稳健运营 防范风险

SOUND OPERATION
AND RISK MANAGEMENT

PRACTICE OF BUSINESS CONTINUITY
MANAGEMENT FOR COMMERCIAL BANKS

商业银行业务连续性管理实务

中金数据系统有限公司◎编

RISK

中国金融出版社

稳健运营　防范风险

——商业银行业务连续性管理实务

中金数据系统有限公司　编

中国金融出版社

责任编辑：童祎薇
责任校对：孙　蕊
责任印制：丁淮宾

图书在版编目（CIP）数据

稳健运营　防范风险——商业银行业务连续性管理实务（Wenjian Yunying Fangfan Fengxian：Shangye Yinhang Yewu Lianxuxing Guanli Shiwu）/中金数据系统有限公司编．—北京：中国金融出版社，2015.4
ISBN 978-7-5049-7429-7

Ⅰ.①稳… Ⅱ.①中… Ⅲ.①商业银行—银行业务—业务管理
Ⅳ.①F830.33

中国版本图书馆 CIP 数据核字（2014）第 034574 号

出版
发行　中国金融出版社
社址　北京市丰台区益泽路 2 号
市场开发部　(010)63266347，63805472，63439533（传真）
网上书店　http：//www.chinafph.com
(010)63286832，63365686（传真）
读者服务部　(010)66070833，62568380
邮编　100071
经销　新华书店
印刷　北京松源印刷有限公司
尺寸　169 毫米×239 毫米
印张　18
字数　297 千
版次　2015 年 4 月第 1 版
印次　2015 年 4 月第 1 次印刷
定价　46.00 元
ISBN 978-7-5049-7429-7/F.6989
如出现印装错误本社负责调换　联系电话（010）63263947

序 一

进入21世纪以后，伴随着中国经济持续快速发展，中国金融业蓬勃发展，金融总量大幅增长，金融现代化、市场化和国际化程度不断提高，已建立与社会主义市场经济体制相适应的金融体制，并在优化资源配置、支持经济改革、促进经济持续发展和维护社会经济稳定方面发挥了重要作用。商业银行是我国金融体系的重要组成部门，行业整体业务规模不断扩大，竞争日益激烈，且互联网、云计算和大数据等信息网络技术的加速发展和普及应用进一步促进了银行业务的持续创新。当前，信息网络技术已经与银行业务紧密融合，信息系统对银行核心业务流程基本实现了全覆盖，同时银行数据和重大应用的大集中，也客观上将数据安全和信息系统运营安全提到了前所未有的高度，灾备和银行业务连续性管理应运而生。银行业务运营所依赖的信息系统设备故障、管理人员误操作以及天灾人祸导致的突发事件等极易导致业务中断，给银行带来更为严重的风险和破坏力，这已成为商业银行必须面对且务必解决好的关键问题。如美国2001年“9·11”恐怖袭击事件，我国2003年“非典”爆发事件、2008年南方特大雪灾、2008年汶川地震及2009年湖南长沙大停电事故，日本2011年大地震引发海啸和核泄漏等，都凸显出银行全面增强业务持续运行能力已刻不容缓。从21世纪初起，国家有关部门便陆续出台相关规定、监管要求和标准规范，着力加强商业银行业务连续性方面的监管，积极维护和保障国家金融安全和社会稳定。

我国商业银行业务连续性管理经过多年的研究探索和实践，相关领域的企业、专家和学者取得了宝贵经验和丰硕成果。本书是一本详细阐述商业银行业务连续性管理的专著，既全面介绍了国内外业务连续性管

理的理论方法和标准规范，又充分结合了银行自身具有的业务特点，从实际出发为商业银行开展业务连续性管理提供了一个专业视角，可操作性强，相信会对商业银行进一步优化风险管理和IT治理发挥积极有效作用。

国务院信息化领导小组办公室原常务副主任
国家信息化专家咨询委员会原主任

序　二

金融信息化已成为我国金融运营最基本的生存支撑环境，没有金融信息化就没有现代金融服务。银行业金融机构的业务开展高度依赖信息技术的应用，其业务连续性管理已引起银行业金融机构和监管部门的高度重视。

银行业务连续性管理具有很强的科学性和实践性，有其自身的理论和方法。如需要正确认识灾难备份在保证银行业务持续运行中的地位和作用，合理选择灾难备份策略；需要进一步重视数据中心的建设与管理，努力应用先进适用的技术；需要加强 IT 治理，充分重视利用社会化服务；需要认真学习与采用相关的技术与管理标准等。

