ITIL v3 核心读物 图解集

IT 服务连续性管理

ITIL v3 核心读物 图解集之
IT 服务连续性管理

1.0 图解概述

IT 服务连续性管理(IT Service Continuity Management)是确保灾难发生后有足够的技术和服务设施(如技术支持、操作系统、网络、数据仓库、应用程序)来保证业务在可接受的时间范围内重新运作，为业务部门提供 IT 服务的持续性。IT 服务连续性管理关注灾难恢复的需求分析、灾难恢复计划的制定和应急响应机制的建立等，主要是针对业务认为足够重要的、被看成是灾难的事件，其最终目的是支持整个业务连续性管理流程。IT 服务连续性管理的宗旨是在 IT 服务及其支持组件中维持必要的恢复能力。

设置和运行 IT 服务连续性管理流程，是采用生命周期的方法。IT 服务连续性管理的生命周期主要包括初始阶段、需求和战略、实施以及持续运营四个阶段，见图 1（ITIL 原书 *Service Design* 的 Figure4.21）。IT 服务连续性管理是贯彻该生命周期的一个循环过程，这可以确保 IT 服务连续性和恢复计划制定后，要与业务连续性计划和业务优先级保持一致。

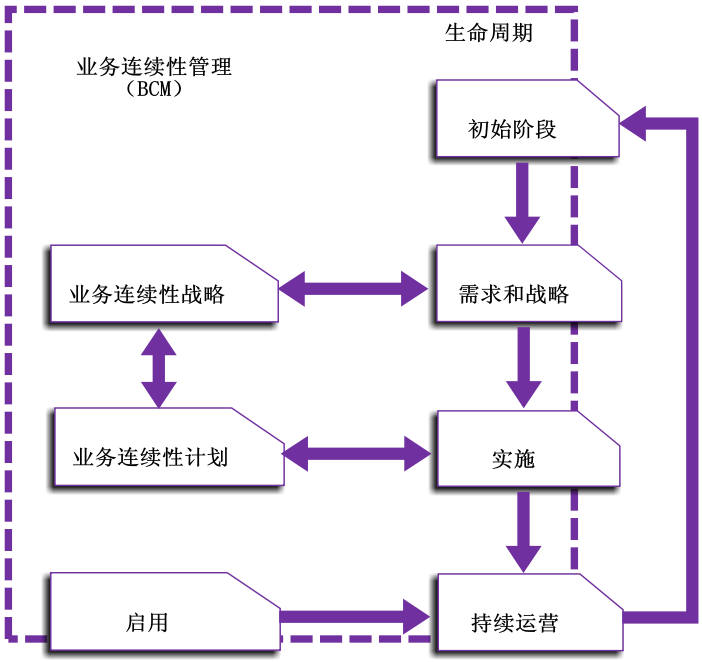

图 1 IT 服务连续性管理的生命周期

2.0 图解说明

下面详细说明 IT 服务连续性管理生命周期中的每个阶段所涉及到的活动以及方法和技巧。

2.1 阶段 1——初始阶段

初始阶段包括如下活动，这些活动是涉及到整个组织的：

- 设定策略：确定并传达策略，使组织中与业务连续性问题有关的所有人都意识到他们有责任执行和支持 IT 服务连续性管理。
- 指定参考条款和范围：主要包括定义组织内所有人员的范围和职责。
- 分配资源：主要指投入大量的资金和人力。
- 启动项目：IT 服务连续性管理和业务连续性管理作为一个复杂的项目来启动，包括定义项目组织及控制结构和达成项目计划和质量计划。

2.2 阶段 2——需求和战略

确定业务需求是 IT 服务连续性的一个重要的组成部分，决定组织是否能够从业务中断或灾难中幸存和所付出的成本。如果需求分析不正确，或者遗漏了重要的信息，可能会对 IT 服务连续性管理的高效运行机制产生重要影响。

需求和战略阶段可以细分为以下两个部分：

- 需求分析——进行业务影响分析和风险评估。
- 战略制定——支持业务的必要风险降低措施和系统恢复选择。

2.2.1 需求分析

1) 业务影响分析（BIA）

业务影响分析的目的是量化服务降低对业务产生的影响。业务影响分析识别对组织最重要的服务，并把这些信息作为战略的关键输入。

业务影响分析能识别以下内容：

- 损失的形式（例如：收入损失、额外成本、声誉损失、竞争优势丧失等）
- 服务中断时的损失情况以及问题随时间的扩散情况
- 支持关键业务流程的最低服务水平所需要的人员、技能、设备和服务
- 恢复最低水平或完全恢复的人员、设备和服务的时间
- 与业务恢复优先级相关的各种 IT 服务

