更，又称为重大变更，主要指对数据中心配电、暖通系统有较大隐患的变更，影响机柜双路供电安全性、影响机房整体制冷类、监控和消防安全的变更。
- 二级变更，包括维护类变更，参数修改类变更，维护类变更主要包括单个设备层的故障维护，单个设备的配置变更，对 IT 负载无双路供电性安全影响的维护类事件；
- 三级变更，主要针对设备级正常状态下的参数修改，运行状态变更。

2.2.3.3．变更角色定义

变更管理将变更流程中涉及的变更委员会、日常运维经理/银行 IT 经理、基础设施经理、工程师、监控岗、技工岗角色及职责进行分别定义。

2.2.3.4．变更分级管理图

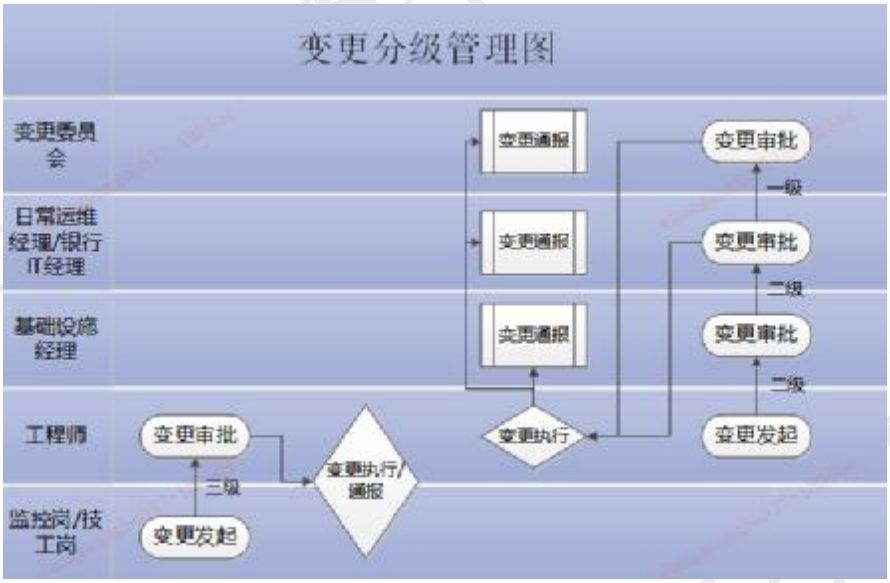

图 2.2-1 变更分级管理图

2.2.3.5．变更发起

变更管理制度详细说明了变更的发起人，变更的主要要素。包括变更单的类型，变更基本信息，变更原因，变更方案，变更等级评定。

2.2.3.6．变更审批

该步骤中，变更的审批者将评估和检查变更请求所产生的影响，确保能够在实施变更时，既能满足业务的要求，同时又对服务造成的影响最小。该步骤将决定是否进行变更。

2.2.3.7．变更实施

通过本步骤，将变更内容在生产环境中进行实施。根据变更单授权审批的实施时间、实施程序等内容，实施人组织筹备现场变更实施，并如实记录实施过程。

2.2.3.8．变更关闭

本步骤的目的是考察变更是否达到了预期的效果，对变更结果进行确认，且变更单的信息是正确、完整的。

2.3．Uptime M&O 实践

Uptime institute 公司的 M&O 认证是数据中心行业的国际权威认证，在全球范围内得到高度的认可，M&O 认证用来对数据中心综合指标进行评估，旨在帮助数据中心提高运营和管理水平。

M&O 的重要思想是收集全球数据中心的运维案例，提供最佳的实践，最低限度的降低人为或者设备带来的风险，提高数据中心的高可用性。

平安数据中心在 2017-2018 年以最短的时间通过了 M&O 的认证，并且得到国内数据中心认证的最高分 96.3 分。M&O 的认证包括对数据中心人员组织、维护管理、培

训管理、计划协调与管理、运行状况 5 个方面进行认证评分，综合得分 80 分以上即为通过认证，有效期为 2 年。下面就 5 个方面进行介绍说明。

2.3.1．人员组织

正确配置的合格人员人数对于数据中心实现长期性能目标非常关键。必须提供充足的合格内部人员和供应商支持，以便执行数据中心所有的维护活动和操作，以尽可能确保符合正常运行时间目标。数据中心的所有工作人员都必须拥有必需的经验和技术资格来执行被分派的活动，所有职位的角色和职责都应有所规定，且其重要程度经过管理层确认。

2.3.1.1．人员配置

平安数据中心承载着重要的核心业务，是 7*24 小时运行保障。为此数据中心配置了满足运维要求的人员。根据岗位的不同，制定了不同的岗位说明书，主要内容包括：从人员招聘开始，不同岗位的人员有教育程度、相关经验、专业能力、核心能力的要求，且明确各个岗位的职责范围、主要职责、工作难点、处理方法等内容，以及各个岗位在组织架构中的位置，确保每一位人员进入数据中心前必须满足各项要求，清楚自己的位置和职责。

岗位职责矩阵，将数据中心的运维工作分为 47 类，描述每类工作的大概内容，定义在每一项工作中，每一个岗位的具体参与方式，包括：执行、审核、支持、知晓四个方式。并根据人员的变动和职责的变化，更新岗位职责矩阵。这样的目的是使所有人员清楚在每一项工作中的角色，方便工作的有序进行。

数据中心区域复杂，设备众多，平安数据中心通过设立责任区的方式，将数据中心的物理空间分为 15 个区域，每一个区域责任到人，负责该区域的物理空间和设备，通过文件定义这些责任区具体的事项。另外责任区定期轮换，使得所有人对数据中心的基础设施有清晰深刻的认识。

2.3.1.2．人员资质

数据中心运维根据日常的作业内容，包括中压配电、低压配电、制冷系统、消防系统、电梯管理、登高作业等，平安数据中心运维人员具备国家安全生产管理总局颁发的中压操作证、低压操作证、暖通操作证，公安部消防局颁发的初级建（构）筑物消防员证，深圳市市场监督管理局颁发的电梯管理证（特种设备安全管理）。

人员资质的管理包括整理收集人员资质信息，定期进行检查，及时督促有关人员进行复证审证，保障证件在有效期内。

2.3.1.3．组织架构

平安数据中心运维团队有清晰的组织架构图，可以显示基础设施、IT 部门、安全管

理、供应商、保洁的工作界面及汇报链，以及各个组织的联系沟通渠道。

2.3.2．维护管理

2.3.2.1．预防性维护计划

预防性维护计划：平安数据中心运维团队每年底会根据设备的种类、设备供应商的建议制定下一年的预防性维护计划，多达 150 多项，这些计划经过管理层审批通过后，按照计划按时开始，并严格通过 MOP 指导文件进行过程管理，这个预防性计划的按时完成率定义在 95%，并且作为数据中心的重要 KPI 指标。

2.3.2.2．维护管理系统

- 有效的维护管理程序以追踪所有维护活动的状态和结果
- 包含所有重要设备的品牌、型号、出厂时间、安装时间、维保合同信息、操作注意事项等在内的信息列表
- 维护工单中包含特殊工具和配料以完成 PM
- 保存设备维护行为和趋势的数据和记录
- 关键备料和再订货点的清单

设备清单：覆盖所有关键设备的信息清单，包括设备信息，设备维保信息，设备关键主件信息。设备信息包括：设备类别、设备安装位置、设备名称、品牌、功格/型号、安装日期、序列号；设备维保商信息，包括维保单位、设备出保日期、维保联系人和联系电话；设备关键主件信息，因各个设备的类型不同，可根据设备类型，列举主要部件的信息。

工具管理：包括设备校准的规定，工具清单，工具的校准记录。

关键备件管理：由于每个数据中心设备类型不同，地理位置不同，供应商支持的程度不同，可以根据自己数据中心的情况，定义关键备件，梳理关键备件的清单，对备件进行定期清点。目标是实现在数据中心设备发生故障时，故障能够快速修复，缩短故障间隔时间（MTBF），减少对业务产生的风险。

2.3.2.3． 机房清洁政策：

数据中心清洁标准包括：

- 机房地板上下干净、整洁
- 机房内无易燃易爆、清洁用具、个人物品、包装纸盒等物品
- 机房环境干净、整洁，包括 IT 主机房，配电房、冷站等功能区域

2.3.2.4．供应商支持：

- 合格供应商清单（正常情况和紧急情况下），包括供应商名称、联系人、联系方式

- Ø 服务级别协议（SLA）的条款，包含工作内容、维护时间、频次、响应时间、培训需要等
- Ø 供应商接入流程以及合格的供应商服务人员

2.3.2.5．延期维护程序：

- Ø 追踪和监督执行延期维护的流程，包括延期维护的风险分析、延期维护的发起、审批、执行、关闭流程。

2.3.2.6．生命周期规划：

- Ø 主要设备或组件在生命周期置换过程中的计划、财务管理程序

2.3.2.7．故障分析政策：

- Ø 设备故障的清单（包括时间、设备，以及故障分析和所学到的教训）
- Ø 有效的流程以确定问题根源，并采取正确的纠正措施

2.3.3．培训管理

2.3.3.1．员工培训

对于每个在职新员工的培训，以确保技术能力和对工作制度的了解满足要求。通过文档化的宣讲和现场演练以达到：

1）所有运维管理中涉及的流程、程序和政策

2）SCP（Site Configuration Procedure）现场配置程序培训

3）SOP（Standard Operating Procedure）标准操作程序培训

4）EOP（Emergency Operating Procedure）应急处理程序培训

5）MOP（Maintenance Operating Procedure）维护操作程序培训

6）MMS（Maintenance Management System）维护管理制度培训

包含课程计划、课件、记录等在内的培训管理程序，正式确定人员合格的程序。

2.3.3.2．供应商培训

内容包括：

- Ø 需要供应商接受的培训清单
- Ø 供应商到现场工作前的必要流程和程序的介绍
- Ø 正式培训程序包含正式员工接受的培训中必要的方面
- Ø 包含课程计划、课件、记录等在内的培训管理程序

2.3.4．计划、协调与管理

2.3.4.1．机房政策

数据中心正式的文档程序包含以下：

1）数据中心员工管理设备的政策（如配置变更的原则，正常、紧急等不同运行状态下的运行方案）

2）SCP（Site Configuration Procedure）现场配置程序

3）SOP（Standard Operating Procedure）标准操作程序

4）EOP（Emergency Operating Procedure）应急处理程序

5）变更管理（评估变更风险及必要的审批）

2.3.4.2．财务政策

必要的财务程序以确保数据中心所需的资金保持充足且可用。

2.3.4.3．文档资料库

以下资料和记录必须具备（在数据中心现场或不在现场）：

1）竣工图

2）运行维护文档

3）研究成果

4）测试报告

5）维保合同及条款

6）书面的自动控制程序

以上资料必须在数据中心现场可以随时获取，必须在数据中心中集中存放并被所有人获取，有一套程序确保以上资料的版本更新，并被所有数据中心人员获取。

2.3.4.4．容量管理

机房 IT 设备安装及移除的程序，机房使用情况的定期回顾与更新，对于空间、电力和冷量增长需求的预测流程，定期跟踪现有空间、电力和冷量容量的使用情况，有效的气流组织管理流程和电力使用及分析的流程。

2.3.5．运行状况

2.3.5.1．负载管理

确保当切换动作时，负载不超过容量上限的程序。

2.3.5.2．操作设定值

基于风险、可用性以及成本等考虑而设置的关键运行设定点。

第三章 数据中心安全管理

数据中心安全管理主要包括三个方面：信息安全管理、物理安全管理和人员安全管理。而金融类数据中心在安全性上较其他类数据中心有更高的要求。平安数据中心参考《ISO27000:2005 信息安全管理体系》、《GB/T 21052-2007 信息安全技术 信息系统物理安全技术要求》以 ISO9001、M&O 体系为指导，力求做精做细，保证数据中心各个环节的安全稳定运行。

3.1．信息安全管理

随着在世界范围内，信息化水平的不断发展，数据中心的信息安全逐渐成为人们的焦点，世界范围内的各个机构组织都在探寻如何保障信息安全的问题。目前 ISO27000:2005 信息安全管理标准已得到大多数国家的认可，平安数据中心参考此标准对信息安全进行系统管理， 制定保密制度如下：

1) 遵守平安科技（深圳）有限公司计算机信息网络安全保密规定。
2) 未经批准,任何人员都不得将机房内的任何物品携带出机房,且不得将机密文件,软件版本,技术档案,内部资料等携带出机房或对外泄密。
3) 不得泄漏其他有关数据中心的秘密、机密、绝密信息,包括数据以及文件等。
4) 不得泄漏服务器资料如账号、密码等信息,严禁盗用其他人员的账号和 IP 地址。
5) 未经授权,任何人都不得进入数据中心非公开区域,不得接触和使用数据中心或与自身工作无关的 IT 设备,不得干扰和妨碍数据中心或其他人员的正常工作。
6) 未经授权,任何人不得变换数据中心内网络及计算机等 IT 设备的安装环境,不得擅自更改网络及服务器等 IT 设备的各项参数。
7) 严禁随意挪用,变换和破坏数据中心内的公共设施。
8) 首次进入数据中心的外来人员（如维护、参观等）需签署《保密承诺函》,并配合数据中心管理人员和保安人员进行必要的安全检查。如有违反安全保密制度的情况,将视其情节轻重,根据数据中心管理规定,对当事人进行必要的处理。如果该行为构成犯罪的,将申报至公司法律和安全部门追究相关法律责任。
9) 办公电脑专人专用，由计算机管理员统一标装操作系统，严禁个人擅自重装操作系统。
10) 严格执行办公系统账号和口令标准，不得随意泄露给他人，登录密码每三个

月更改一次，在工作岗位调动或离职时需按时交还办公电脑。

11) 因工作原因需外发邮件时，需抄送直属上级领导，经直属领导审批后方可放行。邮件内容及附件涉及账号、密码、IP 等敏感信息需采取必要的屏蔽措施。

3.2．物理安全管理

物理安全是指需保证数据中心的机房和所有设备及其他场地的安全。这是整个数据中心信息系统安全的前提。如果机房的物理安全得不到强有力的保证，存在各种不安全的因素，则整个数据中心的安全也就不可能实现。

平安数据中心不仅在建设阶段基于 GB50174《电子信息系统机房设计规范》A 级标准，为数据中心的物理安全打下了良好的基础，而且在日常运维工作中制定了不同级别的访问控制管理制度，对人员出入安全，物品出入管理，消防安全等均作出明确规定。

3.2.1．物理安全配置

平安数据中心的物理安全配置分为五级，分为园区级、大楼级、机房级、区域级、机柜级。

- 园区级：有园区保安负责进入园区人员和车辆的识别，园区内安保人员实时巡逻。
- 大楼级：数据中心大楼设置有大门门禁、安检机、人脸识别，大楼安保岗负责对出入人员的管理。
- 机房级：数据中心各个机房通过人脸识别、刷卡、指纹模式验证，方可进入机房区域。
- 区域级：IT 机房内部，将 IT 区域根据客户的不同进行分区，通过隔笼、冷通道的方式隔离，每个隔离区域都设置有门禁，只有专属用户才允许进入相关区域。
- 机柜级：IT 机房内，各个 IT 机柜前后门都进行上锁，专属用户拥有开锁的权限。

大楼及机房内装配监控摄像头，实施录像并进行双备份存储，支持 3 个月的查询，机房内各门禁记录支持 1 年有效期的查询。

3.2.2．术语及定义

- 直接进出人员

指具备数据中心进出权限（进出卡、指纹信息、虹膜信息）、需长期进出数据中心的内部工作人员，进出人员清单由数据中心基础设施管理人员在出现直接进出人员权

限变动时更新，并每月由基础架构部主管数据中心的领导进行确认。

- 间接进出人员

指不具备数据中心直接进出权限、因工作关系需要临时进出数据中心的平安科技内部及外部人员，在通过相关申请通道的审批同意后，由具备直接进出权限的相关人员带领进出数据中心。

- 数据中心 IT 设备区域

此区域是指数据中心放置 IT 设备的区域。如存储机柜、网络设备机柜、服务器设备机柜等。不包括数据中心其他区域，如基础设施设备房、消防气瓶间、UPS 电池房等。

3.2.3．程序

- 进出权限管理

区域权限划分：数据中心进出人员根据工作内容被赋予进出相关区域的相应权限，其他无关区域不得越权进出。

进出权限申请：凡需进出数据中心的直接进出人员，可按照数据中心进出权限申请流程提交申请。申请通过后数据中心基础设施管理人员根据申请人分配的权限对申请人员员工工牌添加相应进出权限。

- 数据中心进出权限变更

数据中心直接进出人员因工作区域发生变化、工作调动或离职等原因需要进行权限变更、注销，可按照数据中心进出权限变更流程提交申请。审批通过后由数据中心基础设施管理人员进行权限变更。

- 数据中心进出权限记录

数据中心进出权限（包括进出卡、指纹信息、虹膜信息）与其持有人具唯一的对应关系，直接进出人员的进出记录均保存在数据中心门禁系统内，每月由数据中心基础设施工程师检查门禁系统访问权限分配，及时删除不必要的访问权限并提取权限清单报中心经理审批确定。直接进出人员须牢记数据中心安全责任承诺，妥善保管进出卡，严禁转借他人使用；如进出卡不慎遗失，应第一时间办理挂失手续。

- 临时进出数据中心

间接进出人员因工作原因需要在某段时间内进出数据中心，可由对应平安科技内部员工按照数据中心临时进出权限申请流程提交申请。申请内容主要包括对此间接进出人员何时进出数据中心、对何对象进行何动作授权，及统筹工作安排（含风险评估及风险预案内容），审批通过后领取来访证，并由数据中心值班人员带领进入工作区域，并登记使用人员相关信息备案，使用结束后交还给数据中心值班人员。

