IT 服务管理

基于ITIL®的全球最佳实践

（荷兰）Jan van Bon　主编

章斌　翻译

孙强　主审

清华大学出版社

CA 致意

Jan van Bon
IT Service Management, an introduction based on ITIL®
EISBN: 90-77212-28-0
Based on original Dutch edition IT Service Management, an introduction based on ITIL, Zaltbommel 2004, Published by Van Haren Publishing on behalf of ITSMF-NL.

依据原创荷兰语版的《IT服务管理——基于ITIL®的全球最佳实践》，Zaltbommel，荷兰 2004，由范哈仑出版社代表ITSMF-NL荷兰分会出版。

A coproduction of Van Haren Publishing, Zaltbommel, Netherlands
Tsing Hua University Press, Beijing, P.R.China

北京市版权局著作权合同登记号 图字：01-2005-5539

图书在版编目（CIP）数据

IT服务管理——基于ITIL®的全球最佳实践/（荷）博恩（Bon,J.V.）主编；章斌译. —北京：清华大学出版社，2006.1
书名原文：IT Service Management, an introduction based on ITIL®
ISBN 7-302-12080-3

Ⅰ.I… Ⅱ.①博…②章 … Ⅲ. 信息技术—高技术产业—商业服务—研究 Ⅳ.F49

中国版本图书馆 CIP 数据核字（2005）第 129267 号

出 版 者：清华大学出版社　　**地　　址**：北京清华大学学研大厦
http://www.tup.com.cn　　**邮　　编**：100084
社 总 机：010-62770175　　**客户服务**：010-62776969
组稿编辑：张立红（zlh-zlq@263.net）　　**文稿编辑**：崔伟（cuiwei80@163.com）
封面设计：鼎典智造（北京）企业策划公司　　**版式设计**：孔祥丰
印 刷 者：　　**装 订 者**：
发 行 者：新华书店总店北京发行所
开　　本：169×240　**印张**：20.5　**字数**：357 千字
版　　次：2006 年 1 月第 1 版　2006 年 1 月第 1 次印刷
书　　号：ISBN 7-302-12080-3/F•1384
印　　数：1～6000
定　　价：88.00 元

第 13 章

IT服务持续性管理

13.1 概述

许多经理都认为 IT 服务持续性管理是一种奢侈，为此他们不愿意花费任何资源。然而，统计资料表明许多具有破坏性的灾难实际上经常发生。

> 灾难——可以对一项服务或一个系统造成影响从而需要付出很大的努力来恢复初始绩效水平的事件。

“灾难”比“事件”要严重得多。它是一次业务中断。这意味着在一次灾难发生后，全部或部分业务不能正常运作。常见的灾难包括火灾、雷击、水灾、失窃以及暴力破坏等。此外，恐怖袭击也变得越来越常见。互联网也可能带来灾难，如能够中断整个组织的通信联系的“拒绝服务(DoS)”式攻击。有些公司本来是可以阻止此类严重问题发生的，前提是其考虑和制定了相关的业务持续性计划。业务运作越来越依赖于 IT 服务，这意味着服务失败的影响也越来越大和越来越不可接受。事实上，对很多公司来说，做业务就意味着使用 IT，离开 IT 他们几乎不能创造任何收入。因此，考虑如何保证业务运作的持续性是非常重要的。

传统的意外事件规划通常只是被 IT 部门用来免除其责任的一种形式。然而，如今 IT 已经越来越与业务运作的许多方面密切结合在一起。与传统的意外事件规划只是反应性的(在灾难发生之后该做什么)流程不同，新的 IT 服务持续性管理流程侧重于预防，即避免灾难的发生。

13.2　目标

IT 服务持续管理(IT Service Continuity Management)的目标是，通过确保在灾难发生之后 IT 基础设施和 IT 服务(包括相应的支持服务和服务台)能够在规定的时间内得以恢复从而支持总体的业务持续管理(BCM)。IT 服务持续性管理可能有多个不同的具体目标，但其范围必须基于业务目标而确定。在评估业务持续性所面临的风险时，需要确定这些风险是否处于 IT 服务持续性管理流程的范围之内。