业务影响分析得到的一个重要输出是制定出一张图，来反映由于失去业务流程或 IT 服务而导致的预期业务影响的随时间变化，如图 2（ITIL 原书 *Service Design* 的 Figure4.22）所示。

该图可用于帮助业务和 IT 服务连续性战略及计划的制定。图中的虚线以上部分的实线表示的是影响较早和较大的流程和服务，应对方法是需要采取更多的预防措施；而图中虚线以下部分的实线表示影响较小而发展时间较长的流程和服务，这应该是重点关注的，应对方法是采用连续性和恢复措施；图中虚线部分表示的流程和服务的应对方法，应该采用以上两种措施兼顾的方法。

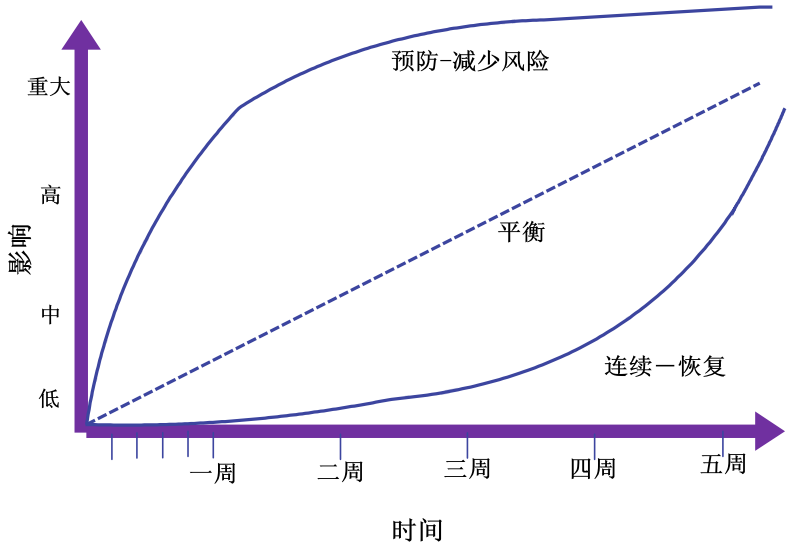

图 2 对业务影响的图示

2) 风险分析

灾难和其他服务中断实际发生的可能性是决定 IT 服务连续性管理的第二个驱动，这是对威胁的等级和承受风险的程度进行的评估，即风险分析。风险管理（M_o_R）常常用来在组织内部评估和管理风险。M_o_R 主要包括五个核心概念 :M_o_R 原则、M_o_R 方法、M_o_R 流程、内嵌和回顾 M_o_R、沟通。M_o_R 的框架见图 3（ITIL 原书 *Service Design* 的 Figure4.23）。

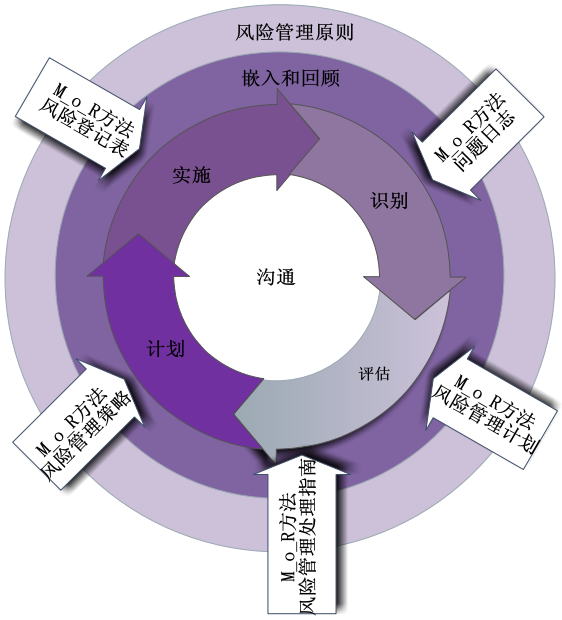

图 3 风险的管理——M_o_R 的框架

风险管理的流程主要包括以下四个步骤：

- **识别**：包含在活动中的机会和威胁，该活动能影响目标实现能力
- **评估**：了解与活动有关的机会和威胁的综合影响力
- **计划**：准备具体的管理响应来减少威胁，增大机会
- **实施**：监测已计划的风险管理行动及其影响，在响应不能达到预期时采取纠正措施

