北京国家会计学院现代内部审计经典系列

BMIA

Brink's Modern Internal Auditing

中国内部审计协会 北京国家会计学院 联合推出

布林克现代内部审计学

第六版（下册）

【美】罗伯特·莫勒尔／著
Robert Moeller
李海风 刘霄仑等／译
王立彦／审校

中国时代经济出版社
China Modern Economic Publishing House
John Wiley & Sons, Ltd

北京国家会计学院现代内部审计经典系列

Brink's Modern Internal Auditing

中国内部审计协会 北京国家会计学院 联合推出

布林克现代内部审计学

第六版（下册）

【美】罗伯特·莫勒尔／著
Robert Moeller
李海风 刘霄仑等／译
王立彦／审校

中国时代经济出版社
China Modern Economic Publishing House
John Wiley & Sons, Ltd

著作权合同登记号　图字:01－2005－1832号

图书在版编目(CIP)数据

布林克现代内部审计学(第六版)/(美)莫勒尔著;李海风等译.—北京:中国时代经济出版社,2006.1

ISBN 7－80169－805－3

Ⅰ.布…　Ⅱ.①莫…　②.李…　Ⅲ.内部审计－研究　Ⅳ.F239.45

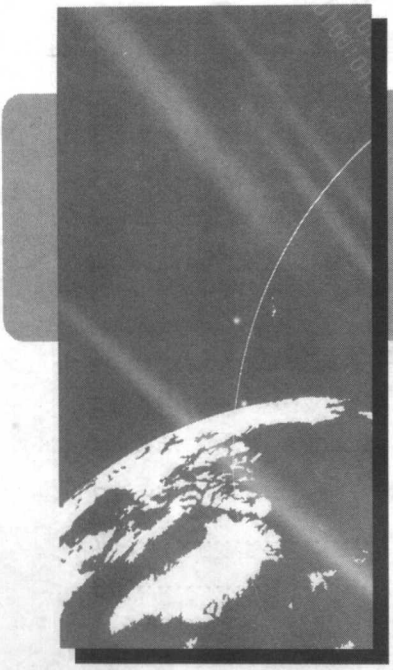
中国版本图书馆 CIP 数据核字(2005)第 115696 号

布林克现代内部审计学(第六版)

[美]罗伯特·莫勒尔　著

李海风　刘霄仑等　译

出 版 者	中国时代经济出版社
地　　址	北京东城区东四十条 24 号 青蓝大厦 11 层
邮政编码	100007
电　　话	(010)68320825(发行部) 68320517(编辑部)
传　　真	(010)68320634
发　　行	各地新华书店
印　　刷	北京市优美印刷有限责任公司
开　　本	787×1092　1/16
版　　次	2006 年 1 月第 1 版
印　　次	2006 年 1 月第 1 次印刷
印　　张	45
字　　数	910 千字
印　　数	1～4000 册
定　　价	86.00 元(上下册)
书　　号	ISBN 7－80169－805－3/F·372



目　录

第五部分　信息系统对内部审计的影响

第 18 章　业务持续性计划与灾难恢复计划 …… 1

18.1　信息系统持续性计划的重要性 …… 1

18.2　目前的业务持续性计划 …… 3

18.3　持续性计划和服务级别协议 …… 6

18.4　业务持续性计划的新技术:数据镜像技术…… 7

18.5　建立有效的持续性策略:我们保护的是什么 …… 10

18.6　建立灾难恢复业务持续性计划 …… 12

18.7　业务持续性计划的测试、维护和审计 …… 18

18.8　持续性计划的发展 …… 22

第 19 章　电子商务及网络环境中的一般控制 …… 23
19.1　信息系统一般控制的重要性 …… 23
19.2　大型机、旧式计算机系统元件及其控制 …… 25
19.3　客户/服务器系统和小型信息系统 …… 40

第 20 章　软件工程、软件能力成熟度模型与项目管理 …… 54
20.1　能力成熟度模型与项目管理 …… 54
20.2　能力成熟度模型 …… 55
20.3　审计、内部控制与能力成熟度模型 …… 67
20.4　信息系统项目管理 …… 67
20.5　项目管理与内部审计人员 …… 70