效益

随着业务对 IT 服务的依赖程度逐渐加深，未能成功地规划业务及 IT 服务的持续性所导致的成本，以及规划所能取得的效益也只能通过风险分析才能确定。一旦业务运作面临的风险，而不仅仅是 IT 服务面临的风险被确定，就应当对制定预防措施和灾难应对措施进行投资。本章所提供的指南可用于控制和管理灾难所产生的影响。

如果灾难发生，建立了 IT 服务持续性管理的企业可以取得如下效益：

- 可以对恢复他们的系统进行管理；
- 减少了服务不可用的时间，从而为用户提供了更好的持续性；
- 可以最小化业务活动的中断。

13.3　流程

13.3.1　IT 服务持续性管理活动

IT 服务持续性管理主要负责：

- 评估在一次灾难发生后 IT 服务被中断的风险和影响；
- 确认需要制定额外的预防措施、对业务有关键性影响的服务；
- 确定服务恢复的时间限定；

- 采取措施来预防、检测和应对灾难的发生，从而减缓或减轻灾难的影响；
- 确定恢复服务的方法；
- 制定、测试和维持一个足够详细的恢复计划，从而保证能够承受灾难的发生并在规定的时间内恢复正常的服务运作。

由于作为总体的业务运作和 IT 结合得越来越紧密，因此 ITIL 对这两方面都进行了阐述：

- 业务持续性管理(BCM)通过风险分析和管理确保组织在任何时候都具备最低要求的生产能力和服务供应。业务持续性管理的目标在于将风险降低至可接受水平，并为恢复被灾难中断的业务活动制定恢复计划；
- IT 服务持续性管理(ITSCM)是应对影响 IT 服务运作的灾难并维护 IT 服务以支持业务的持续运作的流程。

IT 服务持续性管理是总体业务持续性计划的一部分，并依赖于业务持续性管理流程所提供的信息。IT 服务的可用性是通过风险降低措施(如安装可靠的系统)和恢复方案(如进行系统备份或准备备用系统)的结合使用来保障的。IT 服务持续性管理的成功实施需要整个组织的理解、支持和一贯的承诺。特别地，高级业务经理和董事们的明确支持对于 IT 服务持续性管理的有效性是非常关键的。

13.3.2 与其他流程的关系

IT 服务持续性管理与所有其他的 IT 服务管理流程都存在交互关系，特别是下列流程：

- 服务级别管理——提供有关 IT 服务职责的信息；
- 可用性管理——通过制定和实施预防措施支持 IT 服务持续性管理；
- 配置管理——定义基线配置和 IT 基础设施，为 IT 服务持续性管理提供灾难发生后哪些组件需要进行恢复以及恢复到什么状态方面的信息；
- 能力管理——确保业务需求可以得到适当的 IT 资源的充分支持；
- 变更管理——通过在所有影响预防措施和恢复计划的变更项目中引进 IT 服务持续性管理，从而确保所有的 IT 服务持续性计划是正确的和保持更新的。