M_o_R 方法需要评估并开发风险预测，如图 4（ITIL 原书 *Service Design* 的 Figure4.24）所示，这是一个风险预测的示例，其中包括了“可接受风险”级别以外的许多风险，如“重大网络故障”、“服务器故障”等。按照风险分析，可以确定适当的风险响应或风险降低措施，从而来管理风险，即将风险降低到可以接受的水平或减轻风险。

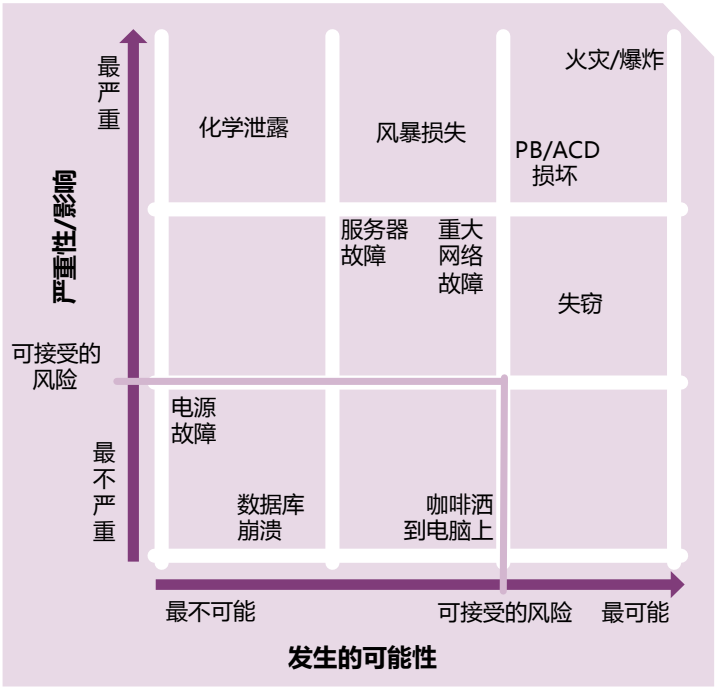

图 4 示例风险预测

在 IT 服务连续性管理环境中，是有许多风险需要考虑到的，下表是一个不完整的风险和威胁的清单的例子，如表 1（ITIL 原书 *Service Design* 的 Table 4.1）所示。

表 4.1 风险和威胁的示例

风险	威胁
失去内部 IT 系统或网络、PABX、ACD 等	火灾
	电力故障
	纵火和破坏
	洪水
	飞机碰撞
	天气灾难，如，飓风
	环境灾难
	恐怖袭击
	怠工

	灾难性故障 电气损坏，如，照明 意外损坏 劣质软件
失去外部 IT 系统或网络 ,例如电子商务服务器、密码系统	以上所有 对服务的需求过剩 拒绝服务攻击，如，针对互联网的防火墙 技术故障，例如密码系统
丢失数据	技术故障 人为错误 病毒，恶意软件，例如，攻击小程序
失去网络服务	网络服务提供商的设施损坏或拒绝访问 服务提供商的 IT 系统或网络失败 服务提供商的数据丢失 服务提供商的故障
关键的技术和支持人员不可用	罢工行动 拒绝访问设施 辞职 疾病/受伤 运输困难
服务提供商的故障，例如 IT 外包	商业失败，例如破产 拒绝获取设施 服务提供商的人员不可用 未能达到合同的服务级别

2.2.2 战略

业务影响分析和风险分析的结果能使业务和 IT 服务连续性战略符合业务需要。IT 服务连续性战略包含风险响应措施和恢复方案两个方面的内容。

1) 风险响应措施

大多数组织都需要在降低风险和采取补救措施之间取得平衡。采取风险降低措施时应该提倡联合可用性管理流程，因为其中一些措施可降低服务可用性因受影响而失效的概率。一般的风险降低措施，举例如下：

- 为计算机安装 UPS 和备用电源；
- 为关键应用安装容错系统，如银行系统；

- 为局域网服务器安装 RAID 阵列和磁盘镜像，以防数据丢失并确保数据连续可用性；
- 将服务外包给多家服务提供商；
- 全面的备份和恢复战略，包括异地存储。

2) 恢复方案

组织的 IT 服务连续性管理策略需要在降低风险措施所需要的成本和在可接受的时间表内支持关键业务流程恢复的恢复策略之间进行平衡。以下列出了在制定策略时需要考虑的 IT 恢复相关问题。

