**文件编号：ITSS-06-09**

**版** **本：V1.0**

**北京星河千帆科技有限公司**

**服务可用性和连续性管理过程**

编制： 张龙超 日期： 2025.01.08

审核： 罗荣辉 日期： 2025.01.08

批准： 武太瑞 日期： 2025.01.08

**修订记录**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 日期 | 版本 | 变更说明 | 编写人 | 审核人 | 批准人 |
| 2025.01.08 | V1.0 | 新建文档 | 张龙超 | 罗荣辉 | 武太瑞 |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**目录**

目录

[**1** **目的** **4**](#bookmark1)

[**2** **范围** **4**](#bookmark2)

[**3** **术语** **4**](#bookmark3)

[**4.职责** **4**](#bookmark4)

[**5** **程序** **5**](#bookmark5)

[**5.1** **确定主要输入及来源：** **5**](#bookmark6)

[**5.2** **主要输出及去向形成** **5**](#bookmark7)

[**5.3** **控制的主要指标** **5**](#bookmark8)

[**5.4** **需求识别与分析** **5**](#bookmark9)

[*5.4.1* *可用性需求识别与分析* *5*](#bookmark10)

[*5.4.2* *持续性需求识别与分析* *6*](#bookmark11)

[*5.4.3* *需求识别时间：* *6*](#bookmark12)

[*5.4.4* *需求识别内容：* *6*](#bookmark13)

[**5.5** **可用性目标** **7**](#bookmark14)

[**5.6** **调查组件的可用性** **7**](#bookmark15)

[**5.7** **识别可用性风险和对策** **7**](#bookmark16)

[**5.8** **可用性设计** **7**](#bookmark17)

[*5.8.1.1* *可用性计划* *7*](#bookmark18)

[**5.9** **服务组件设计** **8**](#bookmark19)

[*5.9.1* *服务组件监控设计* *8*](#bookmark20)

[*5.9.2* *服务组件维护设计* *8*](#bookmark21)

[*5.9.3* *服务组建恢复设计* *8*](#bookmark22)

[**5.10** **可用性需求满足测试或评审** **9**](#bookmark23)

[**5.11** **可用性需求满足监控** **9**](#bookmark24)

[**5.12** **可用性报告** **9**](#bookmark25)

[**5.13** **定义持续性实施范围** **9**](#bookmark26)

[**5.14** **业务影响分析** **10**](#bookmark27)

[**5.15** **防止信息系统的业务中断** **10**](#bookmark28)

[**5.16** **潜在信息系统的业务中断分析** **10**](#bookmark29)

[**5.17** **信息系统的连续性业务测试** **11**](#bookmark30)

[**5.18** **信息系统的业务恢复性计划** **11**](#bookmark31)

[**5.19** **信息系统的业务连续性计划更新** **11**](#bookmark32)

[**5.20** **信息服务水平持续保持的持续计划制定** **11**](#bookmark33)

[**5.21** **保证服务水平的持续进行，组织并实施计划** **12**](#bookmark34)

[**5.22** **服务水平有效维护，持续性计划维护变更控制** **12**](#bookmark35)

[**6** **考核度量** **12**](#bookmark36)

[**7** **关联文件** **13**](#bookmark37)

[**8** **记录** **13**](#bookmark38)

1 目的

提供符合预定可用性级别且成本合理的IT服务， 以帮助企业实现其业务目标；确保已经取得的可用性级别能够得以评价和计量， 以及在必要时进行持续改进，特制定本程序。

规定了当发生重大信息安全事件或灾难时，为保护公司业务活动免受影响，迅速恢复已中断的业务活动，确保在所有情况下都可以实现向客户承诺的服务持续性，帮助客户服务在发生灾难之后尽快恢复客户服务和确保业务的持续运营,确保业务运作所需的客户基础架构和客户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持续性管理提供支持，实现公司业务持续发展而实施的管理活动，特制定本程序。

2 范围

本过程适用于本公司的服务业务的持续可用性及信息安全的业务持续性控制的持续管理。

所有新增IT服务以及服务承诺：

1) 公司维护的服务工作；

2) 涉及到的服务组件，如服务器、信息系统、网络设备、硬件设备等。

3 术语

3.1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有功能的能力，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。