13.4　活动

图 13-1 中显示了 IT 服务持续性管理的活动。图中的数字对应着本节所包括的 4 个小节，并将依次介绍这些活动。

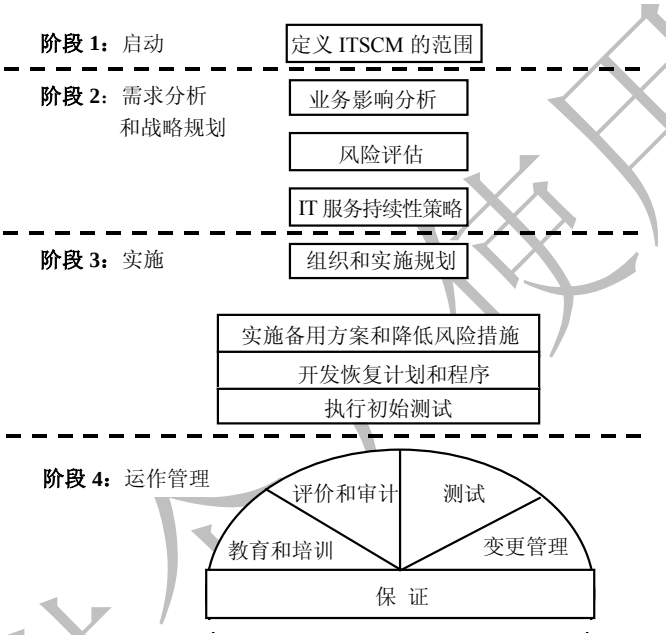

图 13-1　IT 服务持续性管理流程模型

（以 OGC 的业务持续性管理模型为基础，但主要针对 IT 服务的持续性管理）

13.4.1　确定 IT 服务持续性管理的范围

在发起 IT 服务持续性管理时，组织应当被作为一个整体加以考虑，并且应当进行以下活动：

- 确定政策——有关 IT 服务持续性管理的政策应当尽可能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。

- 确定范围和相关的领域——保险需求，如 ISO 9000 质量标准和 BS 7799 安全管理标准，以及总体的业务政策原则都需要被用来选择风险评估和业务影响分析(BIA)的方法。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。
- 分配资源——建立一个 IT 服务持续性管理环境需要投入大量的人力和物力。为了确保配备的人员能够实施 IT 服务持续性管理第二阶段的活动(需求分析和战略规划)，需要对他们进行培训。
- 建立项目小组——最好使用一种由管理软件支持的正式的项目管理方法，如 PRINCE2。

13.4.2 业务影响度分析

在分析 IT 服务之前，弄清公司在其业务持续性管理中包括 IT 服务持续性管理的原因，以及确定某个严重的服务中断的影响是非常明智的。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；而在其他情况下，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。大部分企业都需要在这两个极端之间选择某种平衡。

在业务持续性管理中包括 IT 服务持续性管理的可能原因包括：

- 确保业务流程的顺利运作；
- 防止发生违规事件；
- 快速恢复服务；
- 避免在竞争中被淘汰；
- 保住市场份额；
- 维持利润率；
- 维护在客户中的声誉。

或是上述多种原因的结合。比如在金融行业——如货币交——市场信息的丢失意味着企业将会由于交易(主要的业务流程)的中断而失去收益。如果法律要求使用一种指定的系统记录所有的交易活动，那么即使该系统发生中断交易也可以继续进行。不过这种法定要求迟早会遭到违反，而违反者也因此被施以罚款。在这两种情况下，公司都会失去客户和市场份额。

1. 服务分析

在弄清了发起 IT 服务持续性管理的原因之后，需要分析对业务（如信息系统、办公应用、会计应用、电子邮件等）具有关键性影响以及服务级别协议规定必须可用的 IT 服务。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。

2. 基础设施

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。可用性管理流程提供的信息可用来分析 IT 资源在支持前面所讨论的 IT 服务时可在多大程度上发挥关键性的作用。能力管理提供有关所需的能力方面的信息。进而确定从最初服务失败到全面恢复期间这些服务在多大程度上可能被中断是非常必要的。之后，这些信息可用来为每项服务制定恢复方案。

13.4.3　风险评估

这里没有有关灾难的官方统计数据，下面是一些著名的事件。

- **毒气**
  - 东京地铁，日本（1995 年 3 月）
- **电力中断**
  - 奥克兰，新西兰（1997 年 12 月）
- **地震**
  - 洛杉矶，美国（1994 年 1 月）
  - 神户，日本（1995 年 1 月）
- **恐怖袭击**
  - 世贸中心，纽约，美国（1993 年 2 月）
  - 伦敦，英国（1993 年 4 月）
  - 俄克拉荷马市，俄克拉荷马州，美国（1995 年 4 月）
  - 港口，伦敦，英国（1996 年 2 月）

- 曼彻斯特，英国(1996 年 6 月)
- 世贸中心，纽约，美国(2001 年 9 月)

- **洪水**
  - 孟加拉国(1996 年 7 月)
  - 巴基斯坦(1996 年 8 月)