第 21 章　审核并评估应用控制 …… 72
21.1　信息系统应用程序内部控制的重要性 …… 72
21.2　信息系统应用程序的组成部分 …… 74
21.3　选择内部审计要审核的应用程序 …… 82
21.4　执行应用控制审核:初步工作 …… 83
21.5　完成信息系统应用控制审计 …… 90
21.6　大型机会计应用程序审核举例 …… 96
21.7　审核客户机/服务器预算编制应用程序举例 …… 99
21.8　对开发中的系统进行审计 …… 103
21.9　审核应用控制的重要性 …… 111

第 22 章　基础架构服务与支持交付控制 …… 113
22.1　信息系统基础架构的重要性 …… 113
22.2　信息技术基础架构库(ITIL)最佳实务模型 … 114
22.3　正确的信息技术基础架构库(ITIL)流程观 … 132
22.4　基础架构的 IT 人员支持 …… 133

第 23 章　计算机辅助审计技术 …… 134
23.1　计算机辅助审计技术的定义 …… 134
23.2　确定计算机辅助审计技术的需求 …… 137
23.3　计算机审计软件的类型 …… 140
23.4　建立有效计算机辅助审计技术(CAAT)的步骤 …… 157
23.5　计算机辅助审计技术(CAAT)对收集审计证据的重要性 …… 158

第六部分　内部审计工具与趋势

第 24 章　HIPAA 与日渐增长的隐私关注 …… 160
24.1　超越《萨班斯—奥克斯利法案》:日渐增长的隐私关注 …… 160
24.2　《革兰—利奇—贝利莱法案》(Gramm-Leach-Bliley ACT)法案 …… 161
24.3　《革兰—利奇—贝利莱法案》(GLBA)合规性审计 …… 166
24.4　《健康保险转移和责任法案》(HIPAA):医疗健康及其他 …… 167
24.5　其他立法提案:日渐增长的隐私关注 …… 175

第 25 章　持续性保障审计,XBRL 和 OLAP …… 176
25.1　什么是持续性保障审计 …… 176
25.2　执行持续性保障审计 …… 177
25.3　基于网络的扩展式标识语言:XBRL …… 184
25.4　数据仓库、数据挖掘与 OLAP …… 188

25.5 新兴技术、持续清算与《萨班斯—奥克斯利法案》 …… 193

第 26 章 内部审计质量保障与 ASQ 质量审计 …… 194
26.1 ASQ 审计标准:另一种方法 …… 194
26.2 质量审计员标准与实务 …… 195
26.3 质量审计员的角色 …… 197
26.4 质量审计员与 IIA 有关的内部审计师 …… 198
26.5 内部审计职能的质量保障复核 …… 199
26.6 启动内部审计质量保障复核 …… 205
26.7 质量保障审计的未来方向 …… 217

第 27 章 控制自我评估 …… 218
27.1 控制自我评估的重要性 …… 218
27.2 控制自我评估(CSA)模型 …… 219
27.3 启动控制自我评估(CSA)过程 …… 220
27.4 评价控制自我评估(CSA)结果 …… 225

第七部分 职业内部审计师

第 28 章 职业认证——CIA、CISA 及其他 …… 227
28.1 为何要寻求职业认证 …… 227
28.2 注册内部审计师考试 …… 228
28.3 IIA 发起的其他认证 …… 240
28.4 注册信息系统审计师考试 …… 245
28.5 信息系统审计与控制联合会(ISACA)的另一项认证 …… 248
28.6 注册欺诈核查师认证 …… 249

28.7　注册信息系统安全专家(CISSP)和信息系统安全认证 …… 250
28.8　ASQ质量审计认证 …… 250
28.9　有关内部审计人员的其他认证 …… 251
28.10　为何要取得这些认证 …… 252

第29章　ISO与内部审计全球标准 …… 253
29.1　一个不单单发生在美国的问题 …… 253
29.2　《萨班斯—奥克斯利法案》(SOA)的国际性要求 …… 254
29.3　国际会计和审计准则 …… 255
29.4　全球范围内的COSO框架:国际性内部控制框架 …… 261
29.5　ISO与标准认证程序 …… 264
29.6　ISO9001:2000内部审核 …… 269
29.7　另一种标准:ISO14000环境管理 …… 270

第30章　现代内部审计师的未来 …… 272
30.1　当前的内部审计职业 …… 272
30.2　不断演化的问题和趋势 …… 273
30.3　现代内部审计 …… 277