中金数据系统有限公司经过多年的理论研究和实践经验的积累，集合各领域的专家，历时近 2 年时间编纂而成的《稳健运营　防范风险——商业银行业务连续性管理实务》，是一本以商业银行为特定对象，结合国内监管要求和现实问题，将理论与实际有机结合的业务连续性管理领域的专业书籍。

本书深入浅出地介绍了相关的概念及国内外的发展历程，紧密结合银行业金融机构开展业务连续性管理的实际需求，详细介绍了建设的必要性、建设的要求、建设的方法、建设的契机等，翔实地分析了实际工作中的重点和难点，较为系统地介绍了业务连续性和灾备建设方面的主流技术。尤其难能可贵的是，该书逐一介绍了中国工商银行等 15 家主要商业银行业务连续性管理的实践及发展情况，可供银行业金融机构学习、借鉴，在附录中还介绍了相关的法规和标准体系等，具有很强的可读性。

这是一本专门服务于银行业金融机构的高质量、实用性很强的工具性书籍，对于我国银行业金融机构进行业务连续性管理体系建设有重要

的参考价值。相信本书的出版，不仅能够帮助商业银行提高业务连续性体系建设的效率和质量，促进实现“稳健运营、防范风险”，而且对于对业务连续性管理有较高要求的许多其他行业及企业也有很好的参考价值。

国家信息化专家咨询委员会委员
中国互联网协会互联网金融工作委员会常务副主任
中国人民银行科技司原司长
陈静

目 录

1 银行业务连续性管理的起源及发展

1.1 业务连续性管理

1.1.1 业务连续性管理的起源

1.1.1.1 理论来源

业务连续性管理（Business Continuity Management，BCM）的历史可以追溯到20世纪60年代，那时业务连续性管理的思想和方法是包含在风险管理、危机管理等理论中的，并未作为一门单独的学科来独立研究。那时人们关注的主要是事件本身直接造成的损失，如人和物方面的损失，而对事件造成的其他损失并未给予足够重视。计算机系统在解决系统持续运行的问题时，率先对单点故障采用了冗余措施，这就是最早业务连续性管理思想的开端。

20世纪70年代，出现了容灾恢复的概念。1979年，SunGard在美国费城建立了全世界第一个灾难备份中心，那时候在IT方面人们关注的主要是数据备份。金融组织，如银行和保险公司大都将备份磁带存储在远离主中心的其他地点。灾难主要是火灾、水灾、暴风或其他物理损坏。到了80年代，随着计算机技术的迅速发展，人们对于计算机技术的依赖性增强，对数据安全提出了新的要求，这就产生了一种新技术——灾难恢复技术，而灾难恢复是为了业务的持续运营，业务连续的概念应运而生。这时出现了很多商业恢复中心，在共享设备上提供计算服务，但重点还在IT的恢复。到了90年代，IT出现了重大的革命，灾备建设已经从原来的IT范畴提升到关注业务连续性规划的高度，在IT技术之外，业务连续性管理中加入了业务影响分析、风险分析、灾备策略、恢复预案、演练培训等内容。在恢复过程中涉及了更多业务流程、资源调配、人员组织和策略制定。

十几年间，由于美国“9·11”事件，中国的雪灾、地震等自然灾害，更多的企业开始认识到业务连续性管理的重要性，业务连续性管理因此开始被广泛关注。如今，业务连续性管理已经成为包括灾难恢复、危机处理、供应链管理

和企业可持续发展等的管理类综合问题。

业务连续性管理已经把灾备提升到了管理问题的新高度，而要保持业务连续性，最大的威胁并不是自然灾害这种小概率事件，而是潜伏在企业日常生产运营过程中的流程设计缺陷，一般情况下，这种设计缺陷并不明显，但一旦发生会给企业带来致命的打击。所以，现在的业务连续性管理更多的是企业整体流程合理性的设计规划。

1.1.1.2 理论整合

灾难恢复：灾难恢复侧重于当发生诸如自然灾害、恐怖袭击、设施损坏、人为失误等引起的灾难性事件造成业务中断后，如何进行业务恢复和业务重建，主要用于数据和信息系统的保护。