风险分析可以帮助识别一个企业所面临的风险。这样的分析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。实施一个灾难恢复计划是比较昂贵的，因此应当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。

图 13-2 所示的模型显示了风险分析和风险管理之间的联系，该模型是基于 CCTA 的风险分析和管理方法(CRAMM)确定的。

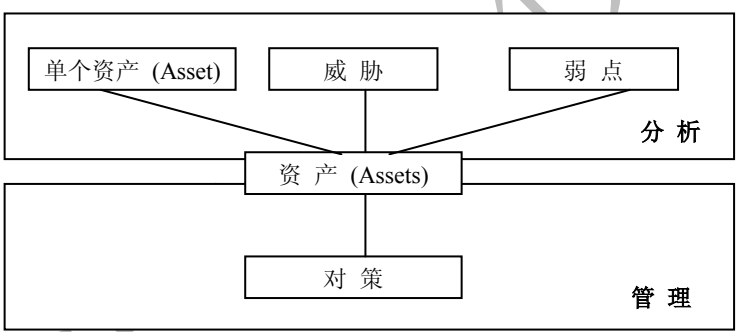

图 13-2 CCTA 风险评估模型

资料来源:OGC

该模型通过采用一种分阶段的方法可以支持有效的应急规划。

风险分析

首先，必须确认相关的 IT 组件(资产)，包括建筑物、系统和数据等。有效的资产确认要求有关每个组件的所有者和用途都必须文档化。

其次，要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)。例如，不稳定的电力供应和一个易于遭受风暴的地区这两个因素就存在较大的相关性。

接着，要确认这些资产的薄弱环节，并进行分类(高、中、低)。一个避雷

装置可以保护建筑物免受雷击的破坏，但雷击仍然可能严重地影响到网络和计算机系统。

最后，需要根据各 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。

在评估风险时应当考虑在第 1 个阶段已经定义好的 IT 服务持续性管理流程的范围。例如，对于一些小的问题可以由服务台和(或)事件管理流程来应付，或者由可用性管理措施来解决。有些业务风险则不属于 IT 服务持续性管理的范围。

13.4.4　服务持续性战略

大部分的企业都希望在风险降低和恢复规划方面达到某种平衡。风险降低措施、业务恢复行动以及 IT 恢复方案之间是有明显区别的。风险降低(预防)和恢复规划(恢复方案)之间的关系将在下面进行讨论。

威胁是不可能完全消除的，比如在大楼附近的一场火灾也可能烧毁您的大楼。此外，降低某一种风险又可能导致另一种风险的增加，如外包就可能增加安全方面的风险。

1. 预防措施

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。有些措施的目标是减小意外事件发生的概率或影响，因此也可以缩小恢复计划的范围。例如，可以针对灰尘、超高温或超低温、火灾、漏水、电力中断以及失窃制定预防措施，而将其他风险留给恢复计划来处理。

要害/关键控制法是用得最多的预防形式。它可以消除大部分的薄弱环节，例如通过建立自己的电力和水供应储备来应对电力和水供应方面的薄弱环节。但是，随着非现场恢复变得越来越困难，这种方法的应用也会带来其他诸如网络中断或网络拥塞等薄弱环节。要害/关键控制法可适用于大型的计算机中心，这些大型的计算机中心一般都太复杂，以至于不能通过恢复计划来解决。如今，增强要害/关键控制法的快速反应能力是至关重要的，即及时发现问题并在失控之前将其解决的能力。

2. 选择恢复方案

如果还存在部分没有被预防措施消除掉的残余风险，则应当将这部分风险交由恢复计划来处理。恢复方案应该提供下列措施来确保业务的持续性。

- 人员和场地——如何应对其他假定情况的发生，所需要的家具、运输和旅行的距离、以及支持业务所需要的关键人员；
- IT 系统和网络——恢复方案将在下文讨论；
- 支持服务——电力、水、电话、邮政和快递服务；
- 存档——文件、文档、纸质系统和参考资料；
- 第三方服务——例如电子邮箱和网络服务提供者。