中英文词汇对照表 …… 278

第五部分 信息系统对内部审计的影响

18 业务持续性计划与灾难恢复计划

CHAPTER

内容提要

18.1 信息系统持续性计划的重要性
18.2 目前的业务持续性计划
18.3 持续性计划和服务级别协议
18.4 业务持续性计划的新技术:数据镜像技术
18.5 建立有效的持续性策略:我们保护的是什么
18.6 建立灾难恢复业务持续性计划
18.7 业务持续性计划的测试、维护和审计
18.8 持续性计划的发展

18.1 信息系统持续性计划的重要性

现在,组织若是没有自己的信息系统、通讯网络、数据仓库和技术人员,其业务将不能正常运行。为防止某些灾难发生时我们对当前版本只拥有有限的访问权限,组织针对计算机文件和程序,会在异地、安全的场所,有规律地建立程序来备份旧文件版本,并配备相关流程来恢复那些备份数据。早期备份程序是基于那些相对简单的系统配置,如今的大规模集成系统使得备份和恢复变得复杂得多。然而,

直到最近，许多组织还限制他们的信息系统备份程序，只备份关键文件。

最近几年，信息技术(IT)专业人士和内部审计师，对一个组织失去信息系统资源后会怎么样，产生了疑问。早期的信息系统资源通常是基于集中的数据中心，自20世纪80年代开始，改进的信息系统灾难恢复计划和备份程序策略回答了这些担心，它们通常包括远程灾难恢复数据处理场所的安排。关键的备份文件和程序在异地存储，且要求IT人员在灾难事件发生时转移到备用场所。专业人员考虑的信息系统灾难有火灾、洪水及其坏天气等情况。在早期的大型机时代，组织甚至采用目前认为较为怪诞的行为来开发他们的IT灾难恢复计划，其中包括与拥有相似的IT资源的邻近组织签署互惠协议，从而当一方发生紧急事件后，可转移到另一方进行处理。有的组织则在它们的某个设施中修建活动地板以提供临时空间，并与计算机系统硬件和网络提供商签署协议，以便在发生紧急事件时，能快速地搬入替代系统。现在发生紧急事件时，计算机硬件厂商仍将同意更换设备。事实上，由于在过去计算机设备普遍采用定制生产，而现在通常都是现货供应，因此更换设备已容易了许多。两个首席信息执行官之间的互惠协议在理论上听起来不错，但是作用往往局限于低层面，很少能真正超越，多数是出于人道主义的帮助。那个邻近的互惠协议站点可能由于相同的天气灾难而无法运作，或很可能不会关注要在工作时段运行系统的其他人。最终障碍是，组织的法律顾问将提出一打理由来拒绝互惠协议。

20世纪80年代和90年代早期的那些灾难恢复计划并不健全，此时出现了一批专业灾难恢复厂商，他们拥有配备齐全并处于空闲操作状态的计算机系统站点，或称作“热站”。组织签署合同在灾难发生时使用这些站点，定期进行测试，并将重要的备份文件存储在该站点或其他安全站点上。尽管技术变更对这些灾难恢复操作产生了一些挑战，这些专业的“热站”备份厂商仍为许多组织进入21世纪提供了初级IT备份方案。

2001年9月11日，通常被称为“9.11”，改变了所有一切。两名恐怖分子驾驶大型客机撞向纽约世贸中心大厦，该建筑轰然倒塌，除了造成许多生命和财产的损失，该事件也触发了组织的IT灾难恢复计划。世贸中心有很多以IT系统为基础的金融机构，实际上许多组织都有某种形式的灾难恢复计划，但事后证明这些计划都名存实亡。灾难的即时后果是，电话线路被阻塞，进出曼哈顿的桥梁及航空公司被关闭。许多IT灾难恢复计划(DRP)不能工作，只有很少一部分组织的DRP发挥了作用。

本章讨论建立一套有效的IT持续性计划和灾难恢复计划的步骤及内部审计师从“9.11”事件中学到了什么。本章的重点在于业务恢复而不仅仅是IT系统与操作的恢复。在过去的几年中，内部审计仅是少数几个关注组织灾难恢复的组织职能之一，而现在它已经成为组织内部控制基础的重要方面。有效的信息系统持续

性程序逐渐成为美国联邦法规要求的一部分，同时，各级管理者应认识到对有效的信息系统恢复的需求。与组织中的其他职能部门一起，内部审计师在检查、测试和评估组织的持续性计划时扮演了重要的角色。