- 手工的变通解决办法：

对于一些特定类型的服务，在时间有限的条件下，采取手动的解决办法可以取得很好的效果。例如，服务台呼叫记录可以在短时间内通过使用电子表格的形式替换。

- 互惠协议

如建立协议以共享高速打印设备。在过去，互惠协定是典型的应急措施，但现在对多数类型的 IT 系统不再有效或不再具有可行性，不过仍可用于特定情况中。

- 逐步恢复

该方案有时被称为“冷备份”，这种恢复方案不适合要求快速恢复的服务。

- 中等恢复

该方案有时被称为“暖备份”。组织需要在预定的时间内恢复 IT 设施，以免影响业务流程时，选择次方案。而预定的恢复时间是在 BIA 阶段与业务部门商定的。

- 快速恢复

该方案有时被称为“热备份”，提供服务的快速恢复和复原。

- 立即恢复

该方案有时被称为“热备份”、“镜像”、“负载均衡”或“站点分离”，提供即时的服务恢复，没有服务损失。

IT 服务连续性战略很可能包括风险响应措施的组合及以上恢复方案的组合，如表 2（ITIL 原书 *Service Design* 的 Figure4.25）所示，该图显示了许多可以用于提供服务连续性的方案。如图，最初使用如一套表格来通过人工流程提供服务台工作的连续性， 同时在备用“快速恢复”地点完成服务的恢复计划，一旦备用地点恢复运行后，服务台就可以恢复工作并继续使用 IT 服务。但使用外部“快速恢复”备用地点很可能受时间限制，因此在此临时地点运行时，可以让“中级恢复地点”运行，并将长期的工作转移到此备用地点。

表 2 恢复方案示例

	人工	立即	快速	中级	逐步
服务台	是		是	是	是
大机报告表	是			是	是
财务系统			是		是
经销商系统		是		是	是

2.3 阶段 3——实施

在 IT 连续性战略得到认可后，应制定与业务持续性计划相一致的 IT 服务连续性计划，因此本阶段包含以下内容：

- **建立和实施业务连续性计划：**如紧急响应计划、危险评估计划、挽救计划、危机管理和公共关系计划、安全计划、安全计划、人力计划、沟通计划、财务和行政计划等；
- **基于灾难恢复流程的执行、协调和恢复计划；**
- **组织规划：**在灾难恢复过程中的组织架构必定不同于正常运营时的架构，灾难恢复过程中的组织架构主要围绕执行、协调、恢复三个方面开展；
- **进行必要的演练，**有四种常用的演练类型：排练演练、全面演练、局部演练、场景演练。

IT 服务连续性管理计划是一份关于灾难后恢复 IT 服务的完整计划，包含了恢复的所有细节，所要描述的情节细致到能够指导对系统完全不熟悉的人员进行灾难恢复。恢复计划应包括重要的恢复信息，

例如恢复时间点、相关的系统列表、系统之间的关联关系、系统数据之间的恢复点、软硬件的需求、配置信息，以及其他有关服务和系统的信息。在恢复行动中，需要检查恢复过程中的关键活动。例如在系统恢复到正常工作状态后，需要对系统连接、功能、数据一致性和完整性进行检查，其后再开始支持业务运行。

2.4 阶段 4——持续运营

持续运营由以下阶段组成

- 教育和培训
- 审查
- 演练
- 变更管理
- 启用

启用阶段是业务持续性和 IT 服务连续性管理计划的最后步骤。如果所有的准备工作都已经完成，计划已经制定并经过演练，那么启用业务持续性计划就是个简单的过程，但如果计划没有经过演练，就可能出现故障。

3.0 点评

连续性管理与可用性管理不能混为一谈，连续性管理所关注的是对业务产生严重影响的灾难性的服务中断。哪些服务中断的情况属于灾难，这是需要与业务的客户协商并得到他们的确认。当服务中断后，连续性管理将恢复到客户所能接受的最低服务级别。这个最低的级别同样需要预先和业务的客户之间确认。而可用性管理恢复是在服务中断后恢复到服务的正常的服务级别。可用性管理更多集中在应对那些每天均可能出现的常见，而罕见、重大或意外风险则由 IT 服务连续性管理加以应对。

连续性管理关注如下活动：与业务客户确认哪些服务中断是重大的灾难，进行风险分析、风险评估；制定连续性计划；计划何时触发、计划的参与人员和各自的职责；具体的应对措施与方案；连续性计划方案的测试演练等。