下面列举了几种快速恢复 IT 服务的方案。

- **不作任何反应**——在这种方法下，很少有业务能够有效地运作。运用这种方法的目的是表明尚未查明情况。声明在没有 IT 恢复设施的情况下仍可以继续运作的部门可以给人以这种印象，即在他们的眼里，那些丧失的服务对该部门的业务运作提供的支持微乎其微，因而也是可有可无的。不过，在运用这种方案之前还是应该针对每项服务查明，这种方案是否是可以接受的，例如，作为一种短期的解决方案。
- **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，因为一般来说缺乏足够的具有使用传统系统经验的人员。而且，过去使用的基于纸质的系统也未必还有用，并且在短期内也很难对其进行改造。然而，纸质系统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。例如，为一个信用卡终端所制定的恢复方案可能是使用纸质信用卡单据。
- **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。采用这种方案时，两个公司必须达成一个协议并确保所有的变更都得到协调从而使双方的硬件环境都处于可互换的状态。能力管理应当确保储备的能力没有用于其他用途，或能够被快速地释放。然而，这种方案在如今的分布式计算机环境中并不是很有吸引力，因为在分布式环境下对独立处理能力和高可用性系统的需要越来越大，如 ATM 和在线银行等。

- **逐渐恢复（冷支持）**——这种方案适用于那些在一段时间内（如 72 小时）没有 IT 服务也能运作的企业。在这种方案下，可以安排在一间空的计算机房为企业提供约定的固定设备，或者将移动的计算机房运至企业所在的位置，为企业提供移动设备。该计算机房应当配备电力、空调、网络设施以及电话连接。该恢复方案可以在与外部供应商签订合同后实施。针对 IT 组件的供应商还应当另外签订协议以确保他们能够快速地送货。这种方案的优点在于，设备总是随时可用的。其效益和成本对于固定设备和移动设备是不同的，并且与下列问题相关：
  - **与设备的距离**——很少有提供商提供固定设备。这些设备可能是在远离故障现场的一个地方，这是一个在使用移动设备时可以避免的缺点。
  - **时间**——放置固定设备的场所一般只是在有限的一段时间内可用。
  - **时间延迟**——运送需要的计算机硬件可能要花费一些时间。
  - **网络**——通常难以提供恰当的网络设施。移动设备所需的网络连接可由大楼里用于原来正常运作的网络设施来提供。
- **中期恢复（暖支持）**——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。这种方案存在三种具体的方式。
  - **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。这种方案可以在最短的过渡时间内完成全面恢复。那些具有多个分布式系统的组织通常对这种方法进行一定的变动，即将所需的能力保存在每个系统中。这些备用的能力由能力管理进行监控（有点类似于互助协议安排式的恢复方案）。
  - **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。成本在这些客户之间进行分摊，并且依赖于所需要的硬件和软件以及约定的设备提供的时段（如 16 周）。这种安排通常用来作为建立一个冷支持设备所需时间内的一个过渡。这种方法一般也是比较昂贵的，设备一般都在比较远的位置。
  - **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。这辆拖车可作为一间计算机房并配备了空调等环境控制设施。IT 部门必须提供一个位置来停放该拖车，并且在离大楼一定

距离的指定位置提供电力供应、数据和通信连接等设施。这种方案的优点在于缩短了响应时间和企业现场的距离。这种方案只适用于有限的几种硬件平台。一些大的硬件供应商通过众多装备了标准化硬件配置的拖车来提供这种服务。按照约定的次数，如一年一次，拖车将到企业所在地测试有关的恢复安排。

- **立即恢复(热启动、热支持)**——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。这可以通过提供同样的运营环境、镜像有关的数据，甚至在可能的情况下复制生产流程来实现。这种方案需要可用性管理的紧密合作。
- **上述方案的组合**——有些情况下，应急计划可以提供一个更昂贵但时间更短的恢复方案来连接不作恢复和引进一个耗时较长但更便宜的方案之间的时差。例如，一个装载了运营性计算机中心(移动式热启动)可以提供一个临时性的解决方案直到移动设备建立起来和新的主机送到(移动式冷启动)。在大楼装修和新的主机运到大楼里后，正常的运作就可以恢复。