3.2可用性管理：建立和维护可用性流程的信息系统及为达到此目的而根据特定需求所提供的服务。

4 职责

4.1 可用性管理员：负责可用性服务的具体实施，计划和报告的编制。

4.2 可用性负责人是可用性管理的关键角色，其职责有：

4.2.1定义、开发并管理可用性管理流程；

4.2.2确保IT服务在经过设计后，实际的服务重要性（一般、重要、紧急、重要紧急）能够符合约定的服务级别；

4.2.3制定可用性计划；

4.2.4撰写可用性报告,归并于IT服务报告中；

4.2.5提出优化IT基础架构的改进建议。

4.3 运维部门经理：

4.3.1 安排人员对 IT 服务的风险评估报告和可用性计划的编制；

4.3.2 根据服务承诺，提交 IT 服务报告给公司主管领导。

4.4 持续性管理负责人职责：

1）实施和维护客户服务的持续性管理流程。

2) 负责项目实施过程中设备及软件系统的故障处理及与之相关的作业中断的恢复。

3）负责系统设备及网络系统的故障处理及与之相关的作业中断的恢复。

4) 维护和改进《持续性计划》。

4.5 持续性负责人职责：

负责《持续性计划》和《持续性测试报告》的编制。

4.6 其他部署

4.6.1 负责部门相关系统的故障处理及与之相关的作业中断的恢复。

4.6.2 各部门在发生重大信息安全及服务事件或灾难时，负责保护本部门使用的信息系统及业务数据，及时恢复中断的业务活动，保证服务水平。

5 程序

5.1确定主要输入及来源：

|  |  |
| --- | --- |
| 输入 | 来源 |
| 服务级别需求 | 服务需求调研、服务级别协议 |
| 配置管理 | 系统的配置项，记录和报告配置。 |

5.2 主要输出及去向形成

|  |  |
| --- | --- |
| 输出 | 去向 |
| 风险评估报告 | 可用性负责人、部门经理。 |
| 可用性计划 | 可用性负责人、部门经理。 |
| 服务报告管理 | 服务报告过程中的主要步骤。 |
| 持续性计划 | 持续性负责人、运维部门经理 |
| 持续性测试报告 | 持续性负责人、运维部门经理 |