18.2 目前的业务持续性计划

目前，一个组织的信息系统资产面临很多的风险。通常不是一个主要的或中央计算机设备来处理的自动应用系统，而是由大量桌面设备，服务器及其他通过复杂通讯系统、存储管理网络和因特网连接而成的计算机系统组成。组织并未使它们所有的信息系统资源连接到一个或几个中央数据中心，且管理者更关注如何保持信息系统正常运行，而不担心丢失中央计算机系统设备的风险。20 世纪 70 年代，信息系统灾难恢复的概念是指如果一些单个的灾难使计算机中心不能正常运行，则启动相应的程序恢复操作。

IT 灾难恢复计划(DRP)语言和战略方式发生了改变。虽然我们不否认“9.11”事件是一个巨大的灾难，但目前的专业人员考虑更多的是 BCP，用于恢复整个业务运作需要的计划和流程。一个在线订单系统的用户所关心的并不是服务器是否运行，而是通过因特网提交的客户订单能否被正确有效地处理。信息系统应该尽可能快速并有效地恢复和运行，但更为重要的目标是要支持和恢复业务流程。

除了关心灾难发生时恢复运行，目前的组织也应关心 IT 资源的持续性和可用性。任何形式的计算机系统中断对一组织来说都可能带来巨大损失。例如，灾难恢复协会[①]估计如果机票预定系统中断，平均每小时造成的损失将是 89,500 美元；如果信用卡系统中断，平均每小时造成的损失将是 260 万美元。实际造成的损失远远超出这些估计值。1999 年 8 月，eBay 国际拍卖网站中断了 22 小时，导致 400 万美元的直接损失和价值 50 亿美元的市场份额[②] 丢失。这些信息表明高的系统可用性对一个组织来说非常重要，因此，内部审计师应该不断寻找能实施 BCP 及提高信息系统可用性的领域。

① 国际灾难恢复协会：www.dri.org.

② “福布斯”网站有关技术的内容，2004 年 3 月 29 日。

(a) 紧急事件响应计划

在原有的IT持续性计划基础上,通过扩展项目建立起了恢复计划后,这些资料常常装订为厚厚的一本书,摆上了少数几位管理层的办公桌。大家的想法是当紧急事件发生时,人们可以拿出灾难恢复手册,然后像查找电话号码一样在备份站点找到重要的数据,以报告该紧急事件或获取处理紧急事件的程序。如果手册能经常保持更新,并且紧急事件允许先查阅计划再实施的话,这些恢复计划在理论上是可以起作用的。然而,许多紧急事件是突发性灾难,没有时间翻阅灾难恢复计划,掌握相关知识。例如,当建筑物发生火灾时,人类的本能是尽可能快地逃离建筑物,而不是花时间研究恢复计划上的疏散指导策略。组织应事先考虑到这些各种可能的情况,他们需要紧急事件响应计划。

重要的紧急事件可分为两种。第一种是建筑物失火型紧急事件。良好的紧急事件响应计划应包括标明安全出口并经常进行消防训练。该类型的紧急事件响应计划应覆盖组织的所有部门,而不仅仅是信息系统部门,并定期进行测试。然而,第二种紧急事件响应计划包括特殊的个别事件,它可能是重要的也可能是不重要的,但是在调查和改正行动计划之后,必须马上改正,以避免更多的事件发生。这些被称为紧急事件,经常包括安全漏洞或软硬件的失窃。一个好的紧急事件响应计划重点应关注快速响应时间,以减少事件影响的进一步扩大,降低任何副作用的影响。

紧急事件响应计划可分为4部分:

1.即时响应活动。无论是安全漏洞,设备失窃或物理入侵,都应有已分配的资源来调查事件并立即采取改正行动。

2.事件调查。应深入调查所有报告的事件,确定引发紧急事件的根源以及将来可能采取的改正措施。

3.改正或修复。资源应能按需进行改正或恢复操作。由于紧急事件可能覆盖很多的领域,这些资源应包括信息系统安全专业人员,建筑安全管理人员或其他。

4.紧急事件报告。整个紧急事件和接下来采取的纠正措施要进行记录,记录还应包括对经验教训的分析和所有纠正措施的下一步计划。

紧急事件响应必须果断和快速执行,就像我们应该在火刚刚燃起来就浇灭它那样,而不是建立短期策略来阻止它烧得更旺。许多情况下,需要快速做出反应,不要给错误留下任何扩大的空间。通过开展火灾演习并测量响应时间,有可能开发出一种能提高速度和精度的方法。迅速响应可以减少资源的不可用造成的影响及任何系统和设备损坏带来的潜在损失。一个组织可能面对许多突发事件或其他