- 数据中心参观

来访宾客如要进入数据中心参观，必须由平安科技内部员工作为申请人，提前两个工作日按照数据中心参观申请流程在对应的工作平台中提交申请，列明来访原因、到访时间、参观区域等信息，审批通过后由数据中心运维组人员安排现场参观。

3.2.4．人员进出登记制度

间接进出人员进出数据中心，必须在保安岗一一进行登记，参观类来访人员及物流搬运人员可以由一名代表进行登记。快寄服务人员可以凭工作证免登记手续进入办公区域，但需要机房内部的被访人员陪同。第一次进入数据中心的间接进出人员需签署保密协议。

保安值班岗应督促间接进出人员在“访客登记系统”上登记，包括姓名、单位/部门、进入时间、来访目的、进出区域、携带进出的物品及人数等相关信息。间接进出人员中的平安员工需提供工牌进行信息录入，外单位人员需提供有效证件（身份证或护照或社保卡或驾照）进行信息录入。并领取来访证及来访单。

间接进出人员离开数据中心，应归还来访证及来访单，被访人需在来访单上签名确认，并填写来访人离开时间。来访人员需主动在“访客登记系统”中登记离开时间，保安值班岗位应确保“访客登记系统”各项内容的真实和完整。

在“访客登记系统”出现技术性故障时，可使用《数据中心进出登记簿》临时登记进出人员信息，并按相关记录管理规范保存及归档。

保洁人员及相关管理人员可凭专用门禁卡出入被授权区域，未授权区域必须由数据中心值班人员全程陪同带领进出。

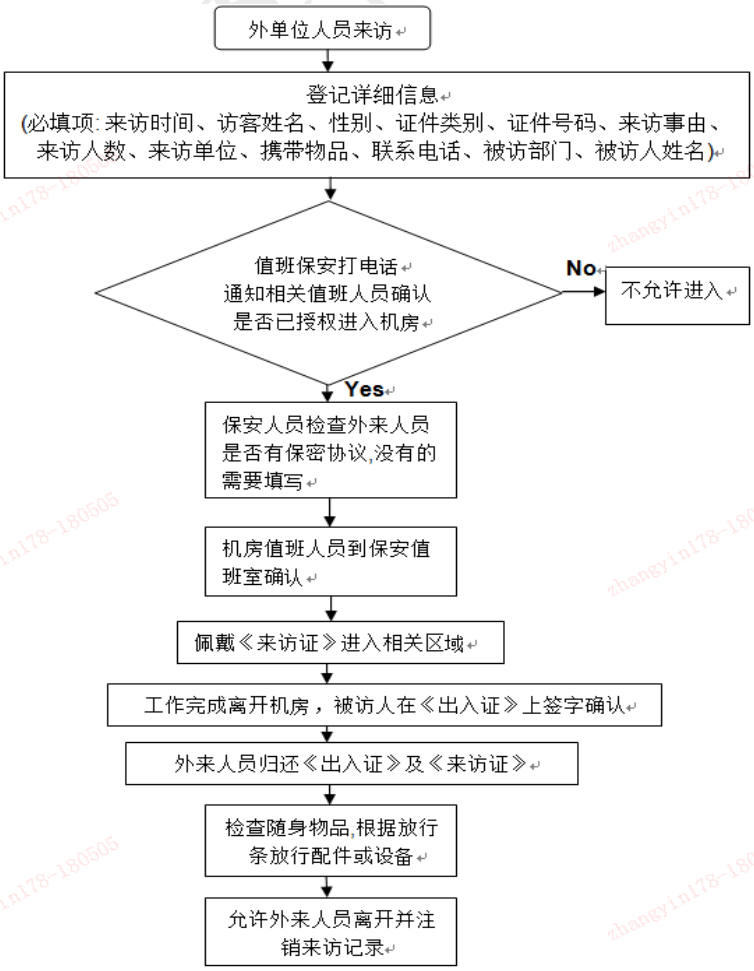

图 3.2-1 外来人员进出管理图

间接进出人员管理

1）当来访者要求对数据中心或者其他包含有敏感信息的工作区域进行访问时,应事先向数据中心管理部门提出申请,在获得进入许凭证后（许可凭证：管理部门审批通过的授权文件），由数据中心运营当班人员在规定的时间段内带领进出数据中心。但如需进入新机房外来人员（除运送货物至库房区域外来人员）必须先通过安检门检测，通过安检门人员及物品需服从值班保安管理。

2）来访人员到达数据中心后，需在指定区域做维护前准备工作或者休息，其他办公区域未经许可下禁止逗留。

3）涉及到机房变更的间接进出人员需在数据中心每日维护窗口时间（每日 23:00 至次日 06:00）之前做好准备工作，如 IT 设备出库，备件查找等工作。

4）进出数据中心人员须注意进门后门禁的闭合情况，严禁将机房门保持常开状态。数据中心值班人员应留意各机房门禁闭合状态，发现问题及时处理。

5）对于未经授权进入的区域，来访人员不得随意进入或尝试进入。一经发现,将向

客户有关方及数据中心的领导进行通报，如果情节严重，数据中心有权取消其访问权限。

6）未经批准,任何人员都不得使用摄像 IT 设备在数据中心内拍照、摄影（除机房工作人员因工作需要外），或将数据中心内的任何物品携带出数据中心,且不得将软件版本、技术档案、内部资料等秘密以上级别的文件等携带出数据中心或对外泄密。来访人员必须根据机房保密制度签署保密协议。

7）进入数据中心人员如需对设施、IT 设备进行硬件维护、装卸、或需移动光纤、网线、电源插座、电缆线等，均须先告知数据中心运维当班人员，并在其指导下进行。

8）数据中心的一切线缆和地板不允许随便触动。需要拉接电源线、网络线等强弱电线路，须通知数据中心规划管理人员，由其统一规划和分配插座、端口，并由数据中心运维人员安排实施；严禁私自揭开地板，乱拉电源线和网络线。

9）所有外来人员进入数据中心 IT 设备区域，一律不得携带背包。

10）涉及到设施、IT 设备维护的人员维护结束后，在离开数据中心前，若有登陆相关服务器的须退至安全口令上一级，并等待 IT 设备相关管理组人员确认无误后，再在保安值班岗处办理离开手续后方可离开数据中心。

3.2.5．物品进出管理

保安值班岗位负责对数据中心的物品进出情况进行监督，确保符合物品进出相关管理要求。

数据中心内不得带入食品和饮料及与工作无关的物品（包括个人手提袋）。

严禁携带易爆、易燃、易破碎、易污染等危险品和可能干扰计算机 IT 设备的强磁场物品进入数据中心。

所有需带入数据中心 IT 设备区域内的物品，都需放入由保安人员提供的篮子内带入，进出前后由保安值班人员清点；个人物品统一存放至储物柜。

严禁携带未经授权的个人笔记本与数码相机进入数据中心，如需使用请填写《数据中心工具借用登记表》向数据中心运维当班人员借用。

非个人物品带出数据中心，须凭物品放行条，涉及到数据安全隐患的磁性介质类 IT 设备还需要经过运维值班人员消磁处理，由保安值班人员核验无误后方可放行。

3.2.6．消防安全管理制度

3.2.6.1．消防安全教育、培训制度

1、定期组织员工学习消防法规和各项规章制度。

2、每年以消防系统笔试考核和实操演练等多种形式，提高全体员工的消防安全意识和消防技能。

3.2.6.2．防火巡查、检查制度

1、落实逐级消防安全责任制和岗位消防安全责任制，落实巡查检查制度。

2、消防维保厂家每月对数据中心消防设施进行一次防火检查并复查追踪改善。

3、检查中发现火灾隐患，检查人员应填写防火检查记录，并按照规定，要求有关人员在记录上签名。

3.2.6.3．安全疏散设施管理制度

1、数据中心应保持疏散通道、安全出口畅通，严禁占用疏散通道，严禁在安全出口或疏散通道上安装栅栏等影响疏散的障碍物。

2、应按规范设置符合国家规定的消防安全疏散指示标志和应急照明设施。

3、应保持防火门、消防安全疏散指示标志、应急照明、机械排烟送风、火灾事故广播等设施处于正常状态，并定期组织检查、测试、维护和保养。

3.2.6.4．用火安全管理制度

（1）严格执行动火审批制度，确需动火作业时，作业单位应按规定提前申请“动火许可证”，审批完成后方可实施。

（2）动火作业前应清除动火点附近 5 米区域范围内的易燃易爆危险物品或作适当的安全隔离，并向保卫部借取适当种类、数量的灭火器材随时备用，结束作业后应即时归还，若有动用应如实报告。

（3）如在生产区域就地动火施工，应按规定经理级(含)以上主管人员审批通过，运维人员需现场全程跟随监督。离地面 2 米以上的高架动火作业必须保证有一人在下方专职负责随时扑灭可能引燃其它物品的火花。

3.3．人员安全管理

在保证数据中心正常运行过程中，运维人员的人身安全必须摆放在重要位置。平安数据中心高度重视运维人员的人身安全，把安全贯穿到数据中心生产的每一个环节当中。

3.3.1．人员安全培训

员工安全培训覆盖新入职员工和已经上岗的运维人员。

新入职员工试用期内需按照《数据中心人员培训作业指导书》进行岗前安全培训，培训完成后需进行安全考核，考核成绩 80 分为合格。通过考核后方可上岗工作。

安全培训负责人每年 12 月份制定下一年度安全培训计划提交领导审批通过后实施，培训内容应在往年安全培训内容的基础上，结合本年度运维工作实际事例和外部安全事故，进行优化、梳理，保证运维人员在日常运维工作中的人身安全。运维人员需按照

《数据中心人员培训作业指导书》每年定期进行安全培训，培训完成后需进行安全考试，80 分以上为合格。考试成绩纳入年度考核指标。培训内容包括：

1、电气安全规范
2、暖通安全规范
3、场地工具使用规范
4、机房出入规范
5、往年安全事件回顾

3.3.2．日常运维安全管理

运维人员在日常运维工作中，需严格遵从数据中心电气安全规范、暖通安全规范和场地工具使用规范等。

3.3.2.1．电气安全规范：

1. 运维人员操作电气设备应身体健康,经医生鉴定无妨碍工作的疾病 ;具备必要的电气知识,执证上岗; 必须会触电急救法和电气防火和救火方法。
2. 运维人员操作电气设备时不得少于 2 人，一人操作，一人监督。值班时如遇特殊情况仅有 1 人，此人必须具有独立工作和处理事故的能力,并只能监护设备运行,不得单独操作电气设备。
3. 运维人员必须穿绝缘鞋;接触设备外壳和构架时,应戴绝缘手套。
4. 在一经合闸即可送电到工作地点的开关和刀闸的操作把手上，均应悬挂"禁止合闸有人工作!"的标示牌。
5. 供电设备无论仪表有无电压指示,凡未经验电、放电,都应视为有电。
6. 经重大变更审批同意停电时,应按范围停电,不得随意扩大停电范围。
7. 运维人员需按时巡检，严肃认真,正确无误地记录运行日志,按时按质抄报所规定的表单和报表。
8. 运维人员不得在醉酒状态下值班，不得在值班时间做与工作无关的事,不得擅自离开工作岗位。

3.3.2.2．暖通安全规范：

1、 运维人员应身体健康,经医生鉴定无妨碍工作的疾病；具备必要的暖通知识,执证上岗。
2、 运维人员操作暖通设备时不得少于 2 人，一人操作，一人监督。
3、 冷水机组运行切换为每月月度例行维护时进行，不得随意切换。如冷机故障需切换至备用机组运行时，需上报值班工程师同意后，方可实行。
4、 运维人员需按时巡检，严肃认真,正确无误地记录运行日志,按时按质抄报所

规定的表单和报表。

5、 运维人员禁止赤脚赤膊，禁止穿着短袖、短裤及拖鞋进入数据中心；严禁在酒后、疲劳和重病状态下进入数据中心。严禁在数据中心内追逐打闹。

3.3.2.3．工具安全使用规范：

1、 运维人员使用工具时需遵循《数据中心工具管理规定》，认真填写工具借用登记表，谨慎使用，及时归还。

2、 运维人员进行现场焊割作业时，必须符合防火要求，遵守“电焊作业规范”，佩戴护目镜等必要的劳动保护用具。

3、 运维人员进行高空作业离地 2 米以上时，必须佩戴安全带。安全带需定期检查，每次使用前应检查安全带结实可靠，不得擅自接长使用。遵循高挂低用，严禁低挂高用的原则。

4、 带电作业时必须穿绝缘鞋，佩戴绝缘手套。试电笔、万用表等设备必须按时进行电气性能检验。

5、 使用打磨机、切割机和电动螺丝刀等电动手持工具时需佩戴防护眼镜，工具需带有漏电保护装置。如有损坏必须由专人修理，并检查合格后方可再次投入使用。

6、 使用梯子进行低空作业前，需检查梯子的牢靠度，防止跌落受伤。

第四章 人员保障与发展

4.1．组织架构

数据中心在企业 IT 信息基础设施中居于基础和核心地位，数据中心建立合理的组织架构形式和清晰明确的职能定位，对于企业达成业务目标，实现高效能、高效率、高安全的数据中心运维，具有巨大的牵引和指导作用。

合理的组织架构设计，能够引导数据中心合理的流程流转、紧密的部门合作、清晰的职能界定、规范的责任权利设定，同时也有利于充分调动人的主观能动性，让组织架构的效率充分体现出来，实现人事相宜，上下同心，从而众志成城。

在 Uptime <Tier Standard:Operational Sustainability>标准中也明确提出人员的配置情况，不同级别的数据中心要求匹配的人员数量不一，等级越高对人员数量和技能水平要求越高。如表 4.1-1 所示，Uptime 将数据中心分为四级，其中 Tier I 级别最低，Tier Ⅳ级别最高，级别越高匹配的人员能力要求越高，同时值守时间也最长，Tier Ⅳ往往要求全年数据中心无业务中断，对运维的要求非常高，必须安排专业技术的人员现场 24 小时值守，以便在出现问题时，及时排除，或者能立即切换到备份系统上，让业务不受影响。

数据中心运维等级要求 **表 4.1-1**

组成部分	行为	I	II	III	IV
人员配置	1. 分配用以监督关键设施运行的全职或兼职个人	✓			
	2. 支持业务存在目标的员工和/或供应商		✓		
	3. 全天候员工在场: 至少有 1 名合格的 FTE			✓	
	4. 全天候员工在场: 每次轮班有 2 名合格的设施支持 FTE				✓
	5. FTE、		✓	✓	✓
	6. 指定了适用于指派员工和指定供应商，为特定的关键系统和设备提供支持的相应通告升级和呼叫程序		✓	✓	✓
	7. 基于操作和维护要求的 根据轮班分割的工程专业（如电气、机械、控制、建筑管理系统 [BMS] 等）覆盖			✓	✓
资格认证	1. 政府规程要求的相应员工职业许可证	✓	✓	✓	✓
	2. 正确维护和操作已安装基础设施所需的经验和技术培训			✓	✓
	3. 具备个人或作为轮班小组执行具体轮班操作资格的轮班人员			✓	✓

平安数据中心作为整个集团的核心基础设施，承载整个集团重要核心生产业务及灾备，运维要求按照 Tier Ⅳ级别配置，数据中心施行 7*24 小时 5 班 3 运转方式，每班配置一名资深值班工程师（值班负责人），具备对于现场紧急情况进行快速处置的能力，监控岗 1 名，技工岗 3 名(覆盖电气、空调和弱电专业)，观澜数据中心基础设施组监控岗承担平安数据中心集中监控工作职责。在组建数据中心运维团队时，必须考虑运维覆盖的广度和深度。在重要的岗位，配备 A、B 角人员。

在人员的组织架构设计上，平安数据中心分为三大块，每个部分再细分，建设完善的运维系统，如下表：

数据中心运维组织结构 **表 4.1-2**

数据中心运维组	日常运维管理（IT 管理）	网络运维
		服务器运维
		应用软件运维
		存储运维
		云平台运维
	基础设施管理	电气运维
		空调运维
		消防运维
		监控运维
	物业安保&保洁	保安部
		保洁部
		后勤管理部

4.2．区域和人员职责精细化分配

随着互联网、信息化产业的不断发展，作为各种信息载体的数据中心发挥着越来越重要的作用。因此保证数据中心的安全运行变得尤为关键，数据中心运维管理工作也变得越来越复杂，技术难度不断被加大。数据中心运维工作者精细化分配及相对应的工作职责尤为重要，数据中心主要岗位包括数据中心经理、基础设施运维小组负责人、基础设施工程师岗、基础设施监控岗和基础设施技工岗。

- 数据中心经理

数据中心的总负责人。

1、负责数据中心的整体规划（容量、能效、可用性和业务持续性），确保满足业务的需求。
2、负责将业务需求转换为数据中心需求。
3、负责数据中心所有的日常运营管理。
4、负责数据中心的运维体系规划、实施和持续改进。
5、负责数据中心运行计划的制定和实施。
6、负责数据中心运行成本的有效管控。
7、负责推动数据中心服务能力的提升。
8、负责数据中心团队的管理。
9、负责重大事件的上报和跟踪处理等。

- 基础设施运维小组负责人

数据中心基础设施运行的负责人，向数据中心经理负责。

1、 负责数据中心基础设施的规划，确保满足业务的需求。
2、 负责数据中心基础设施服务，保障计划的制定和实施改进。
3、 负责设施、设备的运行、维修和保养工作，进行定期和不定期的巡查，确保操作规程及设备检修保养制度的落地。
4、 负责数据中心服务外包商评审及场地验收。
5、 负责设施类重大、较大变更评审，及时采取措施推动数据中心设备保障能力的提升。
6、 配合项目部门制定与部署运维保障方案。
7、 负责基础设施重大事件的上报和跟踪处理。
8、 负责数据中心节能优化，设备综合效能等。

