**服务可用性和业务连续性**

**管理制度**



青岛慧海联创信息技术有限公司

2025-01-04

文档信息

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 文档名称编号 | 服务可用性和业务连续性管理制度（HHLC-ITSS-FWKYX/YWLXX） | | | |
| 编制单位 | 青岛慧海联创信息技术有限公司 | | | |
| 文档版本 | 版本日期 | 版本说明 | 作者 | 审核 |
| V1.0 | 2025-1-4 | 发布版本 | 郑永伟 | 张仲全 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

目的

为确保公司核心IT服务在面临各种中断性事件（如硬件故障、自然灾害、网络攻击、人为错误等）时，能够保持预定的可用性水平，并能够快速、有效地恢复，最大限度地减少对业务运营的影响和损失，特制定本制度。

范围

1. 本程序适用于为满足服务预定可用性目标和连续性目标所进行的管理。
2. 所有新增运维服务以及当前已经签订服务级别需求（SLR）和服务级别协议（SLA）的运维服务；
3. 那些不一定签订正式的《服务级别协议》但对组织业务却极为关键的运维服务；
4. 可能影响可用性的IT基础设施和IT支持部门的所有方面，包括培训、政策、流程的有效性以及程序和工具等。
5. 导致连续性发生的条件:包括火灾、大规模断电、硬件瘫痪、自然灾害、失窃、暴力破坏、人力资源危机等意外事件，可能中断运维服务并且影响组织的正常业务运营，最终导致业务损失。

定义

可用性：可用性是指一个组件或一种服务在设定的某个时刻或某段时间内发挥其应用功能的能力，因此，高可用性意味着服务对客户是持续可用的，宕机时间少且可迅速恢复，表示方法：

用绝对数来表示，如可用时段为 8：00 到 18：00；

用相对数来表示，如平均可用性级别最低为99%;

两者的结合，如在开发时间内平均可用性级别为99％。

决定因素：

（A）IT 基础架构的复杂程度；

（B）快捷有效地对故障作出反应的能力；

（C）组件的可靠性；

（D）运营级管理流程的质量和范围；

（E）由支持部门和供应商提供的维护的质量；

（F）IT 基础架构的弹性。

业务连续性：是一个综合性的管理过程，它旨在识别组织所面临的潜在威胁，以及这些威胁一旦发生对业务运营可能带来的冲击，并为此建立有效的响应框架和恢复能力，以保护关键利益相关方的利益、保障核心业务功能的持续运作，并维护组织的声誉和品牌价值。

职责

运维服务部：

1.确保运维服务在经过设计后，实际的服务级别（以可用性、可靠性、可服务性、连续性等指标表示）能够符合约定的服务级别；制定《服务可用性和业务连续性计划》；

2.撰写可用性报告；

3.优化IT基础架构的可用性，从而为提供给企业的服务实施成本合理的改进。

4.实施和维护运维服务服务过程中的连续性管理，根据风险评估结果，制定并管理连续性计划

流程

服务可用性

一旦客户确定了一项服务的可用性要求，运维管理部就可以确定一系列输入要求，以满足要求的服务级别。

识别可用性需求

#### 需求识别时间

1. 在签订《服务级别协议》之前进行；
2. 需考虑新的运维服务和需要对现有服务作出的变更两个方面；
3. 应当在尽可能早的阶段确定是否能够满足这些需求以及怎样满足这些需求。

#### 需求识别应考虑内容

关键业务功能；

1. 约定的运维服务中断时间；
2. 可量化的可用性需求；
3. 非计划的运维服务中断对业务功能所产生的可量化的影响；
4. 客户的业务运作时段；
5. 有关维护窗口期的约定。

可用性设计

1. 那些影响可用性标准的薄弱环节应当尽早得到确认。有助于防止额外的开发成本、计划外的后期支出、单点故障、供应商收取的额外成本以及延迟的发布等情况发生。
2. 基于适当的可用性标准的一个良好的可用性设计可以使得有可能与供应商签订有效的维护合同。设计过程中采用了一些技巧，如确认单点故障的组件故障影响度分析。
3. 3,如果可用性标准不能够实现，最好的选择是确认设计是否可以进一步改进。
4. 如果可用性需求特别难以达到，则应当考虑使用其它的容错技术、其它的服务流程（事件管理、问题管理和变更管理）或额外的服务管理资源。