威胁,除了"9.11"类型的事件或计算机系统资源的完全损坏外,应一直关注更多的持续性计划问题,组织应建立一种机制来对任何不定期出现的紧急事件做出反应。

内部审计师应寻找合适的紧急事件响应计划作为内部审计检查的组成部分。这个计划可能针对整个组织设施,像火灾逃离计划,或针对个别情况,像安全漏洞响应计划。在组织的许多领域中,审计师应询问合适的紧急事件响应计划是否到位,是否定期更新,是否是最新的并且是否已经测试过。

(b) 业务持续性计划(BCP)

业务持续性计划(BCP)可以帮助组织从主要服务中断(如火灾、计算机设备或网络设备错误、或其他形式的主要中断)中恢复所需的步骤。BCP 的目标是帮助组织减少灾难损失或使服务中断的影响达到组织能接受的水平,并使业务持续运行。BCP 的重点与 IT 专业人员称之为灾难恢复计划(DRP)的重点不同。DRP 关注的是数据处理程序的持续运行,而 BCP 关注的是业务单元的恢复。

这里列出了建立 BCP 所需的步骤。尽管信息系统组织已经拥有 DRP,但那些旧的方法常常无法有效恢复关键业务流程。就像规划和执行内部审计需要关键步骤一样,建立有效的 BCP 也需要一些关键步骤。一些专业组织,如位于美国的灾难恢复研究所和位于英格兰的伦敦业务连续性研究所采用了一组 10 个被认为常用的 BCP 最佳实践,如表 18.1 所示。这些实践已成为 BCP 的关键步骤或组件的标准,并被广泛接受,接下来的部分将详细讨论这些内容。一个有效的 BCP 对组织来说是至关重要的,管理者应确保整个运营的顺利进行,以满足客户和服务接收者的需求。许多公司和政府组织必须依法开发这些持续性和可能性计划。其他一些情况下,法规则有效地对 BCP 进行间接要求。如《萨班斯—奥克斯利法案》(SOA)的第 409 条款,就要求在纽约证券交易所备案的上市公司以合适的方式报告他们的财务结果。系统失败并不是借口,一个有效的 BCP 计划将能帮助组织预防这些风险。

表 18.1 BCP 推荐的专业实践

以下推荐的实践或步骤最初是由灾难恢复协会开发的:
1. **项目启动与管理。**应通过正式的项目管理流程,在协议的时间和预算限制内管理 BCP 流程。
2. **风险评估与控制。**应使用正式的 BCP 风险评估流程,来确定可能对组织及其设施产生不利影响的事件以及重大灾难、这些事件可能引起的破坏,以及要预防和减少潜在的损失所需的控制方法。该过程应包括成本—效益分析来证明这些控制的确降低了风险。
3. **业务影响分析。**管理者应了解影响组织的灾难性事件给组织带来的全部影响,以及那些可用于确定并量化它们的技术。需要识别关键职能、恢复优先级和相互依存关系,才能设置恢复时间目标。

4. **制定业务持续性策略。**单一的 BCP 并不适用于所有环境，管理层应制定适当的策略来决定和引导选择业务恢复策略，以便在目标恢复时间内完成业务和信息资源的恢复，同时保证组织的关键职能尽快恢复运行。
5. **应急响应和处理。**应急程序应在事件发生后及时对情况做出响应并防止其影响进一步扩大，其中包括建立和管理应急处理中心作为紧急事件发生时的指挥中心。
6. **开发和实施 BCP。**应使用一种规范的、基于最佳实践的流程开发、记录并实施 BCP，以保证业务在设定的目标恢复时间内得以恢复。
7. **认知与培训项目。**通过有效地运用培训项目，使组织的所有适当成员认识到恰当的 BCP 程序在发挥作用。
8. **维护和演练 BCP。**应对 BCP 及其重要组成部分进行定期测试并更新。实施相应的流程维护和更新 BCP 以符合组织的战略发展方向。
9. **公共关系和危机协作。**建立到位的与持续性事件相关的所有事件的沟通流程，并适时地与职员及其家庭、重要客户、重要供应商、所有者/股东和合作管理进行交流，并为他们提供咨询。应及时将必要信息告知所有股东。
10. **与权威机构的协调。**与当地权威机构就业务持续性及恢复活动建立有效的协调机制，确保符合适用的法律法规。