Ø 基础设施工程师岗

数据中心基础设施运行工程师岗，向基础设施运维小组负责人负责。

1、 负责本班次基础设施运行安全。每班次至少对机房进行全面巡查一次，保证设备设施的正常运行。
2、 人员管理：
   a) 对监控岗、技工岗的协调管理：检查本班监控岗、技工岗的工作纪律、工作质量、履行岗位职责的情况，督导其工作，并协调处理有关事务;
   b) 审核当班技工岗交接班报告、巡检记录，并签字确认。
   c) 对服务商的管理：管理服务商的工作，审核当班时段的服务商报告，并签字确认。
3、 故障处理：实时关注监控系统状态、邮件和手机故障报警，发现报警或接到故障通知后，对故障原因迅速定位并组织相关人员及时处理。二级以上故障应立即报告小组负责人及管理者代表，并实时报告故障处理进展情况。
4、 根据实际相关计划或工作需求，负责制定变更的序列并按流程进行变更申请，按计划组织实施变更。
5、 掌握重点负责设备的运行状况、技术数据和技术档案，保障设备处于良好的工作状态。对各种设备隐患和改进需求，按流程制定变更方案，提交变更申请。
6、 按期完成重点负责的文档工作。按照相关规范和时间要求持续更新。
7、 积极主动的承担或参与临时安排的工作。如培训与演练的组织协调、变更跟进、运维方案文件制定等。
8、 组织相关人员，协助进行项目施工、现场管理、竣工验收等工作。
9、 工作交接。按照交接班管理规定进行工作交接。
10、 完成上级交办的其他工作。

Ø 基础设施监控岗

数据中心基础设施监控岗，向基础设施运维工程师负责。

1、 负责 7*24 小时通过机房监控系统对机房基础设施的运行情况进行监控。
2、 每小时在监控系统中巡检机房运行状态，包括机房冷冻水、精密空调、高低压供配电、UPS、STS、精密配电柜、空调配电柜、监控录像等。
3、 出现基础设施故障时，能初步分析故障原因，通知基础设施工程师协调强电技工和空调技工处理故障，或协助召开电话会议进行故障处理，详细记录故障处理进度，发布故障通知。
4、 故障应急状态下，及时通过邮件、对讲机通报监控系统中的故障情况。
5、 统计每班次基础设施六级（含六级）以上告警数量和处理措施。
6、 每个晚班负责进行统一的监控摄像检查，检查出来的问题通报基础设施运维组，上报事件单并跟进。
7、 积极参加公司组织的演练、培训及小组会议等集体活动，通过相关活动提高自己的业务水平和职业素养。
8、 完成上级交办的其他工作。

- 基础设施技工岗

数据中心基础设施技工岗，向基础设施运维工程师负责。

1、 负责对机房基础设施（包括供配电系统、空调系统、消防系统、环境卫生等）管理。每班次按相关规范和频次进行巡检，发现设备隐患立刻上报基础设施工程师。
2、 负责机房楼梯、楼道、墙体、墙面、楼板、天花、屋面等土建装饰修补工作。定期检查机房墙壁、屋顶、有无漏水、渗水、脱落等现象。定期检查机房照明灯具、应急照明设施，确保使用良好。
3、 按照基础设施工程师的指导与要求，合理调整中央空调主机（新机房）和机房内精密空调设备运行，提高空调运行效率，节约能耗。
4、 按照基础设施工程师的指导与要求，及时处理机房供配电、消防设备故障、空调、给排水设备故障，保证机房供配电、消防设备、供冷、供水运行正常。
5、 协助配合维护商对机房供配电、消防设备、空调、给排水设备的维护，跟进后续问题处理。
6、 负责所辖设备环境卫生，管理好值班器材、钥匙、工具。
7、 负责机房各类装潢、办公家具、门窗、门锁、地板、地毯的维修、更换工作，各类粉刷及油漆工作，机房照明、指示灯等维修工作。
8、 负责机房钢架制作，地板支撑，地板切割等工作。负责机房地板的整改、修理工作，监督施工人员对地板的操作，不得拆除地板支撑架，对地板下扎带、线头等杂物要清理干净，并于施工后恢复原状。

9、 熟悉机房的孔洞位置，监督并督促施工人员在施工后，做好孔洞安全封堵工作。

10、 协助新项目施工现场管理、竣工验收。

11、 协助进行人员进出机房管理。未经同意，严禁外来人员进入机房，基础设施变更管理人员不到现场，施工人员及处理故障人员不得进入机房。

12、 值班人员需监督施工人员，保证施工现场的材料整齐有序。并做好进入人员的登记，确保人员进出对设备硬件安全不造成影响。

13、 负责机房内资料、工具、备件等物品的保管工作。每次交接班进行清点，对清点结果和借还情况，在值班日志中体现。

14、 积极参加公司组织的演练、培训及小组会议等集体活动，通过相关活动提高自己的业务水平和职业素养。

15、 按照交接班要求填写交接班日志。对所发生情况详细记录，保证记录的准确、完整性。

16、 完成上级交办的其他工作。

4.3．人员培训

为确保数据中心运维人员满足岗位需求，确保数据中心各项工作安全、有序的开展，规避因运维人员人为因素而导致的运行风险，对于场地基础设施运维团队及新员工应进行完整及严格的培训，以确保其具备岗位需要之知识及能力，实施规范化的管理。培训主要包含五个方面：通用培训、采购培训、专业培训、制度流程培训和从业资格证培训。

4.3.1．新员工培训

新员工培训计划自入职开始实施，培训周期为 2 个月，培训内容涵盖作业安全、规章制度、工作流程、设备操作、设备维护、设备应急等相关基本运维工作内容，各岗位新员工应明确岗位培训课程，有指定培训导师负责完成新员工培训实施，全部课程考核达标后方可上岗，以满足基本岗位要求。计划时间表如下：

新员工培训实施计划表 **表 4.3-1**

序号	课程类别	课程名称	培训内容	讲师	培训方式	合格标准	第1月				第2月				备注
							1	2	3	4	1	2	3	4	
1	基本制度培训	基本制度及管理政策培训	1、人员组织架构培训 2、流程管理培训 3、维护管理培训 4、值班巡检管理培训	***	课件	80									
2	安全培训	基础设施安全培训	1、电气安全规范 2、暖通安全规范 3、场地工具使用规范 4、机房出入规范 5、往年安全事件回顾	***	课件	80									
3	技术培训	供配电系统培训	新老机房供配电/UPS系统架构、操作、维护及应急处理培训	***	课件&实操	80									
4		空调系统培训	新老机房空调系统架构、操作、维护及应急处理	***	课件&实操	80									
5		消防及电梯培训	新老机房消防和电梯系统架构、维护及应急处理	***	课件&实操	80									
6		监控系统培训	新老机房监控系统架构、维护及应急处理	***	课件&实操	80									

针对每门课程的重要性都应划定独立的考核标准，所有要求的受训对象必须考核达标方可上岗。

4.3.2．培训大纲

4.3.2.1．工程师岗培训大纲

工程师岗是数据中心的技术管理核心骨干岗位，承担了数据中心管理类及技术类的各项日常工作，基于其岗位工作内容及目标要求，其岗位培训应涵盖如下内容：

- 数据中心所有管理政策及流程制度培训；
- 数据中心系统配置架构及运行方案培训；
- 数据中心供配电系统设备的操作、维护、应急培训；
- 数据中心暖通系统设备的操作、维护、应急培训；
- 数据中心消防弱电系统设备的操作、维护、应急培训。

4.3.2.2．技工岗培训大纲

技工岗是数据中心现场保障核心岗位，承担了数据中心 7*24 小时巡检职守、场地应急实施、场地管控等工作。基于其岗位工作内容及目标要求，其岗位培训应涵盖如下内容：

- 数据中心所有管理政策及流程制度培训；
- 数据中心系统配置架构及运行方案培训；
- 数据中心供配电系统设备的操作、维护、应急培训；
- 数据中心暖通系统设备的操作、维护、应急培训；
- 数据中心消防弱电系统设备的操作、维护、应急培训。

4.3.2.3．监控岗培训大纲

监控岗是数据中心 7*24 小时告警服务中心，承担了多机房的集中后台告警开单、通报职责。基于其岗位工作内容及目标要求，其岗位培训应涵盖如下内容：

- 数据中心动环监控系统的操作使用培训；

- 数据中心安防系统的操作使用培训；
- 数据中心系统配置架构及运行方案培训；
- 数据中心 Service Bot 系统的操作使用培训；
- 数据中心事件管理程序培训。

4.3.3．培训实施程序

4.3.3.1．培训签到

所有培训应有培训签到记录，培训签到记录中应明确培训目标人员和实际参加培训人员，所有计划内参加培训人员必须完成相关培训，否则为不合格人员，培训不合格人员不得在岗工作。

签到记录由培训负责人监督实施，培训完成后会同其它培训过程记录交由专人进行存档。

4.3.3.2．培训考核

完成培训后，培训负责人应组织参加培训人员进行考核。所有参加培训人员均需要参加培训考核，参加培训人员必须考核合格后方可上岗，若考核不合格可进行 1 次补考，若补考不合格的人员认定为不合格人员，对于不合格人员应予以调整岗位或其它方式进行处理。

考核方式应不局限于固有模式，可以采用笔试、问答或实际操作等多种方式进行，但所有考核形式必须有记录留存，考核结果和其它培训过程文件一并交由专人负责保存。

4.3.3.3．培训总结

培训课程实施完成后，培训负责人应对培训课程的实施情况进行评估，回顾内容应包含培训计划合理性、课件完善度、培训效果以及人员考核情况等。

各课程负责人应根据培训评估情况对培训课程进行优化调整，并落实到下一阶段的培训实施工作中。

新员工应制定培训管理档案，有培训导师负责对培训档案的实时更新与记录，新员工全部考核结束后，其培训档案记录作为岗位任职合格凭证记录，交由资料管理员统一管理。

4.4．人员发展

数据中心单体规模越大、系统越复杂，对于数据中心运行维护管理水平的要求也就越高。通过系统、全面、内容丰富的培训，帮助数据中心管理者更加有效规划我们的运维服务，降低成本，通过运维流程的提升改善及对业务流程的支撑，提高企业整体业务

运营质量。

4.4.1．员工例行培训

员工例行培训计划以年为时间周期进行制定，工程师于每年 12 月份制定下一年度培训计划提交领导审批通过后实施，培训内容应结合运维工作实际情况进行优化、梳理，对管理政策的优化调整项进行宣贯，保证运维管理政策的有效落地实施。此外，除管理政策相关内容外，还应加强员工的职业素养培训，加入提升类培训课程。

培训及演练课程

（1） 机房管理政策培训
（2） 基础设施年度安全培训
（3） 高、低压配电系统培训
（4） 空调系统培训
（5） 消防系统技术培训
（6） UPS 系统培训
（7） 机房给排水系统培训
（8） BA 系统培训

4.4.2．员工专项培训

员工专项培训为不定期、非计划性发起的培训课程，主要针对特定事项、流程、技术等内容而开展的培训，培训包括内部培训和厂商培训，讲师可以是供应商、设备厂商等外部人员，以满足数据中心运维工作持续发展、变化的需要。

借助行业第三方专业培训及职业技能鉴定平台，参加满足国家资质从业资格培训，积极开展运维人员任职资格的评定工作。

4.5．供应商保障

供应商作为数据中心运行维护的重要参与者，服务人员应熟知数据中心场地工作管理政策及技术要求。因此，提供服务支持的供应商人员应通过必备的课程培训及考核，考核达标人员列入服务白名单，准许进入机房提供服务交付。供应商培训周期至少每年进行一次，培训内容应涵盖数据中心相关管理制度、工作流程及关联技术内容，考核不合格供应商严禁进入数据中心现场提供服务。

4.5.1．供应商培训及要求

通过培训使供应商服务人员，了解数据中心相关管理制度，掌握相关流程手续的办

理方法，明确服务要求，使供应商可以安全、有效的为数据中心安全运行提供保障服务。通过该课程的培训，需要掌握数据中心供应商人员要求、场地工作注意事项、人员及物品出入管理制度以及供应商服务要求，考核成绩需 80 分以上通过。

4.5.2．服务 SLA

4.5.2.1．供配电系统及不间断电源系统

响应时间及承诺：

供应商在确认收到甲方说明故障现象的通知（信件、电报、电传或电话）后，应在 0.5 小时之内给予响应，及时修复排除故障，保证系统正常运行：

一级故障：配电设备故障，导致多于一台机房内设备（服务器、存储、小型机、交换机）故障，如 PMM 柜整个机柜跳闸、输出开关跳闸、STS 输出故障、空调配电柜故障等；1 小时内到现场，2 小时内解决问题；

二级故障：配电设备故障，导致单一机房设备故障，如 PMM 柜单一回路故障、单一空调开关故障等；2 小时内到现场，4 小时内解决问题；

三级故障：配电设备故障，没有导致机房设备故障，不影响可用性，如 PMM 柜显示异常，PMM 柜或电量仪通讯异常等；6 小时内到现场，12 小时内解决问题。

4.5.2.2．空调系统

响应时间及承诺：

乙方确认收到甲方说明故障现象的通知（信件、电报、电传或电话）后，应在 0.5 小时之内给予响应，及时修复排除故障，保证系统正常运行。

一级故障：机房室内精密空调设备故障或者精密空调冷水管道破裂，导致多于一台机房内的精密空调设备故障或者停止供冷，如精密空调电源故障、精密空调皮带断裂、风机故障、空调开关跳闸、冷水管道破裂、风冷空调压缩机故障、风冷空调制冷剂泄漏等；1 小时内到现场，2 小时内解决问题。

二级故障：机房室内精密空调设备故障或者精密空调冷水管道破裂，导致单一机房精密空调设备故障或者停止供冷，如一台精密空调皮带断裂、风机故障、单一风冷空调压缩机故障、风冷空调制冷剂泄漏等；2 小时内到现场，4 小时内解决问题。

三级故障：机房室内精密空调部分功能异常，没有导致机房设备故障或停止供冷，不影响可用性，如精密空调显示异常，加湿异常等；6 小时内到现场，12 小时内解决问题。

4.5.3．资质要求

供应商提供的现场服务人员，必须取得相关行业国家职能部门颁发的资格证书，不

得派遣无证人员至现场提供服务。

Ø 供应商通讯程序要求：

数据中心管理人员与供应商的呼入、呼出程序应指定固定接口人，并相互配置冗余人员。

供应商接口人应保持通讯畅通，在数据中心发生应急事件需提供支持时，可快速提供远程电话支持，如有需要可按照 SLA 要求时间内到达现场。

供应商应至少保持有 1 位经过考核合格的人员，可随时为数据中心提供现场应急支持服务。

Ø 工作管理程序：

平安科技数据中心基础设施的相关维护和变更操作采用工单形式发起申请，供应商若需对相关设备进行维护和变更操作需由数据中心管理人员代为发起申请，审批通过后方可实施。

供应商如果有延期维护的需求，需提前 3 天向数据中心管理人员进行书面申请，得到数据中心管理人员同意后，可以延期进行，但是延期不得超过 10 天。

4.5.4．考核机制

基础设施维保商在每半年需向我司提供半年内的维护服务总结报告，报告要求格式规范、内容真实。合同终止最后一个工作日前对全年维护服务进行总结并提交该年度维护服务报告。我们将基于本合同中的服务内容对维护商的服务质量进行考核，并依据考核结果执行付款。考核表格如下：

数据中心服务商 KPI 考核表 **表 4.5-1**

数据中心服务商KPI考核表（2018版）

服务商：					考核时间：	
设备系统：					考核区域：	
类别	权重	指标	评分依据	计算方法	得分	考核得分说明
可靠性（10分）	10	故障情况	设备频繁故障或由于设备故障所对数据中心内部IT系统造成重大故障	发生一次重大故障扣5分，其他视影响扣1-5分，扣完为止		
日常维护（30分）	20	维护情况	按照合同要求，根据维护安排，按时，按质、按量完成设备维护，提高设备可靠性	维护服务不及时、不完整或不规范，每次扣1-5分，扣完为止		
	10	服务报告	及时提供完整有效的服务报告，定期提供服务总结报告。	每发生一次扣1-2分，扣完为止		
响应性（30分）	30	故障及异常的响应处理和重要节点现场技术支持	设备发生故障时，需要按照合同规定的时间到达现场，及时有效的限速处理，并完成故障分析处理报告。 设备运行异常或由甲方对设备运行质量状态存在疑问时，需安排及时有效的限速处理。 当出现一些关联性问题，需要由供应商协助配合定位的，需积极配合关联系统问题的定位及解决。 根据合同要求，当甲方进行重大节点，需要时，供应商需进行现场支持。	超过合同规定标准时间、或者限速处理不及时有效，根据故障及设备异常的严重程度和影响范围，每次扣3-10分，扣完为止； 不按要求进行现场支持，一次扣3-10分，扣完为止。		
现场规范及其他（10分）	5	现场规范	遵守机房出入登记制度，机房注意事项，设备维护规范，现场工作规范、服从现场管理。	每发生一次不合格扣1-2分，扣完为止		
	5	其他条款执行	按时按要求提交审计资料，合同中约定的培训、测试等相关条款的实际履行情况，按时按要求参加服务商会议。	每迟到一次扣1分，缺席一次扣2分，扣完为止		
独立扣分项	/	隐瞒产品缺陷	隐瞒（包括不主动说明）产品的重要缺陷，造成平安系统可用性受到重大影响	每出现一次，根据严重程度扣分，每次扣分上限20分，一次考核周期中可以重复扣分，扣分用负值表示。		
	/	投诉	甲方对服务商进行正式投诉			
	/	人为造成重大故障	服务商由于人员原因造成重大故障			
独立加分项	/	发现潜在问题并支持解决	通过巡检发现潜在较大问题，并提出解决方案，并协助平安完成	每出现一次符合项，根据贡献程度加分，每次加分上限20分，一次考核周期中可以重复加分。		
	/	主动说明产品的重要缺陷	主动说明产品的重要缺陷，并积极协调安排修补计划和完成检查			
总分（最终考核评分）						
甲方科技负责人签字						