13.4.5 组织和实施规划

在确定了业务战略和选定了恢复方案之后，就可以开始实施 ITSCM，并为每个 IT 设施制定详细的恢复计划。为了实施 ITSCM，还必须成立一个专门的小组。这个小组包括针对每项服务的管理(危机经理)、协调和恢复团队。

最高管理层应当针对下列问题制定一个总体性计划：

- 紧急反应计划；
- 损害评估计划；
- 恢复计划；
- 关键记录计划(怎样管理数据，包括纸质的记录)；
- 危机管理和公共关系计划。

这些计划都是用来评估紧急事件并对它们作出反应的。在评估紧急事件后，需要决定是否启动业务恢复流程，同时需要决定下一个级别的计划是否需要被激活，包括：

- 场地和服务计划；
- 计算机系统和网络计划；

- 通讯计划(可访问度和连接)；
- 安全计划(数据的完整性和网络安全)；
- 人事计划；
- 财务和管理计划。

13.4.6　预防措施和恢复方案

这一节主要关于何时将早先时候已经制定的预防措施和恢复方案付诸实施。

为减小事故影响而制定的预防措施必须结合可用性管理而实施，主要包括：

- 使用 UPS 或其他备用电力供应；
- 容错系统；
- 异地存储和 RAID 系统等。

在这一阶段还应当开始考虑制定支持协议，协议应该涵盖的内容包括人员、建筑和电信服务等。即便是在紧急事件期间，也可以就恢复正常运作和订购新的 IT 组件签订有关的支持协议。甚至可以与外部供应商事先签订预防性合同，这意味着被预定的组件可以在需要时以约定的价格供应。在灾难发生时，供应商可以直接处理订单而无需发出报价单。这样的预防性协议应当每年更新一次，因为价格和具体的模式都会发生变化。在更新合同时应当考虑配置管理基线。

为制定支持协议应当实施下列活动：

- 与第三方供应商就异地存储设备进行谈判；
- 维护和装备恢复设施；
- 购买和安装支持硬件(预防性合同)；
- 管理预防性合同。

13.4.7　制定恢复计划和程序

恢复计划应当详细制定并处于正式的变更控制之下。恢复计划应当明确所有需要支持该计划的具体程序。这些问题需要通过计划传达至所有的参与人员和受影响的人员。一个典型的恢复规划问题与基础设施和约定的服务级别方面

的变更是相关的。例如，迁移至一个新的中等面积的房间意味着，在需要实施恢复时，在备用设施处没有相当的单元可用于外部暖支持。因为这个原因，配置管理在监控恢复计划中涉及的基线配置方面起到了重要的作用。

1. 恢复计划

恢复计划应当包括所有与恢复业务和 IT 服务相关的要素，包括：

- 导论——描述了计划的架构和拟使用的恢复设施；
- 更新——讨论维护该计划的程序和协商意见，以及跟踪基础设施中所发生的变更；
- 任务分配列表——恢复计划被划分成几个部分，每个部分介绍了将由某个特定的小组采取的行动。任务分配列表表明了每个部分应当分配给哪些人员；
- 恢复启动——说明在何时以及在何种条件下该恢复计划开始启动；
- 紧急事件归类——如果恢复计划针对不同的意外事件分别说明了恢复的程序，则在这里应该说明这些紧急事件的严重程度(小、中、大)、持续时间(天、周、几周)以及损害程度(小、有限、严重)；
- 专家部分——恢复计划应该根据下列六个方面以及计划所涉及的小组分成多个不同的部分。
  - 管理——怎样以及何时恢复计划将被启动，哪些经理和人员应当参与，以及控制中心设在哪里？
  - IT 基础设施——恢复系统需要提供的硬件、软件和电信设施；恢复程序；以及为购买新的 IT 组件而签订的预防性合同；
  - 人员——恢复设施需要配备的人员，如果该设施的位置离企业较远，还要考虑运输和场地问题；
  - 安全性——针对企业现场和异地支持场所制定的防火、防盗和防爆方面的指导，以及诸如仓库和保险库等外部存储设施的信息；
  - 恢复场所——有关合同、特定职责人员、安全性和运输等方面的信息；
  - 恢复——恢复正常情形的程序(如建筑物)，这些程序被触发的条件，以及预防性合同。