应急管理：紧急事件管理侧重于面对影响企业业务发展和运营的突发事件和危机，如何进行应急响应和处理的策略、方法及流程，主要用于公共事件的应对。

危机管理：危机通信和公共关系侧重于当发生灾难或突发事件时，如何保持企业对内对外通信联络畅通，以及和诸如政府、媒体、运营商等公共关系的协调，主要用于事件的处理。

风险管理：风险管理侧重于识别企业所面临的潜在的威胁，这些威胁所造成的影响和损失，以及相应的在可接受范围内的预防控制措施，主要用于风险的预防。

业务连续性管理不单单是灾难恢复、应急管理、危机管理和风险管理，它不是一个单独的学科，而是由业务自身驱动的综合学科。其中设施管理、供应链管理、质量管理、健康和人身安全都是人们比较熟悉的传统企业管理的重要方面，单独来看，每一个学科都是独立的，但从全面的、整体的企业业务持续过程来看，它们都是必不可少的元素和组成部分。比如当发生灾难或突发事件时，如何保障企业生产的供应链不中断，产品和服务的质量不明显下降，设施资源合理使用和调配，以及保障员工的健康和人身安全。而其他学科则有各自不同的侧重点。业务连续性管理综合运用了以上各种方法，主要用于灾难中企业的生存，确保在预定的时间内恢复组织的业务运行。

同时需要说明的是，业务连续性管理所涉及的范围不仅仅限于上面所列出的四大主要内容，其核心是保障企业业务持续运行。因此，任何与此有关的领域都是其组成部分，例如人力资源管理，制定灾难恢复和应急相应关键岗位的职责以及人员的调配计划。所以说，业务连续性管理是一个开放的架构。

1.1.1.3 行业推动

近年来，中国灾难恢复市场获得了快速发展，互联网数据中心（Internet Data Center，IDC）调研数据表明，2008 年，中国灾难恢复行业市场规模达到了 12.4 亿美元，比上年增长 28%。IDC 预计，2008 年至 2013 年，中国灾难备份市场将保持 20.7% 的年复合增长率。

中国容灾市场的应用呈现出较强的行业特性，其中金融行业包括银行、保险、证券等客户，是目前容灾市场最大的收入贡献者，占市场容量近 42.1%。随着金融行业对于风险控制的进一步加强和深化，这一格局还将延续。

虽然，不容乐观的国际经济大环境影响到了一些产业的发展前景，但有效的业务连续性及灾难恢复系统往往关系到企业核心业务能否连续运行，甚至关系到企业正常业务的经营，因此容灾解决方案需求相对比较刚性。

2008 年之前，中国灾备市场的需求主要集中在金融、电信以及政府行业。2009 年以来，中国灾备市场发展迅速，除这些行业有更深层次的灾备需求之外，制造、能源、交通等行业的灾备需求也大幅增长。各个行业和企业对灾难备份的重视进一步增加，这直接推动了灾备市场容量的进一步扩大，整个灾备行业进入快速发展的良好势头。这一方面是受地震、雪灾等大规模自然灾害的拉动，另一方面也是因为这些行业中的企业信息化程度越来越高，IT 与业务的联系越来越紧密，对数据安全、系统管理和业务连续的需求更普遍。

总体而言，金融、电信、制造、政府行业是中国灾备市场的主要需求力量，其中，地方商业银行、农村商业银行和大型保险企业、制造企业也是中国灾备市场需求的生力军。

随着互联网行业的发展和互联网在企业中的大规模普及，企业一旦受到黑客攻击、网络应用程序攻击、钓鱼攻击等威胁，损失将非常巨大，灾备计划和灾备建设就在企业发展中被提上了工作议程。

随着政府提出电子政务的发展要求，为了保证政府各项工作的连续性、建设政府对外窗口良好形象并保证信息及时有效发布和传播，财政、税务、海关等政府部门都已经通过政府采购开展了灾备系统建设。

为了预防类似地震、雪灾等大范围自然灾害，多点热备将成为中国灾备市场发展的重要趋势之一。其中，比较典型的方式是两地三中心模式，即设立生产中心、同城灾备中心和异地灾备中心。

多点热备的主要作用是在生产中心遭到自然灾害或人为破坏时，同城灾备中心或异地灾备中心仍然能够提供不间断的业务运营服务，从而保证政府、企业的业务连续性。在政府、金融、电信、交通、能源以及制造等行业，多点热

备方式将在未来几年内具有广阔市场。

1.1.2 业务连续性管理的概念

业务连续性管理的概念很早就已经提出了，它是特指一种整体管理流程。该流程的目标在于及早确定可能发生的冲击对企业运作造成的威胁，并提供合理的架构有效阻止或抵消不确定事件造成的威胁，保证企业日常业务运行的平稳有序。业务连续性管理是比灾难恢复更高层面的概念。国际上关于业务连续性管理的专业机构有国际应急管理者协会（International Association of Emergency Managers，IAEM）、业务连续性协会（Business Continuity Institute，BCI）、国际灾难恢复协会（Disaster Recovery Institute International，DRII）和突发事件规划者协会（Association of Contingency Planners，ACP）。已经建立了业务连续性管理专业机构的国家和地区包括：英国、澳大利亚、奥地利、比利时、加拿大、丹麦、爱尔兰、德国、希腊、以色列、日本、马来西亚、新西兰、俄罗斯、新加坡、南非、荷兰、泰国、美国、墨西哥和西印度群岛等。