恢复方案设计

1. 1.确保运维服务故障发生后，运维服务能在最短的时间内得以恢复以使正常的业务运营继续进行；
2. 2.构建一个对故障具有高度弹性的IT基础设施即使不是不太可能，也可能会造成成本过于高昂；因此，在给定的成本约束下，IT基础设施满足可用性需求的能力常常取决于可以对运维服务故障进行及时有效恢复的能力。
3. 设计恢复方案考虑因素：
4. 确保业务与技术恢复流程是正确的；
5. 清晰定义负责主要事件的员工的职责。
6. 安全性问题
7. 安全性和可靠性是密切相关的，一个较差的信息安全设计会直接影响到服务的可用性。
8. 高可用性要靠有效的信息安全来支撑。在规划阶段，应该考虑相关的安全问题，对安全问题可能给服务供应带来的影响也应当加以分析。

与安全问题相关的活动主要有：

1. 确定谁将有权访问安全区域；
2. 确定需要作出哪项关键授权。

维护管理

IT组件都必须按照计划进行维护活动。有计划的维护活动可以使IT支持部门能够：实施预防性维护以避免故障的发生；

1. 及时进行软件和硬件升级以提供新的功能和额外的服务能力；
2. 根据业务需求对IT基础设施实施必要的变更；
3. 激活IT基础设施中新增的功能。
4. 计划性维护活动涉及的首要问题是计划停机时间。
5. 在确定新增或改进后的运维服务的可用性需求时，需要明确计划性维护所需的停机时间以及由此导致的收入方面的损失。
6. 在运维服务1天24小时或一周7天都必须正常运作的情况下，可用性管理就必须在权衡计划停机时间需求和相应的业务损失之后确定最优的维护方案。

制定《可用性计划》

1. 为有效地实施有关可用性管理活动以改进IT组件及服务的可用性，必须制定明确的《可用性计划》。
2. 《可用性计划》不仅需要关注技术方面的问题，还应对可用性管理的人员、流程、工具和技巧等方面进行考虑。在可用性管理的初始阶段，可用性计划与实施通常是紧密结合进行的，但这两者却又是不同的，不能将它们混淆。
3. 《可用性计划》的计划周期应当覆盖协议约定时长。
4. 《可用性计划》应当和《能力计划》和财务预算的周期保持一致。

《可用性计划》一般包括以下部分：

1. 对目前状况可用性的评估；
2. 改善现有服务活动的步骤；
3. 实施新服务与维护的一系列计划。

监控、评价和报告

1. 评价和报告是重要的可用性管理活动，它们为核实服务协议，解决问题和制定改进建议提供了基础。
2. 可用性报告在每次服务报告中作相应说明，其中可以包括下列指标：
3. 以平均修复时间（MTTR）、平均无故障时间（MTBF）和平均系统事件间隔时间表示的可用率（或不可用率）；

总体正常运作时间和宕机时间；

故障的次数；

有关故障可能实际或潜在地导致比约定数更高的不可用率的额外信息。

业务连续性

初始化阶段

#### 定义组织策略

1. 有关运维服务连续性管理的政策应当尽早地制定并充分传达给组织内所有的相关人员，从而使他们意识到实施运维服务连续性管理的需求；同时管理层也需要明确表达他们的承诺。
2. 运用风险评估方法来估计运维服务风险发生的概率，为了管理这些风险，组织需要制定风险预防和风险恢复方案，这些措施应基于质量标准；安全管理指南和通用的组织策略。
3. 确定适当的管理架构（清楚划分职责）和应对灾难的流程。

#### 分配资源

1. 需要投入人力和物力建立一个运维服务连续性管理环境。
2. 组织需要对员工进行培训来保证员工有能力实施风险预防和灾难恢复措施。

分析规划阶段

#### 业务影响分析

1. 在有些情况下，服务在灾难发生后仍可以继续运作一段时间，因而其重点是恢复服务；而在其它情况下，没有运维服务的支持业务将完全不能运作，因而其重点将是预防。
2. 服务分析：对某些不重要的服务而言，可以规定在灾难发生时使用能力和可用性有限的应急服务。但需要注意的是，即便是在灾难恢复期间，服务级别也只有在与客户达成协议之后才能进行修改。对于关键性服务来说，必须在进行预防和制定恢复方案之间选择某种平衡
3. 基础架构分析：在完成服务分析之后，需要评估服务和 IT 资源之间的依赖关系，灾难恢复服务所需要的额外资源。