来源：罗伯特·R·莫勒尔，《萨班斯—奥克斯利法案》与内部审计新规则，版权：2004，约翰·威利出版公司。经允许使用。

18.3 持续性计划和服务级别协议

信息系统部门不能只是武断地对所有的业务程序和应用领域建立一系列 BCP 指南。它必须包括用户和应用系统拥有者的参与，以确保满足期望值和服务价值的实现。如果一个用户部门的高级经理感觉到对于关键交易必须始终具备完全备份的能力，则这个部门应与信息系统部门协商来提高持续服务的级别，同时，必须了解提供持续服务能力所必需的额外的软件和硬件成本。在过去，下载的磁带副本需要运送到备份地，实时备份还只是一个理论观点。一笔交易必须先在主要系统和它的数据库系统里记录，然后再复制到备份设备中。无论是每周或每日备份文件还是实时系统备份的方法，都可能会出现延迟。较新的存储管理方式可以提供立即备份，这种方式称为镜像。以下将介绍这些技术。它们很有效当然也更昂贵。

业务持续性计划的细节部分必须按下列方法来进行，关键用户部门应该通过签署正式的服务级别协议(SLAs)来协调它们的恢复目标。服务级别协议是业务流

程的拥有者和IT服务的提供者就具体恢复目标签署的合同，也是业务持续性活动的基础，第22章中的“基础架构服务—支持—交付控制”部分将其作为信息技术基础架构库（ITIL）服务交付最佳实践的一部分加以详细讨论。服务级别协议可用于定义计算机系统备份和恢复所期望的最低级别，作为信息系统和关键用户之间的合同，规定日常操作及服务中断时应采取的恢复行动。服务级别协议描述了期望和承诺的服务持续性级别，它是建立有效持续性计划的基础。

当供应商对外提供服务时，签署合同就要考虑服务级别协议。例如，一个计算机服务提供商承诺以每个交易X美分的价格提供一些应用服务，并在规定的周转时间内处理相关交易。组织就要为这项服务支付费用，如果没有在预期的周转时间内完成，组织就要认识到需要做出调整。组织中用户部门和信息系统部门也应签署类似的服务级别协议，但内部成本通常基于内部预算账户。对于和业务持续性计划相关的服务级别协议来说，业务部门应制定具体的备份要求，并承担与信息系统及其服务相关的费用。假如预期的服务级别协议目标没有实现，将产生一个预算贷项。尽管服务级别协议借贷双方通常基于内部的“虚拟货币”，但这可以成为管理绩效评价的重要指标。

业务恢复服务级别协议的构建即使没有涵盖组织中的所有部门，也涉及了大多数部门。这当中也包括信息系统部门承诺提供双方商定级别的持续服务。当业务部门有特殊需求时，将制定具体的服务级别协议。在审核持续性计划和组织的业务持续性计划时，内部审计人员应了解服务级别协议的重要性，这种类型的合同规定了适当的规则和期望目标。

18.4 业务持续性计划的新技术：数据镜像技术

当检查系统控制和应用控制时，内部审计师经常需要评估是否对关键文件进行定期备份。然而，在当前的实时交易系统中，许多将关键交易备份到磁盘或磁带的备份程序并不能发挥有效作用。即使对文件或数据进行每周、每天甚至每小时的完全备份，并捕获临时交易数据流，相对于不断更新的应用来说仍然收效甚微。当一些系统由于意外事件而停止时，有必要返回到最近的数据库备份中，作为新的基准线或起点，重新处理自最后一次备份以来进行的交易。然而，当业务流程非常复杂庞大时，比如有大量的交易和订单处理，几乎不可能在不关闭现行应用系统的

情况下，重新处理以前的交易，飞机机票和排程系统就是一个例子。为了组织生存，系统必须实时操作，且保持高可用性。对一个组织来讲强调可用性接近100%或99.99%，才能实现每年中断少于1小时。表18.2列出了一些可用性的百分比，许多现代组织正在努力使自己以及利益相关者都做到接近100%可用性。