同时，经过业务连续性管理专业机构的努力和各国政府的大力支持，国际上已经制定出了成型的 BCM 标准和具体的行业规范。在许多国家，如英国，拥有行之有效的业务连续性管理计划（Business Continuity Plan，BCP）已经成为企业上市的基本要求；在美国，企业法对业务连续性管理的具体措施也有明确的要求；美国联邦储备委员会（Federal Reserve Board）、货币监理署（Office of the Controller of the Currency，OCC）和证券交易委员会（Securities and Exchange Commission，SEC）等机构对美国金融行业的灾难备份建设制定和发布了相应的指南、管理条例和公告；在新加坡，已经拥有若干个业务连续性管理的标准流程和规范，例如新加坡金融管理局的 SS507 标准、新加坡标准/生产力和创新局的 TR19 标准、新加坡中央银行的 MAS BCM 规范。

新加坡金融管理局咨询文件《业务应急计划指导方针》中对业务连续性计划的定义为：为了确定由紧急情况或灾难引发的潜在损失而预先制订的计划和进行的准备。制订恢复计划是为了确保在此情况下机构的关键服务的连续性。

香港金融管理局监管政策指南《业务连续性计划》中对业务连续性计划的定义为：业务连续性计划是提前的计划和准备，对识别因紧急情况或灾难所带来的潜在损失的影响极其必要；制定并实施可行的复苏策略；开发复苏计划以确保连续性；管理一个全面的测试和维护计划。

BCI 是 1994 年在英国成立的 BCM 专业学术组织，BCI 与 DRII 共同制定的 BCM 国际最佳惯例（Professinal Practices for Business Continuity Professionals）是

全世界大多数国家制定 BCM 标准和规范的基础。国际上通用的业务连续性管理的定义就是由 BCI 给出的。

BCI 在 BCM Good Practice Guidelines 2008 中给 BCM 下的定义是：业务连续性管理是一个一体化的管理流程，通过这一流程可以识别那些威胁组织机构的潜在冲击，并提供一个指导性框架来建立组织机构的弹性和有效响应能力，从而保护利益相关者的资产，组织机构的信誉、品牌及其创造价值的活动。

2008 年 4 月，英国标准协会（British Standards Institution，BSI）向全球发布了 BS25999 标准。这些标准和规范皆为 BCM 的应用打下了良好的基础，便于相关企业和机构参照遵循。

BS25999 这样描述业务连续性管理："业务连续性管理是一个整体的管理过程，它能鉴别威胁组织潜在的影响，并且提供构建弹性机制的管理架构，以及确保有效反应的能力，以保护它的关键利益相关方的利益、声誉、品牌以及创造价值的活动。" BS25999 是 BSI 发布的关于 BCM 的英国标准。编写成员来自英国电讯公司、电力公司、水务公司等大型企业，还有地铁警察局、消防局、工贸部等政府机构和证券、保险等行业监管部门。BSI 是一个历史悠久的国际著名标准制定组织机构，1982 年 BSI 被英国政府批准为英国国家标准化组织机构，主要致力于标准制定和推广，在欧洲及全世界标准化组织机构中享有高度声誉。BSI 制定的许多标准都成为国际标准（如 BS5750 成为 ISO9000，BS7750 成为 ISO14000）。

BS25999 是全球第一个业务连续性管理的框架标准，分为 BS25999 - 1 和 BS25999 - 2 两部分。

（1）BS25999 - 1：2006 Code of Practice for Business Continuity Management。业务连续性管理实践要点（已于 2006 年 11 月发布）——主要作为参考文档，提供广泛的业务连续性管理实践要点，作为现行业务连续性管理的最佳实践指南，但不作为评审与认证标准。

（2）BS25999 - 2：2007 Specification for Business Continuity Management System。业务连续性管理系统规范（已于 2007 年 11 月发布）——提供业务连续性管理系统（BCMS）的建立、实施与文档化的具体要求，包括建立组织业务连续性管理系统所需的 PDCA 管理框架和广泛的业务连续性管理措施，同时作为认证标准。

国际公认的由 BSI 发布的 BCM 英国标准 BS25999 已于 2012 年 9 月正式被 ISO22301 取代。ISO22301 管理体系框架能够帮助企业制订一套一体化的管理流