全球第一个业务连续性管理的框架标准 BS 25999 对 BCM 定义为："BCM 识别组织潜在威胁和运营这些威胁所产生影响的整体管理流程。如果潜在威胁变成现实，则可能导致损失，BCM 提供构建组织恢复的框架。这个框架具备有效应答能力而维护关键利益相关者利益、名誉、品牌和创造价值的活动。" 业务连续性计划是一套高级管理和规章流程，它使一个组织在突发事件面前能够迅速做出反应，以确保关键业务和功能持续进行，它的目的是确定并减少危险可能带来的损失，从而有效地保障业务的连续性。业务连续性计划包括高可用性、连续性操作和灾难恢复三个方面的内容，这三个部分内容相互关联相互交叉。IT 服务连续性管理是业务连续管理的重要组成部分，从概念上来说服务如果中断，优先恢复业务，其次恢复 IT 服务。

案例分享：

2010 年 4 月 1 日上午 9 点 10 分，某市医保信息系统出现了约 20 分钟的故障，这是该市近 5 年来最长一次性的医疗信息系统故障。所幸，该市各级医院大多经受住了 20 分钟的信息应急实战考验，就诊秩序仍属平稳。

该市医保局统计：3 月以来，医保交易量急剧增加，比以往的高峰增加了 1/3。以往的高峰是每天 100 万笔，本周以来，数字激增到 130 万笔—140 万笔。如同高速公路堵车一样，突然激增的数据堵塞了医保的信息系统，使得系统网络瞬间瘫痪。市医保局负责信息系统的某高级工程师表示：“发生故障后，我们立即启动了之前制定的 IT 应急预案，按照应急预案，各部门人员按部就班的执行应急流程，保障整个服务的连续性，并重新优化配置了信息资源，使系统尽快恢复。”

应急及时门诊总体稳定 20 分钟，让许多人急出一声冷汗，像大医院门诊办公室主任、医院信息中心的人员，都是最着急的人。“我们各个岗位的人都出来了，有拿喇叭解释的，有维持秩序的，有查原因的……不过幸好，之前 IT 部门就和我们讨论确认过这种事件一旦发生后如何处理，制定了应急预案，并做过相应的培训和演练，才得以保证我们病人看病没有受到特别大的影响。”某医院门诊办公室主任说。

该案例中，我们看到了一个活生生的由于 IT 网络故障而导致的业务灾难，这个灾难的影响是全市的病人不能刷医保卡看病从而导致可能的群体事件，而由于 IT 连续性计划制定得非常完善，业务方面通过手工记账付费、人工维持秩序等方式保持业务的连续性，而 IT 则根据 IT 连续性计划启动了备用系统来及时恢复系统，事后也进行了分析，并从业务、技术、政策多方面入手进行了全面优化。

4.0 术语解释

关键术语	解释
业务连续性管理(Business Continuity Management)	负责管理可能严重影响业务的风险的业务流程。BCM 可以保护主要利害干系人的利益、声誉、品牌和价值创造活动。BCM 流程包括将风险降低到可接受的水平，及在业务发生中断时，设法恢复业务流程。BCM 为 IT 服务连续性管理设定了目标、范围和要求。
业务连续性计划(Business Continuity Plan)	定义在业务中断后恢复业务流程所需步骤的计划。该计划还确定调用的触发、涉及的人员、沟通等。IT 服务连续性计划是业务连续性计划的重要部分。
IT 服务连续性管理(IT Service Continuity Management)	负责管理可能严重影响 IT 服务的风险的流程。通过将风险降低到可接受的水平，同时规划 IT 服务的恢复，ITSCM 确保 IT 服务提供商能够始终提供最低约定的服务级别。ITSCM 应该设计用来支持业务连续性管理。
IT 服务连续性计划（IT Service Continuity Plan)	定义恢复一项或多项 IT 服务所需步骤的计划。该计划还确定如何触发调用、涉及的人员、沟通等。IT 服务连续性计划应该是业务连续性计划的一部分。
业务影响分析(Business Impact Analysis)	BIA 是业务连续性管理中的活动，它确定了关键业务功能和它们的依赖关系。这些依赖关系可以包括供应商、人员、其他业务流程、IT 服务等。 BIA 定义了 IT 服务的恢复要求。这些要求包括恢复时间目标、恢复点目标和每项 IT 服务的最低服务级别目标。