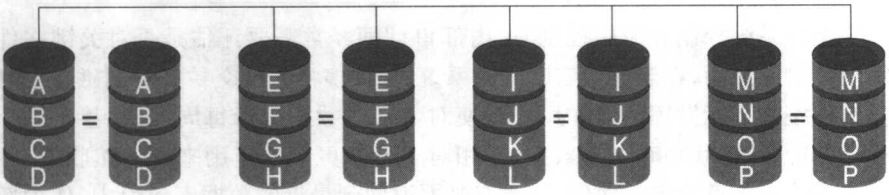
表18.2 高可用性百分比

可用性	9的数字	预计死机时间
99%	2个9	每年87小时
99.9%	3个9	每年8小时
99.99%	4个9	每年52分钟
99.999%	5个9	每年5分钟
99.9999%	6个9	每年不到1分钟

现在，与业务持续性计划相关的法律法规规定，组织应保持高可用性，组织应该转移并复制自身的数据，以便发生数据丢失、数据破坏或灾难时能迅速恢复关键的业务操作。幸运的是，近些年已涌现出许多新技术，能快速、定期进行备份。一种被称为冗余磁盘阵列(RAID)的技术，经常用在将数据同时储存在不同地点的一个或者多个磁盘文件中，以创建冗余。表18.3使用RAID 1配置解释了此概念。从RAID概念的提出到现在，已经发展出很多种类，如RAID 0、1、2、3等。本章的目的不是对RAID的内容做详细介绍，但为了介绍此内容，我们将其统称为镜像。内部审计师不需要详细了解这些技术，但应具备相应的知识提出一些合适的问题作为检查的一部分。

表18.3 RAID 1数据镜像技术

所有数据分布在某个磁盘中上，A到P通过多个磁盘镜像达到100%冗余。



来源：罗伯特·R·莫勒尔，《萨班斯—奥克利斯法案》与内部审计新规则，版权：2004，约翰·威利出版公司。经允许使用。

冗余磁盘阵列(RAID)技术提供了100%的应用数据冗余校验,因此当磁盘有误时不必重建磁盘文件架构。在使用Microsoft XP操作系统的桌面计算机上,我们会遇到基础级别的RAID,如果电源出现故障或类似事情发生时,磁盘文件的可恢复版本就会保留下来。当整个磁盘被"碰撞"的情况下,这种技术可提供最有效的备份级别,恢复桌面计算机系统。

RAID技术允许数据中心使用许多磁盘同步来恢复"碰撞"型损坏。当交易数据通过广域网(WAN)镜像到异地时,这项技术尤其有价值。管理多个磁盘、多个地域的备份与恢复实际上是存储厂商提供的一套软硬件解决方案。市场上一些厂商推出了有效的存储管理产品,我们这里举个例子,"EMC公司的SRDF解决方案"①。SRDF中的字母S代表EMC的Symmetrix高速多磁盘存储设备。一个厨房冰箱大小的设备可连接许多单个磁盘驱动器,拥有储存万亿字节数据的能力。SRDF是一个镜像储存设备,允许在两个独立的Symmetrix系统之间,通过公共网络或私有网络快速、实时地传送数据。"镜像"顾名思义,如果我们在桌子上放两杯水,以45度的角度去看,我们将马上看到我的两个像,数据镜像能达到同样的效果。按回车键进行计算机处理,就能立即将一个数据写入两个或更多的镜像储存设备中。

在表18.4描述了这类配置。计算机系统对所有交易进行的常规处理都使用Symmetrix储存设备,这些交易存储在初级存储设备中,同时通过高速线路镜像到另一储存系统中。这需要两个冗余的系统。这种镜像操作产生了具有相同数据配置的多个复制版本,以便紧急事件发生时,能迅速且容易地进行恢复。之所以重点介绍这种产品,是因为在"9.11"世贸中心恐怖袭击中,它表现出比其他竞争对手更为优异的性能。当那两栋建筑倒塌时,计算机系统基本上没有数据丢失。当恢复人员能够到达远程站点重新运作业务时,基本上没有数据损失。

本书几次提到的存储管理系统在不断更新。正确使用存储管理系统,将大大改善信息系统的可靠性和备份能力。专注于研究信息系统硬件的内部审计人员应更好地学习和了解存储管理流程。前面提到的EMC是存储管理产品的供应商,其他如Veritas和legato等软件提供商,也可提供高效的备份和存储管理功能。

① 作者本人,以前曾在EMC公司工作,帮助启动了业务管理咨询集团。