备注：
1、本补充协议作为维护合同的附件，如有条款和原合同冲突的，以本协议为准；
2、考核说明：按分数分A/B/C/D/E共5级，优秀（A≥90）；良好（90>B≥80）；合格（80>C≥70）；待改进（70>D≥60）；不合格（E< 60）
3、统一按照70分为考核合格分，如考核得分≥70分，按照100%付款；如考核得分<70分，付款金额=维护费用×（0.6+0.5%×考核得分%）；半年度或年度考核得分<60分，甲方有权解除维护合同，且无需向乙方支付违约金；
4、参考服务商的日常服务情况，每半年按照本考核表进行审核，作为相应时间段合同款支付、及合同续签的依据。

第五章　可靠性运维分析实践

5.1．日常巡检概述

平安数据中心可用度要求极高，为确保数据中心 IT 设备稳定、可靠地运行，必须安排值班人员对数据中心基础设施进行 7*24 小时日常巡视、检查。千里之堤，溃于蚁穴，任何的基础设施故障在出现之前都可能有所表现，小的隐患不消除，可能导致重大故障出现，数据中心日常巡检非常重要，可以及时发现一些运行中的隐患，并及时排除。

机房日常巡检主要分为两类，一类是基础设施技工岗、工程师岗到现场对基础设施进行定期巡检，另一类是基础设施监控岗通过机房监控系统对机房供配电系统、暖通系统、消防系统、安防系统、机房环境等进行实时监控。两类日常巡检相互补充，最大限度降低机房基础设施重大故障发生率，确保数据中心 IT 设备的高可用性。

5.1.1．日常巡检基本要求

- 嗅：放电嗅味及绝缘过热之焦味；
- 听： 火花放电声，机械振动声，电压过高或电流过大所引起的异常声音，水泵、风机有无异常机械振动声；
- 摸：设备非带电部分的温度和振动情况；
- 看：放电火花、变色、变形、变位、损坏、渗油、渗水、继电器、电度表转动、仪表和信号灯指示、系统管道及阀门有无跑、冒、滴、漏现象及其它情况。

5.1.2．巡检频率及巡检方式

- 中低压开关柜、UPS、精密配电系统、柴发系统、暖通空调系统、消防系统每四个小时一次；通过人工现场巡检、移动巡检 PAD 记录，发现异常及时通知基础设施工程师处理，并上报 ServiceBot 工作平台，以便跟进处理。
- 安防系统：每 8 小时巡检指定的摄像机录像存储状态，每 24 小时巡检所有的摄像机实时视频状态；通过机房监控系统或视频联网监控系统巡检摄像机实时视频状态，通过视频联网监控系统巡检录像存储状态。发现异常及时通知工程师安排处理，并上报 ServiceBot 工作平台，以便跟进处理。
- 弱电监控系统：每 2 小时一次；通过机房监控系统客户端（以下简称“监控客户端”）巡检机房运行状态，包括环境系统、配电系统、安防系统等。发现异常及时通知工程师安排处理，上报 ServiceBot 工作平台，以便跟进处理。

5.1.3．中、低压开关柜日常巡检

1、 看：中低压开关柜面板指示灯、仪表显示是否正常，有无告警灯；中低压开关柜断路器分、合闸状态，检查各断路器的状态是否属于机房供电正常下的分、合闸状态；
2、 听：中低压开关柜是否有局部放电异常声响、开关柜是否发生异常振动等；
3、 嗅：中低压开关柜是否有放电嗅味及绝缘过热之焦味；
4、 摸：中低压开关柜非带电部分的温度和振动情况是否正常。
5、 记录中压进线开关电压、电流值，记录中压变压器馈线开关电流值，记录低压进线总开关电压、电流值。
6、 根据移动巡检 PAD 预设的阀值，若输入数值超出预设阀值，移动巡检 PAD 页面将会显红，提示异常。巡检时如发现异常情况，也可以实时拍照上传至移动巡检 PAD，移动巡检 PAD 并将此异常实时同步至机房 ServiceBot 管理平台，进入工单处理环节，经过处理后工单关闭、验证；
7、 移动巡检 PAD 具有巡更打卡功能，记录并存储巡检路线，确保了日常巡检数量及质量。

5.1.4．UPS 不间断电源日常巡检

1、 检查 UPS 主路输入、旁路输入、输出开关是否在合闸状态，合闸指示灯是否正常，断路器保护单元是否有告警指示；
2、 检查 UPS 面板显示是否有告警信息，蜂鸣器是否有告警声；
3、 检查 UPS 面板各指示灯是否都处于正常运行状态，运行参数是否都处于正常值范围之内，检查历史记录是否有新增告警信息；
4、 检查UPS运行是否有其他异常声响及振动情况、检查有无电气元件烧焦之异味；
5、 检查 UPS 柜体上风扇运转情况，过滤网有无堵塞；
6、 检查 UPS 房及电池房温、湿度值是否在规定范围内环境；
7、 检查电池有无异常，包括电池清洁情况，有无变形、鼓胀、漏液、爬酸现象，电池房有无异味、有无异常声响等；
8、 检查电池组的连接点是否有明显过热现象，连接螺栓有无氧化等；
9、 检查 UPS 房及电池房工具是否完整，各项操作贴士、标示标签是否完好。

5.1.5．精密配电系统日常巡检

1、 检查配电柜面板指示灯，是否有报警红色灯闪烁，配电柜有无异响及异味；
2、 检查并记录配电柜面板各电量参数值，市电双路电源指示是否正常；

3、 检查精密配电柜面板有无告警信息、蜂鸣器是否有告警声；
4、 检查柜内隔离变压器有无异常振动，有无异常过热焦糊味；
5、 检查柜内散热风扇运转情况是否正常；
6、 检查各项操作贴士、标示标签是否完好。

5.1.6．柴发系统日常巡检

² 柴发机组巡检：

1、 检查发电机本机控制盘状态及有无告警，控制选择开关是否处于“远程”位置；
2、 检查机组输出开关柜、并车开关柜、接地电阻柜状态及驱潮加热器工作情况；
3、 检查机组零部件表面、管路连接处有没有漏油、漏水迹象，地面有无水迹、油迹。有没有老鼠等啮齿动物咬痕或在机房的痕迹；
4、 检查机组水箱冷却水是否足够，冷却水加热器工作情况；
5、 检查机油液位是否足够；检查油水分离器底部含水情况并从底部排除水份；
6、 检查机组充电屏电池充电电压及电流是否正常；检查电池及启动继电器端子氧化及腐蚀情况；检查应急电池组充电情况；
7、 检查日用油箱油量是否足够、油箱有无渗漏。

² 柴发低压配电间巡检：

1、 查看并车柜面板显示，选择开关是否在自动位置，有无报警指示及报警蜂鸣声；
2、 检查供油控制柜面板指示灯，选择开关是否在规定位置（机组待机时选择开关处于手动位置、机组带载运行时处于自动位置）；油箱油位（低液位 500mm、高液位 900mm）；
3、 检查直流屏显示各参数是否正常，有无报警，中央信号柜有无报警，电源模块箱散热情况；
4、 检查动力配电箱及照明配电箱是否工作正常，检查机房照明情况。

² 柴发高压配电间巡检：

1、 巡检开关状态，各个开关的状态是否属于柴发热备正常下的状态；
2、 检查开关柜 REF615 仪表指示灯状况，有无报警；
3、 检查开关柜柜内电加热器工作状态；
4、 检查柴发机组假负载控制器是否正常，有无告警信号；
5、 检查高压操作防护用品及工具是否放在规定位置。

² 柴发供油系统巡检

1、 检查并记录室外油罐磁翻板液位显示是否在 200mm 至 1800mm 之间；
2、 检查油罐区阀门井有无积水；检查阀门井是否有下陷及变形等；

3、 排查油罐区安全防火隐患；检查油罐区防雷接地措施是否完好;
4、 检查应急输油油泵及临时油管存放情况。

5.1.7．暖通空调系统日常巡检

- 机房精密空调巡检：
  1、 查看面板各项参数是否正常，有无报警信息；
  2、 检查机组运行有无振动及异响。
- 离心式水冷冷水机组巡检：
  1、 查看主机面板各项参数，有无报警及警报；
  2、 仔细聆听主机运行声音；
  3、 检查机组有无漏水、漏油；
  4、 检查主机油位，主机停机时下视镜油位不低于 1/3；
  5、 检查制冷剂管路视镜正常颜色为绿色；
  6、 检查主机冷冻水及冷却水进出水压差不低于 500Kpa；
  7、 检查、记录主机运行电流百分比。
- 冷水机组循环水泵及控制柜巡检：
  1、 检查、记录启动柜运行电流；
  2、 检查启动柜散热情况，检查启动柜是否有过热之焦糊味。
- 冷却塔巡检：
  1、 检查冷却塔冷水盘水位、结垢、藻泥；
  2、 检查冷却塔风机运行情况；
  3、 检查冷却塔循环水水质情况。

5.1.8．消防系统日常巡检

1、 火灾/气体灭火报警主机面板是否有火警、故障、屏蔽及监管信息，有无报警蜂鸣声；
2、 消防报警联动控制柜面板是否显示“系统正常”，多线控制盘指示灯、消防电话、消防广播、音频输入、功放是否在正常工作状态，打印机是否正常；
3、 气体灭火手动控制箱面板有无报警指示灯及报警蜂鸣声，正常时“手动”灯亮。气体灭火手自动转换开关指示灯正常为“手动”灯亮；
4、 空气采样控制箱面板电源指示灯常亮，检查有无故障指示灯；
5、 检查气瓶间 IG541 气瓶压力表指针是否在绿色区域，检查气瓶间气瓶瓶头阀及各分区选择阀门，检查气瓶间电磁阀控制箱；

6、 检查柴发配电间七氟丙烷无管网灭火气瓶压力表指针是否在绿色区域；

7、 检查各区域灭火器压力表指针是否在绿色区域；

8、 检查排烟风机、消防泵、喷淋泵、稳压泵电源控制箱选择开关是否在自动位置。

5.1.9．安防系统日常巡检

1、 将所有摄像机按照物理接线位置和七天三班制制成检查记录表，每班次通过视频联网监控系统检查指定的摄像机三天内的录像存储状态。通过这种方式能覆盖所有存储设备、视频编码器、摄像机，及时发现异常，确保录像存储正常；

2、 每日晚班除指定的摄像机录像存储外，还要在机房监控系统或视频联网监控系统上，一一查看所有摄像机实时视频，检查摄像机名称、系统时间、角度和清晰度等是否正常。

5.1.10．弱电监控系统日常巡检

机房基础设施监控内容表 **表 5.1-1**

服务对象	监控内容
空调系统	环境温度、湿度、出风温度、回风温度，告警情况等
供配电系统	电流、电压、功率因数、有功功率、无功功率等
发电机	启停情况、电流、电压、负载率、控制系统供电情况等
UPS 系统	输入电流电压、输出电流电压、频率、功率因数、负载率、温度、报警情况等
消防系统	报警情况等
安防及弱电监控系统	门禁状态、告警情况、监控录像、访客登记情况等

1、在监控客户端“安全时段”中检查是否有设备处于屏蔽状态；

2、在监控客户端“设备栏”中检查是否有设备处于通讯中断状态；

3、巡检监控客户端页面，查看是否有显红报警。机房监控系统通过颜色的变化来区分设备运行状态，蓝色或绿色表示正常，红色表示异常或报警，灰色表示设备通讯中断。

5.2．设备预防性维护介绍

预防性维护是为了延长设备的使用寿命和减少设备故障的概率而进行的有计划的维护。其目的是通过定期检查和保养，使设备的某些缺陷或隐患在变得更严重之前被发现。

平安数据中心根据系统设备运行情况与供应商进行沟通，按照供应商的建议提前制定年度、季度、月度预防性维护计划。各专业运维人员需按照各设备系统特性、维护流程及规范，及时、完整地落实维护工作，并形成客观实际的记录和报告予以存档。运维团队还应定期对设备的运行状态、数据进行统计和趋势量化分析，对于异常

的趋势，做出报警及相关预案，提出优化整改措施、方案，并付诸实践，最大限度降低设备发生重大故障的可能性。

5.2.1．设备预防性维护要求

- 平安数据中心基础设施的所有维护作业，均按照标准详细维护作业程序 MOP 实施，记录每一步的维护情况、维护人、维护时间。维护过程中设备操作均严格按照 SOP 进行，确保预防性维护的顺利进行，避免因误操作导致设备发生重大故障或造成人身伤害。如中压开关倒闸操作、手动启动发电机组操作，或将 UPS 转换到旁路的操作流程等必须严格按照 SOP 执行。
- 平安数据中心所有预防性维护均严格按照年度计划实施，年度维护计划达成率必须达到 95%以上。

5.2.2．设备预防性检查、维护、操作内容（包括并不限于以下系统设备或内容）

机房基础设施预防性检查内容表 **表 5.2-1**

服务对象	性能检查内容	脆弱性检查内容
供配电系统	断路器工频耐压试验、断路器主回路绝缘电阻试验、开关柜传动试验、开关柜联锁试验、柜内一次、二次回路检查、柜内除尘、孔洞封堵检查、市电外线电缆及变压器绝缘、耐压、接地检测	断路器定值试验、开关柜局部放电测试、电容检测、防雷装置检查、导线、器件发热情况等
发电机	各项运行参数检查、机组震动、发热情况等	启动电池检查、油位，冷却液位、吸气、排烟通道等
UPS 系统	器件发热情况、电池情况（外观、液位、接线柱）等	器件、导线发热情况，电池放电时间等
空调系统	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、过滤网检查等
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
安防系统	器件灵敏度、画面清晰度（不同照度情况下）	器件灵敏度、监控死角问题等

机房基础设施预防性维护、操作内容表 **表 5.2-2**

服务对象	基础类操作	测试类操作	数据类操作
供配电系统	倒闸操作	备自投测试、备自投闭锁测试	断路器保护装置日志备份
发电机	更换三滤、机身清洁等	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、机内清洁等	旁路测试、电池放电测试等	运行日志备份，报警记录备份、清除等
空调系统	启停机、清洗更换滤网、清洗更换加湿系统、清洁冷凝器等	漏水报警测试等	运行日志备份，报警记录备份、清除等
消防系统	探头清洗等	启动测试、探头测试等	报警记录备份、清除
安防系统	门禁授权等	器件灵敏度、画面清晰度（不同照度情况下）	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

5.2.3．预防性维护案例介绍

- 中压配电柜预防性维护介绍：
  1、 中压配电柜预防性维护包括一般性带电检查（每半年）、备自投切换逻辑测试（每年）、开关柜试验及柜体维护（每三年）；
  2、 以上维护均由开关柜原厂工程师实施，维护过程严格按照平安数据中心制定的 MOP、SOP 实施；
  3、 预防性维护是平安数据中心供配电系统最重要维护方式，能够发现开关柜运行中的一些潜在的安全隐患，及时排除，延长设备使用寿命确保，提高系统的可用性。
- 中压配电柜预防性维护项目：

一般性带电检查 **表 5.2-3**

分类	维护项目
配电房环境	检查并记录配电房温湿度、通风情况、电缆沟封堵、防鼠措施、防护工具、操作工具等
开关柜负荷	电压、电流值记录
开关柜温度	记录开关柜低压室、开关柜背面、开关柜正面温度
开关柜状态	保护单元显示面板及指示灯状态、电加热指示、分合闸指示、储能指示、接地开关指示、高压带电指示、保护装置压板、低压室照明等

备自投切换逻辑测试 **表 5.2-4**

分类	测试项目
市电备自投	实际断开一路市电，中压两进线一母联备自投逻辑测试
市电—柴发备自投	两路市电都中断情况下，市电与柴发备自投逻辑测试

开关柜试验内容 **表 5.2-5**

分类	试验项目	试验内容
柜体	柜体接地检查	接地主回路完整性及电阻测试
	整柜主回路试验	主回路电阻测试，耐压试验（破坏性试验，非必要不推荐）
	避雷装置试验	避雷器、监测仪检查与测试
	电流互感器	极性、变比及励磁特性曲线校核
	电压互感器	变比、空载电流等测试
	保护继电器试验	定值试验，保护、信号功能专递
	五防连锁试验	机械、电气连锁校验
	低压室二次回路绝缘试验	器件灵敏度、画面清晰度（不同照度情况下）
断路器	主回路试验	主回路电阻测试
	分合闸线圈试验	直流电阻检测、低电压动作试验
	操作机构维护	调整、维修、润滑等深度维护（用专用溶剂、专有润滑脂），以及易损件更换
	断路器控制部分绝缘试验	分合闸线圈、辅助触点、继电器、储能电机等二次元件的绝缘电阻测试
	真空灭弧室破损检测	耐压试验（破坏性试验，非必要不推荐）
专有诊断检测试验	局部放电检测	开关柜局部放电检测
	熔断器特性检测	对熔断器进行预防性故障诊断检测
	断路器机械特性检测	对断路器机械特性进行检测