5.3 控制的主要指标

5.3.1 平均无故障时间（MTBF）。

5.3.2 平均系统事件间隔时间（MTBSI）表示的可用率（或不可用率）。

5.3.3 总体正常运作时间和宕机时间。

5.3.4 故障的次数。

5.3.5 平均修复时间（MTTR）。

5.4 需求识别与分析

5.4.1可用性需求识别与分析

可用性负责人根据服务级别需求识别和分析可用性需求，加入到《服务需求说明书》中，可用性需求分析包括：

1) 对各个系统维护服务的定义；

2) 各个系统对公司的重要性；

3) 各个系统所支持的可用性功能；

4) 系统故障时间或服务不可用状态造成的业务影响；

5) 故障停机时间或服务不可用状态产生的成本代价以及成本代价随时间推移相应变化的方式；

6) 所需服务小时数；

7) 较容易承受停机故障的次要服务时段；

8) 专为计划内维护与升级工作设定的停机时段；

9) 启动应急计划之前所能容许的故障停机时间。

5.4.2持续性需求识别与分析

持续性负责人及运维部经理根据服务合同和服务承诺、SLA识别持续性需求分析，持续性需求分析包括：

1)服务针对其所提供信息系统售后服务业务处理的定义；

2)服务对所在组织具备的重要性；

3)客户服务所支持的用户数量；

4)故障发生以后，如何保证业务持续性。

5.4.3 需求识别时间：

1) 在签订合同协议之前进行；

2) 需考虑新的IT服务和需求对现有服务做出的变更的方面；

3) 尽可能早的阶段确定运维的部门是否能够实现这些需求以及怎样实现这些需求。

5.4.4 需求识别内容：

1) 关键业务功能；

2) 可量化的可用性需求；

3) 非计划的IT服务中断对业务功能所产生的可量化的影响；

4) 客户的业务正常运作时段；

5) 有关定期维护约定的中断时间。

6) 重点关注支持关键业务流程的客户服务项目及关键业务功能。

7) 对具体的客户技术和服务需求提供支持

8) 可量化的持续性需求。

5.5 可用性目标

5.5.1 可用性管理负责根据可用性定义的结果确定可用性目标。识别可用性管理的服务对象和组件，并提供可用性目标。

5.6调查组件的可用性

5.6.1 可用性负责人调查服务组件的使用年限、性能、已发生故障情况等内容，并把调查的结果写入到《风险评估报告》中。

5.7 识别可用性风险和对策

5.7.1 可用性负责人员根据服务组件的调查情况识别组件的薄弱点、威胁及可能存在的风险隐患，编制《风险评估报告》。

5.8 可用性设计

5.8.1 可用性负责人员根据《风险评估报告》进行可用性管理的方案设计，设计的原则包括：

1) 确认那些影响系统运行和服务运行的薄弱环节。

2) 确认信息系统中具备可用性功能的部分。

3) 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。

4) 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。

5) 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。

6) 由于可用性设计而增加的成本，在设计完成后，需上报客户审核。

5.8.1.1 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)可用性计划包括运行监控、 日常维护和故障恢复方案等内容。

3)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、工具和技术等方面进行考虑。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。

4)可用性计划的计划周期应当覆盖1至2年，并且对于前6个月的计划应当提供更为详细的信息。

5)值得注意的是，可用性计划应当和能力计划和财务预算的周期保持一致。

6)可用性计划一般包括以下部分：

a)对目前状况可用性的评估；

b)改善现有服务活动的步骤；

c) 实施新服务与维护的一系列计划

5.9 服务组件设计

5.9.1 服务组件监控设计

所有IT组件都必须按照计划进行有关监控活动。有计划的监控活动可以：

1) 及时发现IT组件的健康状况。

2) 找出系统运行存在的薄弱点和风险隐患。

3) 针对发现的隐患，可及早制定相应的规避或处理方案。

5.9.2服务组件维护设计

1) 所有IT组件都必须按照计划进行有关维护活动。有计划的维护活动可以使IT支持部门能够：

a)实施预防性维护以避免故障的发生。

b)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。

c)根据业务需求对IT基础设施实施必要的变更。

d)激活IT基础设施中新增的功能。

2) 计划性维护活动涉及的首要问题是计划停机时间。

3) 在确定新增或改进后的IT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。

4) 在IT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。

5.9.3 服务组建恢复设计

1) 确保IT服务故障发生后，IT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) 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。

3) 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IT服务故障进行及时有效恢复的能力。

4) 设计恢复计划考虑因素：

A 确保业务与技术恢复流程是正确的。

B 清晰定义负责主要事件的员工的职责。

5) 安全性问题

A 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。

B 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。

C 与安全问题相关的活动主要有：

a)只有管理员、高级用户有权访问安全区域。

b)安全区主要包括：审批权限分配、人员新增、服务有效期时间调整。

5.10可用性需求满足测试或评审

1) 可用性管理负责人根据实施情况对《可用性计划》进行测试，可用性负责人、部门经理对提《可用性计划》进行评审，以确保实施计划的可行性。

5.11 可用性需求满足监控

1)对可用性需求满足进行有计划监控活动，可以能及时了解到需求能否正常运作，发现问题能及时找对应的方法纠正。

5.12可用性报告

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） 可用性报告可以包括下列指标：

a 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（MTBSI）表示的可用率（或不可用率）；

b 总体正常运作时间和宕机时间；

c 故障的次数；

d 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。

2) 形成能力报告，包括项目实施过程中，服务交付过程的主要步骤。

5.13定义持续性实施范围

1) 定义组织策略

- 有关系统运行和客户服务持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客户服务持续性管理的需求；

- 同时管理层也需要明确表达他们的承诺。

2) 识别应用客户持续性管理流程的相关领域

- 运用各种不同的风险评估方法来估计客户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；

- 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。

3) 分配资源

- 需要投入人力和物力建立一个客户服务持续性管理环境。

- 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。

5.14业务影响分析

1) 服务运行时间识别：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，没有客户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，需要评估服务和客户资源之间的依赖关系，灾难恢复服务所需要的额外资源。

