**服务可用性和业务连续性**



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（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 | 宫海亭 | 张仲全 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**1** **目的**

确保在所有情况下都可以实现向客户承诺的服务连续性，帮助客户组织在发生灾难之后尽快恢复 IT 服务和确保业务的持续运营。确保业务运作所需的 IT 基础架构和 IT 服务在灾难发生后的限定时间内能够得到恢复，从而对组织的总体业务连续性管理提供支持。

**2** **适用范围**

本程序适用于 ITSM 所覆盖的所有项目。

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 IT 服务并且影响组织的正常业务运营，最终导致业务损失。

实施连续性计划的范围包括：

a)重点关注和支持关键业务流程的 IT 服务项目；

b)对具体的 IT 技术和服务需求提供支持。

**3** **定义**

3.1 服务连续性管理 : 负责预防灾难、增强 IT 基础构架的弹性和容错能力的流程，确保组织在发生灾难后具有足够的技术、财务和管理资源来确保 IT 服务的连续性和稳定性运作。

备注：本体系文件中，连续性和持续性具有相同含义，特殊说明除外。

3.2服务可用性：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。

3.3服务可用性管理：建立和维护信息系统可用性的流程及为达到此目的而根据特定需求所提供的服务。

**4** **职责和权限**

4.1 运维服务负责人责任:

a)实施和维护 IT 服务连续性、可用性管理流程；

b)保证该流程任何时候都能满足业务连续性、可用性管理的需求；

c)在业务连续性管理中代表 IT 服务组织。

d)成员组成：客户服务人员

4.2 项目经理职责：

a)安排 IT 服务项目的服务风险评估报告,连续性计划, 连续性测试报告的审核；

b)成员组成：运维部主管、技术中心主管。

**5** **工作描述**

5.1 过程流程图（见图 1 持续性管理流程）

5.2 业务连续性过程描述

5.2.1 连续性需求识别和分析

5.2.1.1 项目经理或连续性负责人员根据服务合同（SLA）识别连续性需求分析，连续性需求分析包括：

a)服务针对其所提供业务处理的定义；

b)服务对所在机构具备的重要性；

c)服务所支持的用户数量；

d)故障发生以后，如何保证业务连续性和稳定性。

5.2.1.2 需求识别时间：

a)在签订服务级别协议之前进行；

b)需考虑新的 IT 服务和需要对现有服务做出的变更两个方面；

c)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。

5.2.1.3 需求识别内容：

a)关键业务功能；

b)可量化的连续性需求。

5.2.2 确定连续性管理范围

5.2.2.1 定义组织策略

a)有关 IT 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 IT 服务连续性管理的需求；

b)同时管理层也需要明确表达他们的承诺。

5.2.2.2 识别应用 IT 连续性管理流程的相关领域

a)运用各种不同的风险评估方法来估计 IT 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发生后恢复方案，这些措施应基于 ISMS 管理体系，安全管理指南和通用的组织策略；

b)此外，还需要确定适当的管理架构（清楚划分职责）和应对灾难的流程。

5.2.2.3 分配资源

a)需要投入人力和物力建立一个 IT 服务连续性管理环境；

b)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。

5.2.2.4 项目管理

使用项目管理方法应用到恢复措施的实施中。

5.2.3 业务影响分析

a)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 IT 服务的支持业务将完全不能运作，因而其重点将是预防。

b)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。

c)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。

d)灾难扩散影响的层叠效应。

5.2.4 风险评估

5.2.4.1 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。

5.2.4.2 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。

5.2.4.3 风险分析

a)确认相关的 IT 组件（资产），包括建筑物、系统和数据等；

b)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（高、中、低）；

c)要确认这些资产的薄弱环节，并进行分类（高、中、低）；

d)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。

5.2.4.4 服务风险评估报告

根据上述分析的结果，由项目经理和连续性管理员编制《XX 信息系统连续性服务风险评估报告》。

5.2.5 制定连续性计划

5.2.5.1 预防措施

a)在充分考虑了预防措施的成本和风险的级别后，可以根据风险分析的结果采取预防措施；

b)要害/关键控制法是用得较多的预防形式，它可以消除大部分的薄弱环节。

5.2.5.2 恢复方案

a)不采取任何措施，此方案应用于无需 IT 服务能独立运营的部门。

b)回退至手工（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。大部分的恢复计划都包括一些基于纸质的备份程序。

c)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。

d)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 IT 服务也能运作的企业。

e)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。

f)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。

g)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。

h)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。

i)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。

5.2.5.3 可用性管理员应根据上述恢复方式与实际情况编制《连续性计划》，连续性计划可以在服务实施方案统一体现，并不断完善。

5.2.6 连续性计划测试

a)项目经理组织连续性计划范围内的人员、设备等基础设施，编制测试计划进行测试。

b)根据 IT 服务项目需要，运维部门会同客户对《连续性计划测试报告》进行评审，记录测试存在的问题。

5.2.7 沟通和培训

a)连续性负责人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。

b)必要时编写《培训计划》，并对培训的效果进行评价。

5.2.8 组织和实施计划

a)组织架构安排。

b)实施规划：制定实施计划。

c)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。

d)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、系统等方面。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。

e)制定连续性管理计划：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。

f)设计计划实施程序：形成文档化的设计计划实施文档，保证实施人员可以直接按照流程文档实施恢复方案。

g)初始测试：在变更实施前进行初始化测试，保证连续性计划和程序的有效性。

5.2.9 连续性计划维护管理

a)对运维部的 IT 服务人员进行连续性方面的意识培养和实践操作，使他们将维护连续性作为常规的工作。

b)对可采用的连续性程序进行定期评审以确保经常性的更新和处于可用性状态。

c)每年至少应进行必要的连续性程序测试。

d)在评审和测试以后需要进行日常的变更管理，因此也需要确认连续性得到及时更新。

e)进行包括 IT 恢复人员和业务人员的培训，以保证在必要的时候他们有能力完成业务恢复工作。

f)保证连续性生命周期的最后程序得到技术中心和运维部门领导的确认，以 保证连续性流程的运营流程得到顺利的执行。

**6** **相关文件**

6.1《变更管理程序》

6.2《配置管理程序》

**7** **相关记录**

7.1 连续性管理过程形成的记录由运维部收集保存。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **编号** | **记录文件名称** | **编制部门** | **保存期** |
| **1** | **F733** | 《XX 信息系统连续性服务风险评估报告》 | 运维部 | 3 年 |
| **2** | **F734** | 《连续性计划》 | 运维部 | 3 年 |
| **3** | **F735** | 《连续性计划测试报告》 | 运维部 | 3 年 |

**8** **流程图**