开关柜维护内容 **表 5.2-6**

分类	维护项目	维护内容

母线室	清洁	主回路、绝缘件用无水乙醇清洁
	力矩紧固校验	母排连接螺栓用力矩紧固检查，应无松动，力矩标准 70N.m
	绝缘件维护	检查主母线柜间绝缘、绝缘板、动静触头盒是否有破损、放电、闪络等，并用无水乙醇清洁
电缆室	清洁	主回路、绝缘件、电缆头、互感器用无水乙醇清洁
	力矩紧固校验	电缆连接螺栓应无松动，力矩紧固检查
	绝缘件维护	检查穿墙套管、绝缘板、电缆头、互感器是否有破损、放电、闪络等，用无水乙醇清洁
	接地开关维护	操作地刀、检查闭锁连杆、位置指示是否正确，辅助触点开关转换转出，触头清洁润滑
	封堵维护	检查电缆室对动物或水汽的密封性、完善封堵
手车室	清洁	触头盒、帘门用无水乙醇清洁
	力矩紧固校验	静触头力矩紧固、帘门机构螺栓、卡簧完好性检查
	绝缘件维护	检查触头盒是否有破损、放电、闪络等，并用无水乙醇清洁
	润滑维护	对帘门机构、手车接地静触头盒导轨用无水乙醇清洁
低压室	二次元件功能性检查	二次元件功能可靠，无松动、放电、烧蚀
	端子接线紧固性校验	接线紧固，端子无烧蚀、虚接
断路器	操作机构维护	操作机构内部检查，是否有零部件缺损，清洁机构并润滑
	二次回路检查	分合闸线圈、储能电机、继电器、微动开关等接线检查
手车室	信号板检查维护	信号板调整或更换
	机械连锁检查维护	机械连锁部分润换检查，连锁可靠
	触头触臂检查维护	触臂清洁，动触头清洁、润滑、紧固

² 低压配电柜预防性维护项目：

1、低压配电柜预防性维护包括一般性带电检查（每半年）、备自投切换逻辑测试（每年）、开关柜试验及柜体维护（每三年）；

2、以上维护均由开关柜原厂工程师实施，维护过程严格按照平安数据中心制定的 MOP、SOP 实施；

一般性带电检查 **表 5.2-7**

分类	维护项目
配电房环境	检查并记录配电房温湿度、通风情况、电缆沟封堵、防鼠措施、防护工具、操作工具等
开关柜负荷	电压、电流值记录
开关柜温度	记录开关柜低压室、开关柜背面、开关柜正面温度
开关柜状态	保护单元显示面板及指示灯状态、分合闸指示、储能指示

备自投切换逻辑测试 **表 5.2-8**

分类	测试项目
备自投	实际断开一路变压器馈线开关，低压两进线一母联备自投逻辑测试

开关柜试验内容 **表 5.2-9**

分类	试验项目	试验内容
柜体	一般检查	柜面无脱漆、变形；盘面标识清晰；柜内整体无异常情况
	主母线及控制回路绝缘电阻检测	采用 500VDC 或 1000VDC 绝缘电阻测试仪测试，绝缘电阻值应不小于 1000MΩ。测试时应考虑接地方式和二次控制功能，断开相应接地
	接地连接检查	根据实际的接地系统要求检查系统及盘柜接地连接的可靠性；出线电缆的接地连接；盘柜门的等电位接地连接
	母线及电缆连接检查	用红外测温枪或成像仪检查电缆、母线连接处发热情况;用力矩扳手对主要连接部分进行紧固性检查,符合力矩要求
	抽屉回路机械性能检查	检查其位置指示状态及抽屉抽出、推入可操作性

断路器	一般检查	外观正常(连接触头无过热氧化迹象、灭弧室外无喷弧痕迹、前面板完整无缺损、框架无变形、二次端子完好、二次线标识清晰等)
	相与相及上下端口间绝检查	用 500VDC 绝缘电阻测试仪测试，绝缘电阻值应不小于 1000MΩ
	触头磨损检查(空气断路器)	打开灭弧室盖、检查三相触头磨损程度是否在可接受范围
	脱扣力检查(空气断路器)	采用专用仪器测试空气断路器主执行机构脱扣力
	机械操作检查	摇入摇出操作、手动储能、手动分合同、框架夹头压紧力检查
	连锁功能检查	检查机械及电气连锁功能正常
	机械特性测试(空气断路器)	采用 Prodiaa 机械特性检查仪测试储能电动机电流曲线及储能时速度、三相同期性、接触电阻、弹跳与超程
	保护单元动作特性检测	采用 Proselect 保护单元测试仪对保护单元进行功能测试与选择性分析
补偿电容器	一般检查	电容器外观无鼓肚变形，连接电缆无变色，接触器及串联电抗器等主要元件外观正常，柜内通风孔无遮挡防尘网无积尘等
	主进线谐波检测(带负载)/	用电能质量分析仪检测总谐波畸变率及各次谐波含量
	控制器设置及报警记录检查	检查其计量显示、参数设定、报警记录等
	电容的分相电流(带电)	手动投入时用钳形电流表测试
	分步投切时接触器状态	观察接触器投入、退出过程中的振动、噪声等
	分步投切时盘面检查指示	手动投切时观察功率因数、电流值、步数指示等显示变化
	风扇启动检查	手动启停风扇检查其功能状态
	温度报警装置检查	手动测试其工作状态
	电容器容值测试(停电时)	用电容表测试每组电容器的相间容值，不低理论值的 10%
	接触器回路电阻测试	分相测量每一路接触器的接触电阻(停电状态下，手动推合)

开关柜维护内容 **表 5.2-10**

分类	维护项目	维护内容
柜体	柜内清灰	用真空吸尘器除灰，用干布及无水酒精擦拭绝缘子、电缆连接部位
	插拔式功能单元夹头润滑	在连接部位(夹头、移动部分的镀银排、抽屉进线侧铜排等处)轻涂少许导电膏
	机械部分清洁和润滑	抽屉的定位机构、轴承、滑动导轨的清洁；只需对定位机构润滑
断路器	外部机构清洁及润滑	对摇入摇出机构、连锁机构等进行清洁及润滑
	空气断路器本体解体维护	拆解储能弹簧、分合闸线圈、储能电机、二次辅助触点、脱扣单元等，进行全面检查及清洁保养。对损耗件进行更换
	连接主触头清洁润滑	对本体及抽架上的触头及夹头进行清洁润滑
	抽架安装螺栓紧固	对抽架与柜体的安装固定螺栓进行紧固
	更换控制单元电池	对控制单元内部电池进行更换
补偿电容器	电容补偿柜内清洁	真空吸尘器除灰，用干布及无水酒精擦拭绝缘子、电缆连接部位
	内部电缆紧固	一次、二次连接电缆紧固
	通风孔防尘网更换	更换防尘网和密封胶条等
	熔断器插接头清洁润滑	清洁熔断器插接头、插接底座夹头，并轻涂少量导电膏
	故障元件及老化电容器更换	对检测不合格的电容器、熔断器、接触器等进行更换

² 柴发系统预防性维护：

1、 空载测试：每月一次，由平安数据中心运维团队实施，检测机组自动启动功能、并机功能是否正常；

2、 单机带假负载测试：每月一次单机带假负载运行，由维护商及运维团队共同实施，检测机组实际带载能力；

3、 并机实际带载测试：每年一次，由维护商及运维团队共同实施，检测机组自动启动功能、并机功能是否正常，检测机组实际带载能力；

4、 机组每月预防性维护：

A、检查发动机外观：检查发动机冷却液、燃油、排烟等系统连接部件有无松动、损坏现象，如有应立即紧固、更换；

B、检查机油油位：机组停机状态或运行状态停机至少 5 分钟后，拔出机油油位标尺,确认油位在油尺的“L”(低)与“H"(高)标记之间，油位偏低时应及时补加机油；

C、检查冷却液液位：打开冷却系统压力盖，检查冷却液液位，冷却液液位明显下降时，加注冷却液，使液位升至散热器的加注颈口下部，切记添加冷却液前应先确认冷却液温度至少下降到 50C°。补充完冷却液后，安装冷却系统压力盖；

D、目视检查冷却风扇：目视检查冷却风扇是否有开裂、螺丝松动、叶片弯曲等异常现象，如风扇有损坏等异常现象，应与供应商联系及时处理；

E、检查发动机冷却液加热器工作是否正常：若加热器工作电源正常，但温度过低，加热器可能未工作，应及时消除故障恢复加热器正常工作；

F、检查发动机进气滤清器：空气滤清器指示计在空滤组件上或组件与涡轮增压器之间，随着滤芯灰尘的增多，指示计窗口内累积计量逐渐上升，当空滤指示计窗口内累积计量超过设定值时，需要更换或清洁空气滤清器的滤芯；

G、检查进气管路有无松动：检查进气软管是否有裂纹、穿孔，卡箍是否松动，必要时拧紧或更换部件，确保进气系统无泄漏；检查卡箍下的软管是否腐蚀，必要时更换该部件以防异物进入发动机内；

H、如果配有燃油系统油水分离器，排放出里面积水的方法：需要放水时，将放水阀逆时针方向旋转大约两圈，油水分离器内的积水排放到出干净的燃油时，顺时针方向旋转关闭排水阀，但不要过分紧以免损坏螺纹；

I、 排放出燃油箱中沉淀物：根据实际需要，先用扳手拧开油箱的排油丝堵，直到放出燃油时，关闭排污阀、恢复丝堵；

J、检查蓄电池及直流启动系统：检查蓄电池接线柱是否干净，连接是否紧密，如有不洁、松动等现象，应进行清洁并重新连接蓄电池电缆线；检查直流系统各线束连接情况，更换损坏的线束；检查蓄电池与交流充电机的连接；目测检查充电机皮带，确认无裂缝等非正常现象等。

5、 机组每年预防性维护：

A、参照以上月度预防性维护项目；

B、更换发动机机油、更换机油滤清器；

C、清理日用燃油箱，更换燃油滤清器；

D、更换冷却液滤清器，更换空气滤清器。

6、柴发系统其他预防性维护：

A、每半月检查地下油罐检查孔水位并排水；

B、每月从地下油罐清油口抽取罐底燃油检查是否进水；

C、每两年更换机组启动电池及启动继电器；

D、每两年更换综合控制柜备用电池；

E、每三年更换机组冷却液；

F、每五年根据燃油品质检测报告及时对地下储油罐进行燃油置换、油罐清洗检测等；

G、每 10 年对机组进行深度保养、检测。若机组存在可靠性降低及主要性能指标达不到要求，则安排报废或更换。

² UPS 预防性维护：

UPS 预防性维护每季度一次、以上维护均由 UPS 原厂工程师实施，维护过程严格按照平安数据中心制定的 MOP、SOP 实施；预防性维护在条件允许的情况下，每季度或更长时间可对 UPS 系统进行更深入的一些功能检查。这些功能检查可能涉及对 UPS 进行切换等操作，必须确保在足够的保障措施下进行。

1、检查 UPS 输入电源质量(包括输入电压、输入频率)，检查输出电源质量(包括输出电压、输出频率以及输出波形失真率等)；

2、检查 UPS 电源切换瞬间，断电时间是否小于规定数值；

3、检查 UPS 电源切换瞬间，输出瞬时电压降是否小于规定数值；

4、检查 UPS 输出谐波失真率是否小于规定数值；

5、检查电池组的浮充电压值及充电电流值是否在设计范围内；

6、检查电池组电压值及单体电池电压值是否在正常范围内；

7、检查电池组后备时间，断开主路输入开关，电池放电 30 分钟，合上输入开关，记录 UPS 后备电池时间；

8、检查电池组是否具有启动瞬间输出大电流的特性；

9、检查电池组内阻，当内阻超过规定值时，需对电池组进行均衡充电后放电处理或活化处理；

10、检查前后级配电柜断路器手动分合操作是否正常；

11、检测并机系统均流是否在正常范围，并机 UPS 切换逻辑是否正常；

12、UPS 停机后的内部接头松紧度检查及内部主要电器部件上的灰尘清理；

13、检查 UPS 散热风扇运转情况，发现异常及时更换；

14、 在具有保障措施的情况下对 UPS 系统进行一些模拟故障检查，这些模拟故障检查可及时发现 UPS 系统的问题，避免在真正需要 UPS 系统提供保障的时候 UPS 发生故障：

A、模拟市电输入断电，观察 UPS 各种工作模式切换过程是否正常；

B、模拟市电输入断电，记录 UPS 电池组电压随放电时间的变化曲线；

C、模拟并机中的一台 UPS 故障，观察另外的 UPS 是否能正常工作。

15、 对运行五年左右的 UPS，按照厂家建议，对 UPS 交、直流电容进行预防性更换。

² 空调系统预防性维护：

1、 平安数据中心通过不间断的预防性维护，确保空调系统运行的安全稳定和绿色节能；

2、 冷水机组的月度预防性维护：

A、检查机组运行情况，记录分析运行工况；

B、检查润滑油位及颜色；

C、检查润滑系统供油，回油，油温及油冷却器工作情况；

D、检查油泵与主机起、停时差；

E、检查是否有不正常的震动及噪音；

F、检查冷冻水温度设定点与实际出水温度是否符合；

G、检查蒸发温度、冷凝温度与对应的冷冻水和冷却水进出水温差情况；

H、检查机组是否有泄漏；

I、检查电机电流并与实际电力需求进行比较，是否正常；

J、检查导叶执行机构工作情况；

K、检查机组控制组态设定情况；

L、分析机组运行工况。

3、 冷水机组的年度预防性维护

A、面板显示蒸发器和冷凝器的压力与实测压力比较；

B、转移制冷剂至冷凝器、从冷冻油充注阀排出冷冻油；

C、检查油系统回路和油冷却系统，更换油过滤器，充注冷冻油；

D、检查制冷剂系统回路，更换制冷剂过滤器；

E、蒸发器除湿抽真空；

F、机组制冷剂系统压力平衡，机组外表进行压力检漏；

G、压缩机电机、油泵电机绝缘测试；

H、检查导叶执行机构工作情况；

I、检查和清理启动柜；

J、 机组参数检查及自动控制测试：冷凝及蒸发压力、轴承温度、马达线圈温度、油槽温度、冷冻水进出水温度、压力、油压力、油压差、开启导叶、关闭导叶、启动油泵确认油压、油加热継电器数位输出信号；

K、开启机组试运行，根据现场工作情况提供机组年度维护工作单。

4、 机房空调月度预防性维护

A、检查并记录精密空调各项运行参数，控制器有无异常告警；

B、检查皮带松紧度和磨损情况，调整或更换；

C、更换或清洁空气过滤网；

D、检查比例调节阀工作是否正常；

E、检查冷凝水排水情况及机组出风情况是否正常。

5、 冷却塔月度预防性维护

A、检查、记录冷却塔运行电流；

F、检查冷却塔运行情况；风叶转动应平衡，无明显振动刮塔壁现象；水盘水位适中，无少水或溢水现象；

G、风扇减速器润滑油补充，对皮带及皮带轮检查，必要时进行调整；

H、检查布水装置是否正常；检查冷却塔补水装置是否正常；

I、 检查填料使用情况，是否有堵塞或破损；

J、 检查冷却塔管路及结构架、爬梯等锈蚀情况，及时进行处理。

6、 冷却塔其它预防性维护

A、每季度清洗冷却塔塔盘及填料；

B、每年对电机绝缘进行检测；

C、5 年左右更换冷却塔填料，可根据具体使用条件确定冷却塔填料更换周期。

7、 水系统管网和水质月度维护

A、检查管道、阀门等处有无滴水、漏水情况；管道保温材料上是否有漏水迹象；

B、检查管道有无异常位移、下沉、弯曲和变形情况，发现情况及时上报；

C、检查阀门表面，看有无渗漏、锈蚀等异常情况，发现漏水情况及时处理；定期对阀门进行操作，确保启闭灵活；

D、检查管道法兰有无腐蚀、松动、漏滴水等异常情况；

E、检查水系统管路，管道及各附件(软接、止回阀、水处理器)外表整洁美观、无裂纹，连接部分有无渗漏，发现问题及时处理；

F、 对水管管路和阀门去锈刷漆，保证油漆完整无脱落；保温层破损的及时进行修补；

G、检查管网吊支架安装是否牢固，有无脱离、变形等异常情况；检查防止管道木托有腐蚀变形等异常情况；

H、检查冷却水是否清洁，根据需要进行水质更换；定期进行水质分析，根据需要进行水质处理，如定期加入杀菌灭藻剂、阻垢剂和缓蚀剂等；

I、 检查冷冻水系统软化水水质情况，检查软化水系统；

J、 检查压力表和温度计指示是否准确，表盘需清晰，损坏的应及时进行更换；

K、 检查冷却塔补水浮球阀和冷冻水定压补水装置是否正常；

L、 清洗水管管路上的过滤器(过滤器两端压差超过 0.05MPa)；

M、 冬季情况下室外管路要做好防冻措施；

N、分水器、集水器压力表及温度计计量准确。

8、 循环水泵预防性维护

A、每季度补充润滑油；

B、 每季度检查水泵密封情况，若有漏水应进行检修；

C、 每年对联轴器同心度进行测试和校准，检查联轴器的连接螺栓和橡胶垫，若有损坏应予以更换；

D、每年紧固机座螺丝并对泵组做防锈处理；

E、 每年一次对水泵检修，对叶轮、密封环、轴承等重点部件进行检查并根据情况清洗叶轮和叶轮通道内的水垢。

9、 电机、配电及控制系统的月度维护

A、电机运行正常，轴承润滑良好，绝缘电阻在 2MΩ以上；所有接线牢固，负荷电流及温升符合要求；

B、各变频器、软起启动器运行情况检查，温升不应超过标准；

C、 各种电器、控制元器件表面清洁，结构完整，动作准确，显示及告警功能完好。

5.3．预测性维护介绍

为了确保平安数据中心安全平稳运行，运维管理团队利用各项仪表、仪器以及第三方专业检测机构，对数据中心关键基础设施（供配电、UPS、柴油机、冷水机组、防雷接地系统等）进行周期性监测。对系统或设备红外温升、振动情况、燃油及