2. 程序

恢复计划为拟定具体的恢复程序提供了一个框架。制定有效的恢复程序是

非常关键的，有了集体的程序，任何人都可以按照程序的指示实施恢复。需要制定的程序包括：

- 安装和测试硬件和网络组件；
- 恢复应用系统、数据库和数据。

这些以及其他相关的程序应当附在恢复计划后面。

13.4.8　初始测试

对恢复计划、程序和相关的技术组件进行初始测试是 ITSCM 非常关键的一个方面。测试应当针对特定的情形实施并具有明确的目标和成功标准。在发生重大变更后还需要实施进一步测试，这类测试至少每年要进行一次。IT 部门负责测试恢复计划和程序中 IT 部分的有效性。这类测试可能是公开的也可能是非公开的，但邀请适当的业务经理参加将有助于促进相互了解，因而更有可能获得业务层的支持和承诺。

13.4.9　培训和意识培养

对 IT 和其他人员进行培训，以及对所有人员和组织进行意识培养对于成功地实施 IT 服务持续性管理是非常关键的。

IT 人员需要对业务恢复团队中的非 IT 人员进行培训，以确保他们熟悉所有的问题并在实施恢复期间能够提供支持。实际的应急设施，现场或异地的，都应当被包括在培训和测试的范围内。

13.4.10　评价和审查

计划应当定期评审和查验以确保它们总能反映最新的情况。这涉及 ITSCM 的所有方面。就 IT 方面而言，每当 IT 基础设施中发生了一次重大变更(如引入了新的系统、网络或服务提供者)后就应当进行一次这样的审查。

当业务战略或 IT 战略发生任何形式的变更时，也应当实施这样的审查。那些快速和频繁地发生变更的组织应当实施一个定期对 ITSCM 进行审验的计划。对计划和战略作任何形式的变更都必须在变更管理的指导下进行。

13.4.11 测试

恢复计划应当定期进行测试，这有点像一艘船上的紧急演习。如果在灾难发生时所有人都需要重新学习恢复计划，这就存在很多问题。通过测试，也可以识别计划中的弱点以及被我们忽略的变更。

13.4.12 变更管理

变更管理在保持所有的 IT 服务持续性管理计划的更新方面扮演了重要的角色，因为它确保了任何对恢复计划所作的变更的影响都得到明确的分析。

13.4.13 保证

保证意味着验证流程(程序和文档)及其输出成果的质量是否足以满足公司的业务需求。

13.5 流程控制

有效的流程控制取决于关键成功因素、管理报告和关键绩效指标。

13.5.1 关键成功因素和绩效指标

IT 服务持续性管理的成功依赖于：

- 有效的配置管理流程；
- 整个组织的支持和承诺；
- 最新的和有效的工具；
- 对流程中涉及的所有人员进行专门的培训；
- 对恢复计划进行定期测试。

绩效指标包括：

- 确认的恢复计划中的缺点的数量；
- 由于灾难所导致的收益减少。

- 流程的成本。

13.5.2　管理报告

在灾难发生后，必须提供一份有关灾难发生原因及影响，以及如何成功应付的报告。所有观察到的弱点都必须在改进计划中得到处理。

IT 服务持续管理流程所提供的管理报告还应当包括恢复计划测试的评价报告。这些报告被用来保证流程的质量。该流程还需要报告由于发生重大变更而导致恢复计划作出变更的数量。有关新出现的威胁也应当纳入报告范围。

13.5.3　职能和角色

IT 服务持续性经理的职责是实施和维护 ITSCM 流程，从而保证该流程任何时候都能满足业务持续性管理的需求。IT 服务持续性经理还需要在业务持续性管理中代表 IT 服务部门。