#### 风险评估

1. 通过确认业务中存在的威胁和薄弱环节以及相关的预防措施可以为管理层提供有价值的信息。
2. 优先考虑使用各种预防措施。如果所有这类预防措施全都用上了，则有必要进一步确定是否还存在需要制定应急计划的残余风险。
3. 风险分析
4. 必要确认相关的 IT 组件（资产），包括建筑物、系统和数据等；
5. 分析这些资产所面临的威胁以及这些威胁之间的相关程度，并估计灾难发生的可能性；
6. 要确认这些资产的薄弱环节，并进行分类；
7. 根据各 IT 组件的具体情况评估威胁和薄弱环节，从而评估风险的级别。
8. 恢复方案
9. 不采取任何措施，此方案应用于无需运维服务能独立运营的部门。
10. 回复至手工（基于纸质的）系统-这种方案对于那些对业务有关键性影响的服务来说是不可接受的，但对于那些不甚重要的、小的服务仍然是可行的。
11. 互助协议安排-当两个组织具有类似的硬件并同意在灾难发生时互相提供相关设施时可以使用这种方案。
12. 逐渐恢复-这种方案使用于那些在一段时间（如 72 小时）内没有运维服务也能运作的企业。
13. 中期恢复-这种方案可以使服务在接入一个类似的运作环境后经历一段短暂的过渡期（24-72 小时）便可以继续正常运作。
14. 内部式恢复（相互支撑）-如果企业有多个办公场所或可用于生产的专门的测试环境，可以采用这种内部式恢复方案。
15. 外部式恢复-由第三方恢复组织提供商业服务，这些组织通常是为多个客户服务的
16. 移动式恢复-这种方案所需的基础设施一般都是用一辆拖车装载着。
17. 立即恢复-这种方案提供了即时的或非常快速的恢复服务，如在不超过 24 小时之内
18. 针对分析结果应形成书面性的建议内容，汇总到《业务影响分析报告》中。

实施阶段

#### 组织和实施计划

1. 实施风险降低措施：故障发生直接影响服务的可用性，因此实施风险降低措施必须结合可用性管理进行。
2. 实施备用方案：恢复方案的实施有赖于一系列的备用方案，包括场所、系统及供应商方面。对于备用方案需要进行测试、操作培训及维护以确保需要时可以立即启动备用方案。
3. 制定《连续性管理计划》，保证实施人员可以直接按照流程文档实施恢复方案：确保可以持续地提供有关关键系统、服务和设施的必要信息或在可接受的时段内能够恢复此类信息。

运作阶段

#### 连续性计划测试

1. 运维管理部经理安排组织连续性计划范围内的人员编制测试计划并进行测试，测试完毕结果归并到《连续性管理计划测试报告》。
2. 根据服务需要，运维管理部经理会同公司领导对连续性管理计划测试结果进行评审，形成《连续性管理计划评审报告》，记录测试存在的问题，并在必要时修改《连续性管理计划》

#### 沟通和培训

1. 项目经理组织有关人员进行沟通或培训，确保有关人员知道自己的职责和任务。
2. 必要时项目经理对培训的效果进行评价。

#### 连续性计划维护

1. 对一线人员进行连续性方面的意识培养，使他们将维护连续性作为常规的工作。
2. 对连续性流程进行定期评审以确保经常性的更新。
3. 每年至少应进行必要的连续性计划测试。
4. 评审和测试以后需要进行日常的变更管理，因此也需要连续性得到及时更新。
5. 进行包括维护人员和销售人员的培训，以保证在必要的时候他们有能力完成业务恢复工作
6. 保证连续性生命周期的最后程序得到市场中心经理和公司领导的确认，以保证连续性流程的运营流程得到顺利的执行。
7. 公司定期对连续性计划所需得到人员、技术及基础设施进行检查、评价，以确保连续性计划的有效性。

与其他流程的关系

与事件管理流程的关系

可用性、连续性中断的发生，均应在事件管理流程中得到记录。

与问题管理流程的关系

系统相关隐患被识别，需要根源调查、处置，以提高可用性，可通过问题管理流程进行管理。

与变更、发布管理流程的关系

为提高系统可用性和连续性，产生的系统变更，应通过变更、发布管理流程进管控。

与配置管理流程的关系

配置管理数据库为可用性、连续性系统分析提供数据基础。因可用性、连续性发生的配置变更，也应对相关的配置项进行更新。

关键指标

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **衡量指标** | **指标计算说明** | **考核频次** |
| 1 | 业务可用性 | 可用时间/整体运行时间\*100% | 季度 |
| 2 | 服务连续性 | 由于突发事件导致故障的次数 | 季度 |

相关文件

《服务可用性和业务连续性管理程序》

《信息安全管理程序》

《运维服务能力管理制度》

记录

《服务可用性和业务连续性管理计划》

《可用性分析报告》

《连续性测试报告》