润滑油化学成分等数据进行综合性及趋势性分析，判断系统运行健康状况，帮助运维管理人员及早发现系统潜在风险，以便得到有效及时处理，预测性维护是平安数据中心安全运行的重要主动性维护活动之一。

5.3.1．预测性维护要求

- 制定详细的预测性维护年度计划，按照维护计划严格落实；
- 预测性维护所使用的仪器、仪表必须严格遵照质量监督部门校准程序，定期对其进行校准、核对，确保仪器、仪表检测的准确性；
- 聘请第三方专业检测机构对数据中心系统或设备进行检测，并出具相关检测报告。
- 预测性维护相关操作需严格按照 MOP、SOP 程序实施，确保维护过程设备安全及人身安全。
- 预测性维护完成，需形成完整的维护报告，并且和往年数据进行对比，进行趋势性分析。

5.3.2．预测性维护项目

机房基础设施预测性维护检查 **表 5.3-1**

检查对象	检查内容
供配电系统	变压器、母排、断路器、电容器等红外热成像检测、直流屏蓄电池核对性放电检测
发电机	燃油及润滑油化学成份检测、电气系统红外热成像检测、机械振动检测
UPS 系统	红外热成像检测
空调系统	冷冻机油化学成份检测、管道探伤、冷机机水泵机械振动检测
机房环境	由第三方专业检测机构对机房含尘、电磁辐射、噪音、防雷接地等进行检测
防雷接地	按照防雷检测规范定期对建筑防雷接地检测

5.4．应急演练介绍

平安数据中心运维团队根据各系统实际运行情况，制定了详细、完善的故障或事件应急操作流程，并定期组织应急演练，很大程度上提高了整个团队应对各种突发故障或事件的应急处置能力，对整个数据中心的高可用性奠定了基础。

5.4.1．应急演练要求

- 必须事先针对某一故障或异常情况制定完善的应急操作流程，组织运维团队学习，并熟练掌握；
- 制定应急演练年度计划，严格按照年度计划推进各项应急演练实施完成；
- 沙盘演练：参与演练的运维人员集合，并分别口述在发生紧急情况下自身所应承

担的职责及将会执行的方案及步骤；

- 跑位演练：参与演练的人员跑位到模拟故障现场，模拟处理故障，参与人员应清晰地说出故障的处理方案及步骤。

5.4.2．应急演练项目

系统或设备故障类应急演练 **表 5.4-1**

演练项目	演练内容
低压配电系统应急演练	模拟变压器进线开关跳闸，联络开关备自投闭锁，手动合闸联络开关
中压配电、柴发系统应急演练	1、模拟双回路市电一路市电中断，中压母联备自投闭锁，手动合闸中压压母联开关 2、模拟市电中断，柴发自动启动失败，手动启动柴发、手动并机流程
供电、空调系统切换演练	供电、空调系统实际切换，验证机房供电系统高可用性
冷冻水系统应急演练（主机故障）	模拟运行中冷水机组故障停机，快速切换至备用机组
UPS 系统和精密配电柜故障演练	1、模拟一套 UPS 系统供电故障，紧急切换到维护旁路供电 2、模拟一台精密配电柜供电中断，紧急恢复供电
监控系统应急演练	模拟主用监控务器故障停机，切换至备用监控服务器
空调系统应急演练（水系统异常）	模拟机房冷冻水管道泄漏，紧急关停各机房区域冷冻水阀门，机房精密空调切换至风冷状态，检查室外机散热能力及机房温湿度变化情况
电梯应急救援演练	模拟电梯轿厢困人，安全解救被困人员
机房给排水系统应急演练	模拟地下室水浸，快速排出地下室积水
消防系统演练	1、模拟机房火灾，气体灭火系统自动流程及手动操作流程、报警联动控制 2、人员应急疏散逃生演练

5.5．系统可用性检查

平安数据中心运维团队通过对数据中心场地环境、各系统或设备运行状况及参数设定、关键设备监控报警阀值、设备信息列表、机柜PDU和开关关联进行定期核查，以及聘请第三方专业机房检测公司定期对机房进行定期检测，进一步提高了数据中心各系统的可用性。

5.5.1．机房基础设施月度检查

在日常巡检的基础上，每月定期组织对机房基础设施进行一次全面检查，对一些异常或需优化项目进行梳理，将问题录入ServiceBot系统，由专业工程师进行跟踪处理，逐一销项，并在备注栏详细阐明优化整改措施，进一步提高系统或设备可用性。

5.5.2．机房基础设施场地环境检查

每月定期组织对机房基础设施场地环境进行一次全面检查，对一些需优化项目进行梳理，将问题录入ServiceBot系统，由区域责任进行跟踪处理，并在备注栏详细

阐明优化整改措施。

5.5.3．机房基础设施其它信息核查

定期对机房基础设施设备运行设定值、开关分合闸状态、机柜PDU对应开关、设备运行或备用指示标签、设备明细及清单、设备操作贴士、监控报警阀值、监控报警过滤等进行核查或更新，便于机房基础设施精细化管理实施。

5.6．生命周期管理

数据中心全生命周期，是指从建设意图产生到数据中心经济寿命结束的全过程。通常分为决策期、实施期和生产运维期，每一个时期又分为若干阶段。决策期包含需求收集、规划、选址、项目的可行性分析等，实施期包括从项目设计到建设，竣工验收移交等，运营是指项目基本建设完成后，从项目投入使用直到项目经济寿命结束的全过程。

本篇章主要讲在运营阶段的设备生命周期管理，良好的设备生命周期管理，通过识别硬件设备在运行中的风险点，制定化解风险的方案，不仅能够降低设备的故障率，提高数据中心的高可用性，而且还能延长数据中心的使用寿命，使数据中心取得最大的效益。

在数据中心基础设施方面，平安数据中心主要考虑对中低压配电设备、变压器、UPS设备、柴发设备、冷机设备进行全生命周期的规划，主要工作包括设备的定期检查，易损关键部件的更换，设备的淘汰和更新。

5.6.1．中压柜生命周期规划管理

中压柜关键部件包括断路器、母排和柜体，需要每半年进行一次例行维护，每三年进行一次深度维护；断路器规划寿命为 15 年（或操作次数 10000 次），需要在第 14 年评估运行情况，必要时作财务预算，对更换断路器进行立项，次年进行采购更换；开关柜母排、柜体划寿命为 20 年，需在第 19 年评估运行情况，必要时作财务预算，对更换柜体进行立项，次年进行开关柜轮换报废工作实施，制定新的生命周期管理规划及维护计划。

5.6.2．低压柜生命周期规划管理

低压柜关键部件包括断路器、母排、柜体和电容补偿器，需要每半年进行一次例行维护，每三年进行一次深度维护；断路器规划寿命为 15 年（或操作次数 30000 次），需要在第 14 年评估运行情况，必要时作财务预算，对更换断路器进行立项，次年进行采购更换；开关柜母排、柜体划寿命为 20 年，需在第 19 年评估运行情况，必要时作财务预算，对更换柜体进行立项，次年进行开关柜轮换报废工作实施，制定新的生命周

期管理规划及维护计划；电容器由于寿命较短，5-8 年，应该根据厂商建议或者使用情况，对电容进行更换，建议整个开关柜生命周期内更换 2 次。

5.6.3．变压器生命周期规划管理

变压器需要每一年进行一次停电维护，每六年进行一次预防式维护；变压器规划寿命为 20 年，需在第 19 年评估运行情况，必要时作财务预算，对更换变压器进行立项，次年进行变压器轮换报废工作实施，制定新的生命周期管理规划及维护计划。

5.6.4．柴油发电机生命周期规划管理

柴油发电机组内的润滑系统、空气滤清器、燃油系统，需要每年对内部的机油滤芯、柴油滤芯、空气滤芯进行更换。

冷却系统中的冷却剂及冷却水滤清器每三年进行一次更换。启动电池每两年更换一次。

柴油发电机组规划寿命为 15 年，需在第 10 年评估运行情况，根据事实情况判断是否继续使用，如果继续使用，在第 14 年制定第二年财务预算，次年对机组进行轮换报废。

5.6.5．UPS 生命周期规划管理

UPS 内部的交直流电容属于易损件，寿命一般为 5-6 年，可以根据厂商的评估建议进行更换，建议每个 UPS 生命周期中，更换两次电容。

UPS 蓄电池根据电池的使用情况，建议在 UPS 的生命周期中至少更换一次。

UPS 规划寿命为 20 年，需在第 19 年评估运行情况，作财务预算，对更换 UPS 进行立项，次年进行 UPS 轮换报废工作实施，制定新的生命周期管理规划及维护计划。

5.6.6．冷水机组生命周期规划管理

冷水机组内的油过滤器、冷媒干燥过滤器、冷冻油需要每年对其进行更换。

冷水机组规划寿命为 15 年，需在第 10 年评估运行情况，根据事实情况判断是否继续使用，如果继续使用，在第 14 年制定第二年财务预算，次年对机组进行轮换报废。

5.7． 风险管理

平安数据中心运维团队通过有效对数据中心在运行中各种风险进行管理，有利于运维团队做出正确的决策，有利于保护企业资产的安全和完整，有利于实现数据中心管理团队的目标达成，对数据中心运维具有重要意义。

5.7.1．缩略语和定义

风险管理是数据中心在运行中发现在一个肯定有风险的环境里把风险可能造成的不良影响减至最低的管理过程。

5.7.2．风险识别

平安数据中心通过运行风险分析列表来识别机房风险，风险识别也是平安数据中心对风险管理的首要环节。在全面了解各种风险的基础上，在进行预测危险可能造成的危害，从而选择处理风险的最佳手段。

风险的识别是通过风险分析表来实现，风险的分类分为三类：高级风险为无法承受的运行风险，一旦发生，机房无法在短时间内恢复正常的运行状态，会给公司造成严重的损失。中、低级风险虽然严重危及运行安全，但大部分只是造成局部运行异常或形成运行安全隐患，属于可承受和可控制的运行风险。

注：数据中心的运维风险不是一成不变的，会随着机房内相关要素的变化而改变，有时会影响风险等级，有时则会产生新的风险，平安数据运维会不定期进行风险分析表的更新。

机房运行风险分析表 **表 5.7-1**

风险分类	高	中	低
机房安全	机房发生火灾	机房部分设备发生火险	
	机房大面积漏水	主要机房地面积水	机房局部漏水
	机房建筑物发生坍塌	机房建筑物局部损毁	机房建筑物险情
		消防系统失控	消防系统异常
		空调系统失效或失控	温度或湿度异常
		门禁系统失控	门禁系统异常
		机房照明系统失效	照明系统异常
		机房监控系统失效	机房监控系统异常
运行安全	核心设备故障停机	主要设备因故障停机	
	机房大面积停电	供电异常	
	空调水系统爆管	单个机房空调系统故障停机	
	整套柴发系统故障	柴油发电机组故障停机	
	核心网络线缆中断	主/备网络线缆中断	部分网络电缆中断
管理及人员安全	人为破坏事故	严重操作失误	一般操作失误
		管理机构及责任缺失	
		规章制度不健全	管理松懈
	人员伤亡		人员受伤
财产管理	重要设备损毁	局部设备损毁	设备故障
	重要设备（数据）丢失	设备丢失	设备配件丢失

其他	雷击导致供电或网络通讯中断	发生雷击	防雷设施失效
		鼠害损毁线缆	发现老鼠、蛇
	发生严重电磁干扰	发生一般电磁干扰	

5.7.3．风险管理表

在识别数据中心运维风险后，将通过风险管理表来对识别后的风险进行管控、跟进、应对、以及关闭或风险转换为问题处理。风险管理表具体内容如下：

- 风险提出日期：一般在风险被识别后即为风险提出日期。
- 风险描述：对可能发生的风险进行内容描述，便于数据中心运维团队人员可通过描述理解风险情况。
- 风险可能性：风险发生的可能性定义为高、中、低三个层级，根据风险可能发生几率判断和定义级别。
- 风险影响程度：参照机房风险运行分析表中内容定义风险影响程度，影响程度分别高、中、低三个级别。
- 风险等级：风险分为高、中、低三个级别。
- 风险负责人：一般风险是专人负责风险管理和跟进。
- 风险管理策略：风险管理策略分为规避、减缓、接受三个策略，由风险负责人根据风险评估后对风险进行策略分类。
- 风险应对措施：对已经识别的风险进行定性分析、定量分析和进行风险排序，风险负责人根据数据中心运行情况制定风险处理方案。
- 风险应急措施：一旦发生风险就要做到快速反应、快速恢复。应急措施需要制订一整套科学有效的机房运行风险应急方案，包括如何启动风险处置的报告体系、组建负责人力资源调动和现场协调指挥的组织机构、安排负责处置风险的各方面专业技术人员等内容。
- 风险管理状态：风险管理状态分为开放和关闭两种，开放状态是需要对风险进行跟进和定期记录更新，关闭状态为该风险已闭合，便于后续对同样风险进行参照可查。
- 风险变更记录：对在风险管理过程中进行的重要操作、风险管理重要进展、进行记录登记。
- 风险更新日期：在风险管理表中内容进行新增、删除、修改需要更新日期。
- 风险关闭类型：分为：风险已规避、风险已转化为问题、接受该风险等。
- 风险关闭日期：风险通过风险各种应对措施，最终将风险进行了规避、减缓或接

受，该时间点为关闭风险时间。

- 风险转移：将一些可以预见但发生概率较低的风险，通过购买保险、设备维修外包等形式，转移给保险公司和机房设备服务商。如购买财产保险，可将机房风险(机房建筑物风险、火灾风险等)转移给保险公司；通过机房设备外包的方式，可将 UPS、精密空调等设备故障风险转移给设备维修服务公司。

5.8．平安数据中心资产管理

5.8.1．平安数据中心资产管理的特性

平安集团作为国内金融牌照最齐全、业务范围最广泛、控股关系最紧密的个人金融生活服务集团之一，业务规模多样化，不同业务之间交互，IT 系统之间耦合度高、架构复杂，以及业务规模发展迅猛和业务频繁变更，导致 IT 设备每天面临上百次的变动/变更，以及金融机构要求出现故障后快速恢复的时效性要求，需要在平安数据中心 10+万级别以上的庞大规模设备中迅速定位故障设备，并找出设备与应用的关联关系等特性，对数据中心资产管理的高效性提出了更高的要求，需要数据中心有适用于自身的管理特性资产管理系统提供工具化支持。

5.8.2．平安数据中心资产管理制度化建设

5.8.2.1 明确数据中心资产管理范围

平安集团涉及到专业公司众多，和 IT 有关的资产众多，分布范围广，基于处理复杂的资产情况，数据中心和负责公司资产管理制度建设和管理职能的资产管理室在公司的资产管理制度中明确数据中心资产管理范围为“总部数据中心内”的物理区域，并在公司发布的文件中予以正式公布。

5.8.2.2 建立公司数据中心资产管理领用制度

数据中心资产从状态上来看，主要有两类，一类是投产设备、一类是未使用设备，对于投产的设备，设备上有应用系统运行，根据公司 IT 系统的管理规范，投产设备会有应用系统层面监控、OS 层面监控、硬件运行状态监控等三层自动化监控手段，设备未经过授权和批准的变动，会引发各类报警，资产管理员可以及时发现。但”未使用设备”，在管理方式上没有有效的自动化监控手段，必须依靠设备领用制度来保证，设备领域制度和公司财务系统相关联，如果不办理领用，设备将无法办理正常的财务报销手续，无法支付购买设备的款项。

5.8.2.3 建立公司数据中心资产管理专人负责制度

平安数据中心设置专门的资产管理员岗位负责数据中心内的资产管理，做到专人专管。资产管理员岗位的技能要求为熟悉数据中心类别，工作细心认真，工作中有耐心、

严格按照资产管理制度处理各类资产的管理工作。

5.8.2.4 建立报废资产处置制度

经过公司资产管理室讨论确定建立报废资产处置制度，对数据中心内未加电运行、并超过财务折旧年限的设备，每年安排 2 次报废处置，及时清理无用资产，提高资产数据的“清洁度”。

5.8.3．开发适用于自身数据中心管理需要的资产管理系统

5.8.3.1 开发数据中心资产管理系统必要性

从平安数据中心发展数量来看，每年设备增长数量都在万级以上，要应对这种增长数量级，必须建立自己的资产管理系统，记录资产变动相关节点，积累信息，就可以采用大数据分析的方式，总结出自身资产管理方面的分析及预测。目前平安数据中心建立了使用于自身管理需要的“收货管理系统”、“IDC 视图管理系统”、“OPCM 管理系统”等多个系统，并开发出 PC 版、APP 版等多个版本支持在办公区域使用，和在机房现场移动办公使用。

5.8.3.2 开发数据中心资产管理系统要重点关注的问题

重点关注配置管理库(CMDB)和配置项(CI)设计，一是在设计过程中不能追求大而全，导致 CMDB 过于庞大，维护 CMDB 耗费过多精力；二是不要期望设计出可以解决数据中心、服务器、存储、网络、应用层面等的全能的系统，而最终发现任何一个组件的问题都无法很好地解决。

另外，在开发资产管理系统的过程中，引入的是一些知名厂商的现成产品，厂商成品最大的问题是产品的通用性，但无法解决平安数据中心资产管理中的实际问题，或是相关开发人员无实际运维经验，开发周期长，开发出来的系统和实际需要的系统差距太大。