针对 IT 服务持续性管理流程，可以确定多个不同的角色及其相应的职责，并且在正常情况和发生危机的情况下其职责是不同的，如表 13-1。

表 13-1　一个 IT 服务持续性管理责任分配的例子

角　色	正常情况下的责任	紧急情况下的责任
董事会	● 启动业务持续性管理(BCM) ● 分配人力和资源 ● 指定政策 ● 确定流程负责人	● 危机管理 ● 作出公司范围内的/业务方面的决策
高层管理者	● 管理 IT 服务持续性管理流程 ● 接收计划和测试报告等 ● 沟通和保持有关人员的 IT 服务	● 协调和决策 ● 提供人员、资源和资金

	持续性方面的意识 ● 将 IT 服务持续性管理融入业务持续性管理中	
部门管理层	● 进行风险分析 ● 确定可交付物 ● 草拟合同 ● 对测试、评估和报告进行管理	● 启动恢复和持续性流程 ● 领导小组处理有关工作 ● 报告
小组经理和成员	● 开发可交付物 ● 就服务进行协商 ● 实施测试、开展评估和提供报告 ● 开发和执行有关规程	● 实施恢复计划

13.6 成本和可能产生的问题

13.6.1 成本

与引入 IT 服务持续性管理相关的主要成本包括：

- 发起、开发和实施 ITSCM 的时间和成本；
- 与引入风险管理有关的投资，如配备额外硬件的需求。如果可用性管理在设计新的配置时考虑了这些预防措施，这些成本就可以减少；
- 恢复安排的后续成本，如签订外部热支持合同的费用，测试安排的成本，以及恢复设施处于备用状态期间的费用等；
- IT 服务持续性管理的日常运作成本，如测试、审查以及更新计划的成本。

这些成本只有在比较了没有恢复计划时可能产生的相关成本，并且针对这两种选择进行充分的考虑后才能实际发生。尽管维持一个恢复计划的成本看起来很高，但这些成本相对于发生在火灾和失窃保险方面的总体支持来说还是相当合理的。并且，有效的 ITSCM 可以减少用于保险方面的成本。

13.6.2　可能产生的问题

在实施 IT 服务持续性管理流程时，需要考虑下列可能产生的问题：

- **资源**——组织应当为项目团队配备额外的能力来制定和测试恢复计划。
- **管理层承诺**——在组织的预算中应当包括用于 ITSCM 的年度成本，这需要获得高层管理的承诺；
- **获得恢复设施**——前面讨论的所有方案都需要对恢复设施进行定期测试。因而，任何恢复服务合同都应当让 IT 部门可以定期地获得这些恢复设施；
- **估计损害**——有些损害，如声誉的丧失，通过估计是很难进行量化的；
- **预算**——对昂贵的应急设施的需求通常都得不到理解，从而使得计划被搁浅；
- **得不到业务经理的支持**——这将导致不能开发有效的 ITSCM 流程，尽管客户认为已经作出了相关的安排；
- **无限期推迟**——由于 IT 服务持续性管理的全部或大部分流程还没有就绪，从而导致进度被频繁地延期。在这种情况下，当询问有关 ITSCM 的情况时，得到的回应将可能是“是的，我们正在开会讨论下周的安排……”，“我们正打算任命一个委员会来处理该问题”等。
- **失盲**(Black Boxing)——是指 IT 服务提供者已经放弃了责任，以及放弃了对 ITSCM 是否准备就绪的控制：“其他的人在处理这个问题”。因为组织为其 IT 系统和服务花费了一大笔钱，或者将其一部分运营工作外包给外部供应商了，管理层希望所花的钱能够确保他们的恢复能力，或者供应商已经制定了计划能够帮助他们在发生业务中断后迅速恢复。
- **IT 部门**——必须以业务的真实愿望和需求作为指导，而不是凭 IT 部门自身的主观假想行事。
- **熟悉业务**——通过识别关键性问题使业务支持 ITSCM 流程的开发是非常重要；
- **意识的缺乏**——整个组织都认识到 ITSCM 的价值是非常重要的。没有全体人员的意识到位和支持，IT 服务持续性管理流程是注定要失败的。