4) 灾难扩散影响的层叠效应。

5.15防止信息系统的业务中断

5.15.1 运维部及各个部门定期进行数据备份，通信线路、电源、设备故障、潜在火灾等日常检查是预防公司业务中断的主要方式

5.15.2对应的控制措施：

监督

访问控制

身份认证

防病毒

过滤

入侵检测系统

5.16 潜在信息系统的业务中断分析

5.16.1运维部组织公司各个部门对信息安全风险评估后进行业务持续性和影响的分析内容包括如下：

a)对本部门的信息安全进行风险评估；

b)识别出对本部门业务持续性造成严重影响的主要事件，如设备故障、火灾、 电源中断可能性

等；

c)分析这些事件一旦发生对公司业务活动造成的影响和损失， 以及恢复业务所需费用等；

d)编写本部门业务持续性和影响分析报告，输入到业务联系性计划中

5.16.2“业务持续性和影响分析报告：应包括以下内容：

a)识别关键业务的管理过程；

b)可能引起公司业务活动中断的主要事件；

c)主要事件对本部门管理的信息系统的影响；

d)信息系统故障或中断对公司业务活动的影响；

e)关于系统恢复或替换的费用考虑。

5.17信息系统的连续性业务测试

5.17.1每年一次，运维部组织对《XXX关键业务恢复计划》进行测试，并对其保持或改进；

5.17.2场部负责对中断业务的事故做出迅速反应，并执行《信息安全事件管理程序》。

5.18信息系统的业务恢复性计划

5.18.1运维部负责执行《XXX关键业务恢复计划》或对应的记录，在规定的时间范围内恢复被中断的业务，使其正常运行。

5.19信息系统的业务连续性计划更新

5.19.1发生如下变化时

设备、人员、系统、运行策略，程序、位置，资源、立法、风险、承包方(第三方)、服务过程5.19.2当发生业务持续性间断，按照持续性业务管理方案执行。

5.20 信息服务水平持续保持的持续计划制定

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/关键控制法是用得多的预防形式，它可以消除大部分的薄弱环节。

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。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） 内没有客户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）-公司有不同的部门和多个分公司，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客户服务，这些组织通常是为多个客户服务的。

h)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。

5.21保证服务水平的持续进行，组织并实施计划

1) 组织架构安排。

2) 实施规划：制定实施计划。

3) 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。

4) 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。

5) 制定持续性管理计划：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。

6) 设计计划实施程序：形成文档化的时序行计划的实施文档，保证实施人员可以直接按照流程文档实施恢复方案。

7) 初始测试：在变更实施前进行初始化测试，保证持续性计划和程序的有效性。

5.22 服务水平有效维护，持续性计划维护变更控制

1) 对运维部，市场部的人员进行持续性方面的意识培养，使他们将维护持续性作为常规的工作。

2) 对可采用的持续性程序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持续性程序测试。

4) 评审和测试以后需要进行日常的变更管理，因此也需要持续性计划得到及时更新。

5) 进行包括研发人员，维护人员的培训， 以保证在必要的时候他们有能力完成业务恢复工作。

6) 保证持续性生命周期的最后程序得到部门经理，持续负责人和公司领导的确认， 以保证持续性流程的运营流程得到顺利的执行。

6 考核度量

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **指标度量项** | **指标要求** | **计算公式** | **频率** | **责任部门** |
| 系统可用率 | ≥98% | 系统可用的数量/系统总数× 100 % | 每季度 | 运维部 |

7 关联文件

7.1《服务报告管理过程》

7.2《配置管理过程》

7.2《服务报告管理过程》

8 记录

8.1 《可用性计划》

8.2 《可用性分析报告》

8.3 《连续性计划》

8.4 《连续性计划测试报告》