5.8.3.3 平安数据中心资产管理系统

为解决上述问题，2016 年平安数据中心开发适用于自身资产管理需要的 OPCM 系统，开发过程中确定了两个原则，一是精简 CMDB 和 CI，在资产管理系统的开发上要追求少而精，只要能解决 95%的日常工作即可，其余 5%的工作可以通过现场查看或登录 OS 系统查看配置的方式解决（例如设备网卡数、每张网卡的 mac 地址等）。从而避免 CMDB 库过于庞大；二是从数据中心运维人员中培养开发人员，解决非专业运维人员开发出来的系统难用的问题；目前已开发 OPCM 系统并投产，解决了平安数据中心资产管理方面的问题。

5.8.4．数据中心资产管理系统使用案例

5.8.4.1 实现数据中心资产的全生命周期管理

下图是 OPCM 管理系统中的一个实例，从收货开始，记录了数据中心中设备信息及整个生命周期过程。

图 5.8-1

5.8.4.2 实现设备硬件相关配置信息管理

图 5.8-2

5.8.4.3 实现设备和应用系统关联关系管理

图 5.8-3

5.8.5．数据中心资产现场管理

5.8.5.1 平安数据中心资产现场管理的特性

平安数据中心资产的现场管理包含两类，一类为数据中心内运行中的设备，一类为库房内未使用的设备。金融行业业务对故障恢复时效有更高的要求，当数据中心内运行中的设备出现故障时，需要迅速获取到设备的配置信息、所运行的应用信息，应用联系人信息，以及使用库房内未使用设备进行故障设备替换时需要迅速获取设备的配置信息等，是数据中心设备管理中的不同于其他行业的一个显著特性。为解决这个问题，平安数据中心对现场设备采用“二维码”标签进行管理，并开发出适用于 Ipad、手机等移动办公终端的“机房管理 APP”。

5.8.5.2 平安数据中心二维码介绍

随着移动技术的发展，二维码的应用越来越广泛，二维码的使用为工作、生活提供极大的快捷性和便利性。平安数据中心在资产管理过程中也引入二维码的管理方式进行资产的管理。目前使用的二维码主要有两种，一种是针对设备等有序列号标识的资产，将设备的序列号采用二维码生成器制作为资产二维码的标签，粘贴到设备附近区域用于识别，另一种是机柜等没有序列号标识的资产，采用按照公司的命名规范进行命名，然后将所命名采用二维码生成器制作二维码标签。具体二维码图例见下：

- 设备二维码标签：

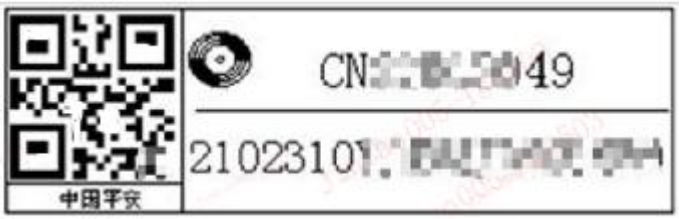

图 5.8-4

- 机柜二维码标签：

图 5.8-5

5.8.5.3 平安数据中心资产二维码使用案例

- 扫码设备二维码查询设备信息

图 5.8-6

Ø 扫码机柜二维码查询机柜中所有设备信息

图 5.8-7

5.8.5.4 平安数据中心资产报废资产处置

数据中心内达到报废年限或是无法再继续使用的资产(即报废资产清单)，要及时安排报废处置，这样既可提高数据中心的电力、空间等的有效利用率，降低数据中心的运维成本，又可提供数据中心资产数据的“清洁度”。资产报废处置由数据中心资产管理员负责，并规定每年安排不少于两次，并纳入资产管理员的 KPI。报废资产处置流程为资产管理员提供数据中心内报废资产清单通过邮件沟通方式和用户确认是否使用．对于确认不再使用的资产，由资产管理员提交报废申请签报，由用户、数据中心经理、数据中心部门长、资产管理室、财务部门审批通过后，再由资产管理室组织拍卖。资产管理室在公司实物系统中对资产实物账务数据进行处理，数据中心对 OPCM 的记录进行清

理。然后提交报废资产处置申请 EOA 签报，经用户、数据中心经理、数据中心部门长、资产管理室、财务部门审批通过后，中标方拉走拍卖的报废资产，至此整个报废资产处置流程完毕。

5.8.5.5 平安数据中心资产盘点

虽然数据中心有 OPCM 系统对资产进行管理，但是偶尔会出现人为录入错误导致的记录信息不准确的“脏数据”，对于这些“脏数据”的修正，目前唯一有效的方式就是通过资产盘点的方式来发现并修正，平安数据中心对资产盘点分为两种方式进行，数据中心内部每季度安排一次自查修正，每年度公司资产管理室从整个公司层面安排一次公司所有资产的盘点，通过这两种盘点方式，目前平安数据中心资产准确率可达到 99.8%以上。

5.9．数据中心日常管理

5.9.1．平安数据中心日常管理的特性

平安数据中心为平安集团保险、银行、投资等传统金融提供服务，也为陆金所、金融一账通、壹钱包等互联网金融提供服务。传统金融类业务成熟，但架构复杂，稳定性要求高，故障恢复时效要求高，出现故障未在规定的时效内恢复必须上报监管部门。因此传统金融业态对数据中心的要求变更少，稳定第一；互联网金融服务属于新业态，要求上线时效短，先在市场上抢先机，使用过程中发现问题在不断修正。因此互联网金融业态对数据中心的要求是变更频繁，迅速抢占市场第一。另外，传统金融服务也在逐步向发展互联网，使平安数据中心内业务架构复杂，既有原来依赖于“OEM”产品的老传统架构，又有依赖于平安“金融云”的新兴互联网架构但又必须和“OEM”产品的老传统架构相关联的架构，还有完全按互联网架构和思维模式运行的新架构，这对平安数据中心的运维管理不断提出新的挑战，需要数据中心对各类业务生态进行细分，精细化管理，既能满足传统金融类业态需求，又能满足互联网类金融业态的需求。

5.9.2．平安数据中心日常管理制度建设

5.9.2.1 建立分区域管理制度

平安数据中心为平安集团内的保险、银行、证券类业务提供服务，所提供的保险类金融服务要符合保监会的要求，银行类服务要服务银监会的要求，证券基金类服务要符合证监会的要求，互联网类金融（例如陆金所、征信）要符合人民银行的要求，并每年接受保监会、银监会、证监会和人民银行登记监管机构的检查。根据这些业务特征，平安数据中心建立了分区域管理的业务制度，根据各类监管部门的规定，有物理隔离要求的，通过独立模块或建立物理隔离栏的方式进行物理区域隔离；没有物理隔离要求的，

但要求独立机柜的，通过业务集中在独立机柜内，并对独立机柜上锁的方式进行隔离。针对不同的业务特点，制定不同的管理制度，从而进行区域化精细管理。

当然，随着新技术，新业态的不断涌现，监管机构为实行新形势的发展，在监管规定上也会不断变化，这就要求数据中心管理者时刻关注监管机构在数据中心管理规定方面的变化，并随之对平安数据中心分区管理的制度进行修订。

5.9.2.2 建立"服务窗口"和"维护窗口"制度

数据中心分区管理制度可以保证完全相互独立的业务之间的设备维护彼此间不受影响，但对于平安数据中心这种既有传统金融架构，又有互联网金融架构的混合型金融类型，不同系统之间存在交互的情形也不在少数，对于这种"牵一发而动全身"的业务类型，如何才能兼顾到"大多数"的业务要求，平安数据中心和各方协商出的"服务窗口"和"维护窗口"，在"服务窗口"内，必须保证业务系统稳定运行，不能进行维护或变更。维护和变更只能放在"维护窗口内"进行。单一业务维护不影响其他业务的，就放在其指定的"维护窗口"进行维护或变更，多个业务之间有相互关联的，放在多方都能接受的"维护窗口"进行，实现针对不同业务类型日常维护上的精细化管理。另外，针对在"服务窗口"内已经造成业务中断或是存在业务中断重大隐患的，也可以在"服务窗口"内实施维护，但必须执行严格的报批管理制度，使针对此类异常情况有解决通道，也不会造成这种异常解决通道的滥用。

"服务窗口"和"维护窗口"简要示例 **表 5.9-1**

业务系统	服务窗口	维护窗口
保险类	**:** - **:**	**:** - **:**
银行类	**:** - **:**	**:** - **:**
证券类	**:** - **:**	**:** - **:**
互联网金融类	**:** - **:**	**:** - **:**

5.9.2.3 建立容灾管理制度

平安数据中心为保证业务的持续可用性，建立了容灾管理制度，根据业务的关键性对业务进行等级划分，等级系统越高，要求建立的容灾级别越高，例如 1 类系统，属于传统架构的类型的，要求建立远程容灾（异地灾备）和同城灾备，并根据系统的 RPO 和 RTO 等指标投入不同的资源，确保 1 类系统提供业务连贯性的能力，对于互联网架构的应用，要求建立多地多活（远程多活）和同城双活，确保 1 类系统提供业务连贯性的能力。并且每年由集团容灾管理部门组织容灾演习，确保数据中心可为业务系统提供连续性。

5.9.2.4 建立数据中心变更管理制度

从业界数据中心的管理经验来看，数据中心故障中 70%都是人为操作所引发的故障，加上平安数据中心作为 IT 系统的最关键一个环节，其中出现故障可能会影响到集

团各个业务系统，因此平安数据中心对变更管理有严格控制。根据变更特点，将变更分为日常变更、常规变更、重大变更，对于日常变更需由当班工程师审核并提交分组经理审批通过才能实施，对于常规变更由当班工程师审核、分组经理审核并提交部门长审批才能实施，对于重大变更，由当班工程师制定实施方案、分组经理和部门长审核，并提交运营管理中心变更管理委员会讨论并审批通过才能实施。从而实现变更管理的精细化管理。

另外，日常管理中还有事件管理、问题管理、配置管理等制度，和变更管理一起构成 IT 管理的四大管理核心，考虑到事件管理、问题管理、配置管理等在其他章节有详细描述，本章节不再赘述。

5.9.2.5 管理权限分级制度

平安数据中心内运行平安集团各专业公司的业务系统，为确保数据安全，平安数据中心采用了权限分级管理制度，规定数据中心管理人员只能管理数据中心现场的设备运行环境、物理布线、设备位置变更等工作，硬件管理员只能管理硬件，操作系统管理员只能管理操作系统级权限，应用运维人员只能具有应用级权限，开发人员不能具有生产系统的权限，即每个岗位只能管理和自身有关的组件，无法管理到整个系统。另外，开发环境、staging 环境、生产环境、容灾环境等分别由不同的职能组管理，测试环境使用生产环境数据必须经过脱敏处理。通过这些权限分级管理制度，将所有人员、环境等的权限最小化，防止用户数据人为泄密、篡改和盗用。

5.9.2.6 信息安全管理制度

作为一个优秀的数据中心，除了保证数据中心的稳定运行外，数据中心信息安全也是一个非常重要的组成部分，尤其作为金融类数据中心，公司对平安数据中心的信息安全性提出两个零容忍（重大合规内控风险事件：零容忍；重大信息安全事件：零容忍）。为实现公司的要求，数据中心对文件（文档）建立分级管理，根据文件（文档）的重要性，将纸质和电子档文件分为秘密、机密、绝密等三种类型，并设置文件管理员岗位，由专人管理数据中心的文档管理。对于带出数据中心的故障硬盘，能通过消磁方式防止数据泄密的，必须进行消磁和物理损毁；固态硬盘等无法通过消磁防止数据泄密的，和厂商在合同中约定故障硬盘不返厂服务，厂商工程师不能将其带走，由平安数据中心回收统一做物理销毁；对于因数据恢复需要备份磁带，必须通过加密方式备份，磁带异地保存时要使用专用的磁带保管箱加锁，磁带交接必须签字锁在保管箱内，由与公司签署保密协议的有资质的专业押运公司进行押运。

5.9.2.7 日常运维审核制度

平安数据中心在日常运维过程中，除了每季度安排 1 次内审外，每年还聘请集团信息安全部、BSI、安永等外部知名机构，对数据中心的信息安全体系、日常运维体系等进行审计，并且对审计发现的问题不断进行整改，提高数据中心管理工作的持续有效

性，目前数据中心已通过 ISO9001、ISO20000、ISO27001、Uptime M&O 等认证。

5.9.3．开发适用于自身数据中心的 IDC 管理系统

5.9.3.1 开发数据中心 IDC 管理系统必要性

平安数据中心内部设备数量达到 10 万+以上，运行的业务系统有上千个，在数据中心的管理过程中发现仅仅靠人无法保证数据中心稳定、持续的运行，主要体现在以下 5 个方面：

1）设备数量庞大，系统众多，人力根本无法满足业务系统运维的要求；

2）人员技能差异化，同一件工作，不同人员做出来结果会有差别；

3）即使同一件工作，同一人在不同状态、不同心态和不同时间点做出的结果存在差别；

4）人员积累的经验无法有效传承；

5）无法实现标准化作业。

因此需要开发出一个有效的数据中心管理系统，实现数据中心标准化管理，平安数据中心培养了有数据中心运维经验的开发人员，开发出了 IDC 视图管理系统和机房管理 APP，提高了机房管理效率，实现了数据中心的标准化和精细化管理。

5.9.3.2 平安数据中心的精细化管理

5.9.3.2.1 平安数据中心整体化精细管理

通过 IDC 视图管理系统，可以实时了解到平安各数据中心模块的电力资源、空间资源、业务系统分布等资源使用情况，以及对业务系统发展趋势和历史使用情况等进行大数据分析，发现业务系统机柜资源不足的，提前进行扩容，完成业务系统在整体数据中心内的灵活调配，实现平安数据中心整体化精细化管理。下图为平安数据中心某个模块的使用情况：

图 5.9-1

5.9.3.2.2 平安数据中心各模块的精细化管理

通过 IDC 视图管理系统，实时了解各数据中心内的所有机柜空间使用情况，功率使用情况，根据各数据中心现状和未来趋势，对数据中心各模块实现精细化管理。

图 5.9-2

5.9.3.2.3 平安数据中心机柜的精细化管理

通过 IDC 视图管理系统，实时了解每个机柜的功率、空间使用情况，以及每个机柜内设备的运行情况，结合机柜的功能分区特性，根据业务特征和大数据分析，在单机柜最大功率为 6KW 的情况下，机柜高度 46U 时，VXLAN 架构每个机柜可支持 18 台服务器，TOR DB 架构每个机柜可支持 18 台服务器，大数据应用可支持 15 台机器，金融云应用可支持 16 台服务器;根据这些数据，结合应用特征，充分利用每个机柜的每个 U 位，做到机柜的精细化管理。

5.9.3.3 平安数据中心设备位置自动分配系统

平安数据中心这种小批量、多批次的服务器上线特征，结合空间、旧线缆充分利用的特征，平安数据中心开发了设备上架位置自动分配系统。

设备机柜位置自动分配系统的设计原理是根据新上架设备的基础信息库中的数据（设备 U 位和该型号设备的历史功率经验值），结合当前机柜功能分区、机柜功耗、空间使用情况来判断某机柜是否可以增加此服务器。

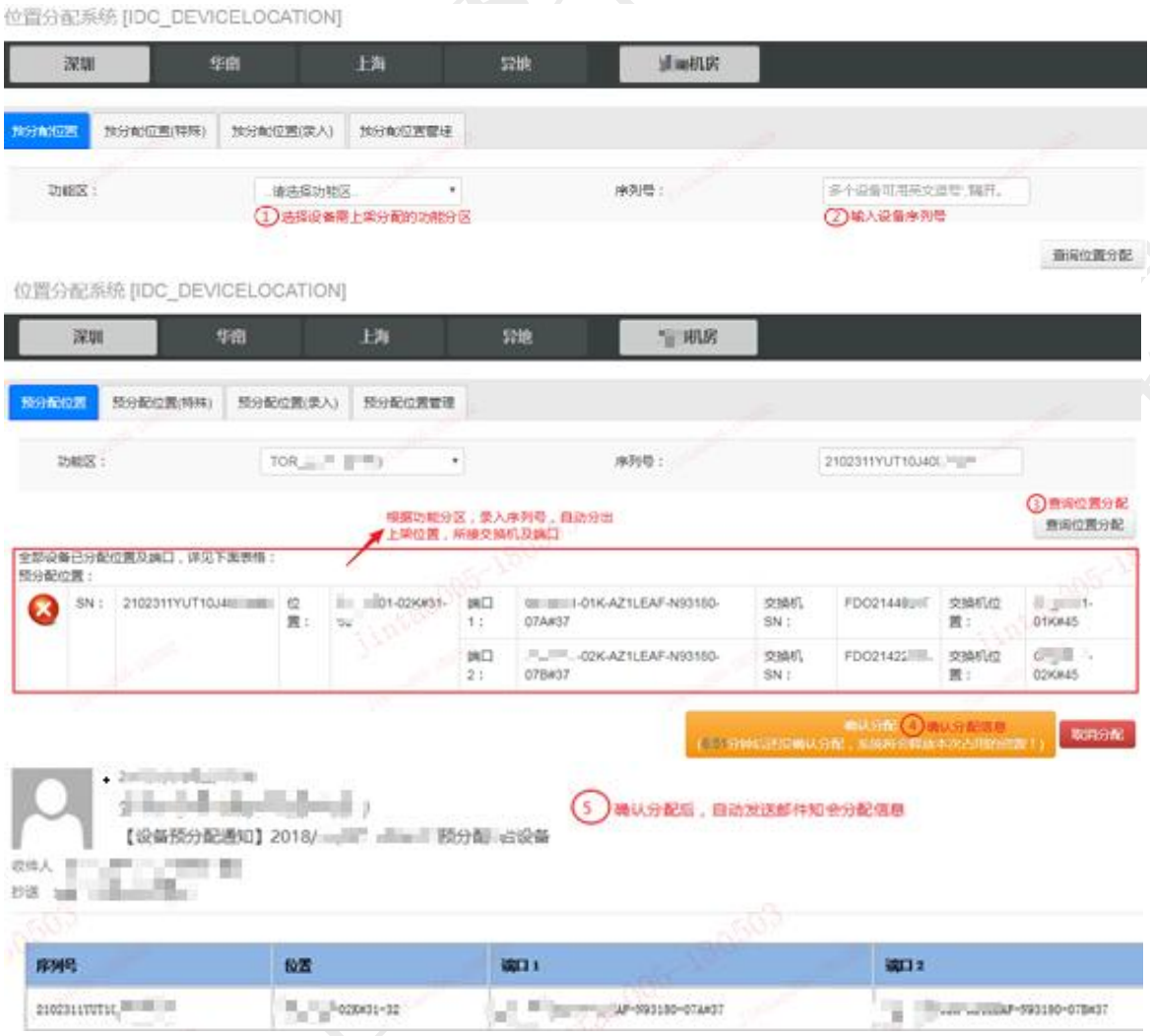
位置分配系统 [IDC_DEVICELOCATION]
深圳
华南
上海
异地
机房
预分配位置
预分配位置(特殊)
预分配位置(录入)
预分配位置管理
功能区：
请选择功能区
序列号：
①选择设备需上架分配的功能分区
②输入设备序列号
查询位置分配
位置分配系统 [IDC_DEVICELOCATION]
深圳
华南
上海
异地
机房
预分配位置
预分配位置(特殊)
预分配位置(录入)
预分配位置管理
功能区：
序列号：
2102311YUT10J40
③查询位置分配
查询位置分配
根据功能分区，录入序列号，自动分出
上架位置，所接交换机及端口
全部设备已分配位置及端口，详见下面表格：
预分配位置：
SN：
2102311YUT10J4
位置：
端口1：
交换机SN：
交换机位置：
端口2：
交换机SN：
交换机位置：
确认分配
④确认分配信息
取消分配
⑤确认分配后，自动发送邮件知会分配信息
【设备预分配通知】2018/
收件人
抄送
序列号
位置
端口1
端口2

图 5.9-3

第六章、运维质量保障体系

本章介绍检验数据中心运维质量的方式，包括平安内部安全部门的审核，平安数据中心内部不同分组的互相审核，外部的 M&O 的认证审核，ISO9001、ISO27001、ISO20000 体系审核。

6.1．内部审核

内部审核，有时称第一方审核，由组织自己或以组织的名义进行，用于管理评审和其他内部目的，可作为组织自我合格声明的基础。在许多情况下，尤其在小型组织内，可以由与受审核活动无责任关系的人员进行，以证实独立性。

平安数据中心内部审核包括科技数据中心内部审核和集团公司内部审核:

6.1.1．科技数据中心内部审核

平安数据中心内部季度审核包括不同数据中心的相互审核、相同数据中心不同分组的相互审核。规范内部质量管理体系审核活动，审查和评价质量管理体系运行的符合性和有效性，确保质量管理体系持续有效地运行，并为质量管理体系的改进和完善提供依据，审核严格按照审查标准程序实施：

- 各岗位职责
  - (1) 中心各岗位：对内部审核发现的不合格项制定并实施纠正措施。
  - (2) 内部审核成员：根据《数据中心内审检查表》实施内部审核。
  - (3) 内部审核组长：编制内部审核的实施计划，组织内部审核小组成员对质量管理体系各岗位实施审核，主持首、末次会议和编写内部审核报告，跟踪纠正措施执行的情况。
  - (4) 管理者代表：评审年度内部审核计划以及内审报告，并提交中心经理审批。
  - (5) 中心经理：批准年度内部审核计划和内审报告。
- 审核程序
- 审核计划

  审核组长负责在管理评审时策划并组织讨论第二年度内审核划，该计划应该确保：
  - (1) 每年内部审核不得少于 4 次；
  - (2) 在一年的审核期间内覆盖 ISO9001 标准要求的所有要素；
  - (3) 审核计划应该对频繁出现的不合格项进行重点审核；
  - (4) 确保交叉审核，即审核员应该避免审核本岗位的工作；
  - (5) 在中心出现重大的质量隐患或者质量体系出现重大改变时，包括文件要求改变、

组织部门调整、运营流程变更、产品（服务）要求变化等，应该及时安排审核；

(6) 年度内部审核计划应该包含审核时间、频率、审核范围。中心经理批准计划，使该计划具有正式的效力。管理者代表将计划传达到中心各岗位。

Ø 审核前准备

(1) 在内部审核的前一个月，由管理者代表指定内部审核组长，并成立内部审核小组，指定其成员；

(2) 由审核组长分配审核小组成员的工作分工，内部审核应由与受审对象(部门或岗位)无直接关系的内部审核员负责；

(3) 审核组长制定内部审核实施计划，经管理者代表批准后，至少提前一周下发给受审核的对象。审核计划的内容包括：确认审核对象、范围、日期；审核的准则；审核分工。

(4)受审核的对象收到审核计划后，若有异议，可在两天内通知受审核小组，经过协商调整审核计划。

(5)审核组长提前检查审核员取得的《数据中心内审检查表》是否为最新版本。

Ø 内部审核实施

召开首次会议，首次会议由审核小组全体人员、受审核对象代表、主要工作人员及陪同人员、管理者代表和高层的管理者(必要时)参加。(本地交叉内审时可不召开首次会议，但异地交叉内审时需召开首次会议)，由内部审核组长主持，首次会议的内容包括：

(1) 审核组长介绍审核小组成员及分工；

(2) 重申审核的范围、准则和目的；

(3) 简要介绍审核采用的方法；

(4) 指出各被审核的对象需要提供的配合；

(5) 澄清审核计划中不明确的内容。

Ø 现场审核

(1) 内部审核员按照《数据中心内审检查表》实施审核，审核方式包括：记录抽样检查、现场观察、询问、凭证检查等；

(2) 在审核过程中，如果发现问题，应当场让该项工作的负责人或操作者确认并记录在《数据中心内审检查表》中，以保证不合格项能够完全被理解，有利于纠正；

(3) 现场审核结束后，在召开末次会议前，审核组长召集审核小组成员召开审核小组总结会，汇总审核发现，确定所有的不合格项报告。

Ø 末次会议

末次会议由审核组全体人员、受审核对象代表、主要工作人员、管理者代表、高层的管理者(必要时)参加。(本地交叉内审时可不召开末次会议，但异地交叉内审时需召开末次会议)，由内部审核组长主持末次会议，对内部审核全过程进行总结。末次会议的

主要内容包括：

(1) 重申审核的范围、准则和目的；

(2) 向受审核方说明审核发现；

(3) 展示审核发现不合格项内容及证据；

(4) 提出审核小组的结论和建议；

(5) 审核组长说明对纠正措施采取的监督工作。

Ø 审核报告

(1) 由内部审核组长编写内部审核报告，对审核进行书面总结，对审核发现的不合格项进行统计分析，找出主要的问题区域和改善区域，并且提出下次审核的重点。

(2) 由内部审核组长把内部审核报告通报管理者代表，并抄送中心经理。

(3) 由内部审核组长向各受审核岗位通报审核情况。

(4) 纠正措施的落实及跟踪

(5) 各被审核对象根据内审检查发现，对不合格项及观察项确定纠正措施，填写措施应该注意：

★举一反三，尽可能杜绝类似的不符合项；

★措施应该清晰明确、可以操作，操作效果能够衡量；

★确定每项措施的落实时间。

(6) 内部审核组长根据《数据中心内审检查表》记录的不合格项跟踪纠正措施的落实情况，如果效果达到则关闭报告，效果没有达到则要求责任人重新采取措施。具体按照《分析与改进控制程序》执行。

(7) 内部审核组长将措施的执行情况反馈给管理者代表和中心经理，同时在下次的内部审核中关注有无类似的问题再发生。

(8) 内部审核中使用的全部记录由审核组长移交文件管理员，按《质量记录控制程序》执行。

(9) 内部审核的结果应提交管理评审，按《管理评审程序》执行。

关联文档

《数据中心内审检查表》

《分析与改进控制程序》

《质量记录控制程序》

《管理评审程序》

6.1.2．集团公司内部审核

公司内部审核主要有内部信息安全审核，审核内容如下表

机房检查资料获取清单 **表 6.1-1**

编码	资料类别	资料名称	时间范围	备注
1	数据中心环境	机房建设规划选址及简介		
2		数据中心布局图		
3		防雷设备分布		
4		烟感温感探头分布图		
5		水管、漏水布线分布图		
6		灭火设备分布图		
7		监控摄像头分布图		
8		物理环境安全评估报告		
9		空调冷水管道平面图		
10	机房管理	机房管理岗位职责分工表		
11		服务商选择\管理\评估记录		
12		设备采购合同		
13		电信运营商合同		
14		机房设备/资产清单		
15		设备进出机房申请及放行、签收记录		
16		设备验收记录		
17		设备移出机房处置记录		
18		介质室磁带进出机房记录		
19		介质目录清单及盘点记录		
20		磁带消磁记录		
21	访问控制	机房门禁权限清单		
22		机房门禁开通申请记录流程单		
23		机房门禁权限删除记录		
24		机房访问权限评审记录		
25		临时进入机房申请记录		
26		机房访客登记记录		
27		进出机房保密承诺书签署记录		
28		门禁系统日志\门禁进出记录		
29	机房运维	机房日常巡检记录		
30		机房设备巡检记录		
31		设备维保记录		
32		安全出口开启报警记录		
33		机房问题清单		
34		机房问题处理流程签报\机房故障处理流程签报		
35	机房运维系统	机房运维相关系统清单		
36		机房运维相关系统账号权限清单		
37	机房演练报告	消防演练报告		
38		电力中断演练报告		
39		漏水报警演练报告		

40		柴油发电机演练报告		
41	制度	ISO 质量管理文档和操作手册		
42		服务商选择\管理\评估标准/制度		
43		访客登记标准流程		
44		手提式灭火器检查标准		

6.2．外部审核

外部审核包括通常所说的“第二方审核”和“第三方审核”。第二方审核由组织的相关方(如客户)或由其他人员以相关方的名义进行。第三方审核由外部独立的审核组织进行，如那些对与 GB/T 19001 或 GB/T 24001 要求的符合性提供认证或注册的机构。

平安数据中心外部审核包括 M&O 换证审核，ISO9001 审核，ISO27001 审核，ISO20000 审核：

6.2.1．M&O 换证审核

M&O 运维标准是从多维度、多架构、多视角、多层面地对数据中心的运营管理进行整体上的管理标准化设置，优化运维管理体系，并从培训演练、规划调整和实际操作等具体层面，设置各类标准化要求并实际考察实施，从而推动标准化运营管理体系的建立与落地实施，提高运维人员的管理水平，进一步提高数据中心的服务水准。

M&O 的一个认证有效期为两年，每两年需对数据中心的流程、制度以及这些流程制度的落地进行审计，审计打分制，80 分合格。

主要审计标准包含 5 大类、20 小类标准框架内容。

M&O 审核项目清单 **表 6.2-1**

序号	类目	组成	信息要求
1	人员与组织	员工	● 员工计划（数量和职责） ● 升级和呼叫流程（包括内部与内部、内部与供应商之间）
2		资质	● 培训证书和培训记录 ● 责任分工（责任区、培训、安全）
3		组织	● 组织架构图显示如下信息： -基础设施组织架构明细 -数据中心组织架构明细（基础设施、IT、安全等部门） 每个基础设施岗位的工作描述
4	维护	预防性维护	● 预防性维护的列表和时间表 ● 预防性维护的方法 ● 预防性维护的工作单 ● 测试用工具的校验 ● 关键备品备件的清单以及订购要点 ● 冗余组建之间的切换流程
5		清洁政策	● 主机房清洁政策

6		维护管理系统	● 预防性维护的完成率 ● 开环和闭环的工作流程
7		供应商支持	● 供应商列表和 SLA
8		延期维护计划	● 延期维护的清单 ● 延期维护的维护程序
9		预测性维护	
10		生命周期管理	
11		故障分析程序	● 断电的历史记录以及纠正动作
12	培训	数据中心 员工培训	● 每个岗位的培训需求表 ● 参与培训记录 ● 每个课程的培训大纲
13		供应商培训	● 供应商培训需求表 ● 参加记录 ● 培训课程大纲
14	计划、协调及管理	机房政策	● 机房政策 -标准操作流程 -应急操作流程 -配置管理政策
15		财务管理	● 发展计划和预算流程
16		参考图书馆	● 图书馆的权限 ● 资料的更新流程
17		主机房管理	● 机房的规划和增长需求 ● 电力和供冷的管理流程 ● IT 设备上下架的管理流程
18	运行状况	负载管理	● 负载管理政策
19		运行设定点	● 运行设定点政策
20		设备轮转	

6.2.2．ISO9001 审核

Ø 有认可的 ISO9001 认证证书意味着什么

ISO 9001 指定了在以下情况下对组织的质量管理体系的具体要求：需要证明其能够持续提供满足顾客和适用法律和监管要求的产品和服务；旨在通过有效应用管理体系提高客户满意度，包括改进体系和保证符合客户和适用法律和监管要求的过程。

Ø 有认可的 ISO9001 认证证书不代表什么

1) 重要的是要认识到，ISO9001 定义了组织的质量管理体系的要求，而不是其产品和服务。获得 ISO9001 认证应该让组织相信，能够“始终如一地提供符合客户和适用法律法规要求的产品”。它不一定保证组织将始终实现 100%的产品合规，尽管这应当是永久目标。

2) 获得 ISO9001 认证并不意味着组织能提供优质的产品或服务，或者产品或服务本身已通过 ISO（或任何其他）标准或规范的认证。

Ø 评审的目的、范围和准则

重审（战略回顾方式）的目的是进行监督评审，寻找积极的证据，以确保组织的管理体系能够在认证周期内有效地、持续满足认证范围的要素及管理标准的要求，获得信任，并且证明体系有能力支持实现法律、监管和合同要求以及组织制定的目标，适用于管理标准的范围，并确认前瞻性战略计划的持续实现和适用性。如果本次审核是多地点审核的一部分，最终认证推荐将由所有地点的审核发现决定。

审核的范围是 ISO9001 标准要求的文件化管理体系，和在审核计划中明确的受审核方管理体系包含的地点和区域：

Ø 审核发现的定义：

(1)不符合项:

未满足要求

(2)严重不符合项:

影响到管理体系实现预期结果的能力的不符合。 在下列情形中，不符合项可以被归类为严重不符合项：

- 对过程控制是否有效、或者产品服务能满足规定要求存在严重的怀疑 ；
- 多项轻微不符合都与同一要求或问题有关，可能表明存在系统性失效，从而构成严重不符合项。

(3)一般不符合项:

不影响管理体系达到预期结果的能力的不符合项。

(4)改进的机会:

这是审核员在审核期间所做的事实陈述，并通过客观证据加以证实，具体是指管理体系的弱点或潜在缺陷，如果不加以改进，将来可能会导致不合规项。 根据公正性要求，我们认证机构可以为过程和体系的改进提供通用信息，包括解释标准的含义和意图、识别改进机会、解释相关的理论、方法论、技巧或工具、分享行业良好实践的非保密信息，等等。但不能针对特定特护提供具体的解决方案。

(5)观察项:

这仅适用于那些禁止认证机构在审核发现中包括提出改进机会的认证项目。观察项是审核员所做的事实陈述，具体是指管理体系的弱点或潜在缺陷，如果不加以改进，将来可能会导致不符合项。

6.2.3．ISO27001 审核

目前，在信息安全管理方面，ISO27001——信息安全管理体系标准已经成为国际上应用最广泛与典型的信息安全管理标准，它是由英国标准 BS7799 转换而成的，最新版本为 ISO27001：2013。

平安数据中心早在 2008 年已经取得了 ISO27001 认证，ISO27001 标准认证证书的有效期为三年；从 2008 年至今，平安每年都邀请专业认证机构进行“年度监督审核”；证书三年到期后，进行全面的再认证审核。

ISO27001 标准的价值在于：

（1）通过定义、评估和控制风险，确保经营的持续性和能力；

（2）减少由于合同违规行为以及直接触犯法律法规要求所造成的责任；

（3）通过遵守国际标准提高企业竞争能力，提升企业形象；

（4）明确定义所有组织的内部和外部的信息接口目标：谨防数据的误用和丢失；

（5）建立安全工具使用方针；

（6）谨防技术诀窍的丢失；

（7）在组织内部增强安全意识；

（8）可作为公共会计审计的证据。

积极持续组织审核，表明平安对数据中心信息安全的重视，通过审核，是对平安数据中心在信息安全保障方面所作出努力的充分肯定，更有益于公司整体信息安全管理水平的提升。

6.2.4．ISO20000 审核

ISO20000 是基于 ITIL 最佳实践与 BSI15000 英标体系进行构建的、于 2005 年 12 月 15 日由国际标准化组织发布的第一部关于信息科技服务管理体系的认证国际标准，是一套通过管理和规范服务流程确保 IT 服务质量的国际标准，是为组织提供能够证明其 IT 服务能力和服务质量的公认认证标准。

ISO20000 认证的意义并不仅仅限于 IT 服务符合规程和提高服务质量。它在服务量化、员工绩效考核、衡量 IT 部门投资回报方面更具有积极的意义。

平安数据中心的运维服务体系已经通过 ISO20000 认证，这表明数据中心的运维服务管理能力得到国际权威机构的认证，同时提高了服务管理水平和人员的服务管理意识，进而提升整体 IT 服务管理和运行管理水平，以支撑平安各项业务不断发展。

平安数据中心持续进行 ISO20000 的“年度监督审核”，以及每三年的换证审核。