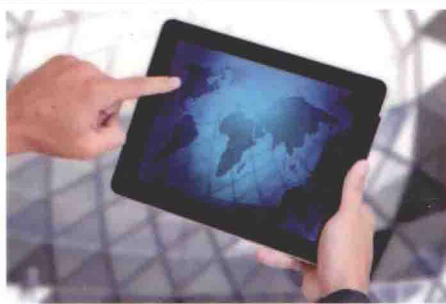


GB/T 30146—2013《公共安全 业务连续性管理体系 要求》宣贯教材



如何在业务持续方面实施全球良好实践的指南

# 良好实践指南

国际业务持续协会(BCI) 著  
余绍强 译

2



Business Continuity  
Institute

如何在业务持续方面实施全球良好实践的指南

# 良好实践指南

国际业务持续协会(BCI) 著

余绍强 译

中国标准出版社

北京市版权局著作权合同登记号:图字 01-2012-1645

图书在版编目(CIP)数据

良好实践指南/国际业务持续协会著;余绍强译. —北京:中国标准出版社,2014.9

书名原文:Good practice guidelines

ISBN 978-7-5066-7372-3

I. ①良… II. ①国…②余… III. ①业务管理—指南—汉、英 IV. ①C931.2-62

中国版本图书馆 CIP 数据核字(2013)第 244189 号

中国标准出版社出版发行

北京市朝阳区和平里西街甲 2 号(100029)

北京市西城区三里河北街 16 号(100045)

网址:www.spc.net.cn

总编室:(010)64275323 发行中心:(010)51780235

中国标准出版社秦皇岛印刷厂印刷

各地新华书店经销

\*

开本 787×1092 1/16 印张 16.75 字数 386 千字

2014 年 9 月第一版 2014 年 9 月第一次印刷

\*

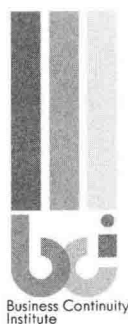
定价 60.00 元

如有印装差错 由本社发行中心调换

版权专有 侵权必究

举报电话:(010)68510107

# 序 1



国际业务持续协会（BCI）已经发布了《良好实践指南》2013 版。在业务持续管理（BCM）国际标准颁布的背景下，这个新的版本不仅强调了业务持续管理的全球发展趋势以及面临的问题，更为业务持续从业人员、审核人员以及监管人员在应用知识方面，提供了更为全面的业务持续管理知识。

就在我为这个新版本指南作序的时候，朝鲜半岛核危机在不断发酵，H7N9 这个新型的禽流感在影响中国，美国波士顿马拉松比赛爆炸案成为自“9·11 事件”以来美国本土遭受的最大的一次恐怖袭击。就在刚刚，中国的西南部再次遭到强烈地震的袭击，引起全世界的高度关注。进入 2013 年，世界似乎越来越不安定，经济危机、自然灾害、流行疾病和恐怖袭击等依然威胁着我们的生活和组织的运营。这些都在敦促我们更加关注业务持续管理。业务持续管理作为一个切实可靠的策略，能保护利益相关方的利益，同时尽量减小危机和灾难事件造成的影响。值得欣慰的是，一方面，越来越多此前并未重视业务持续管理的组织已经开始将业务持续管理纳入他们

的规划之中；另一方面，作为亚洲的主要国家，中国正在制定本国的业务持续管理标准并已经开始对关系国计民生的行业明确提出业务持续管理要求。此时发布这个新版指南，无疑是与时俱进且顺应形势的。

作为国际业务持续协会亚洲区域的执行董事，我很高兴地看到《良好实践指南》中英文双语版本得以不断地更新和出版。向阅读中文的专业人士提供综合性的专业手册，是我们对业务持续行业坚定承诺的一部分。

借此机会，我想向国际业务持续协会技术总监 Lyndon Bird 先生、国际业务持续协会英国办公室的 Lorraine Darke 女士，以及我们的翻译校对团队王川女士、袁德铨先生、秦挺鑫先生、魏军先生、尤其先生、丁涛先生、王二乐先生、乔锐先生以及我们专业翻译员陈弋桃女士对本指南的翻译出版所做出的贡献表示由衷的感谢！

此外，最新的《良好实践指南》2013 版还能为准备通过国际业务持续协会个人认证考试(CBCI)的人们提供一个有针对性且通俗易懂的双语教材。

对于这本指南将为业务持续管理专业人士，以及那些计划实施业务持续管理的人士所带来的裨益，我深信不疑。

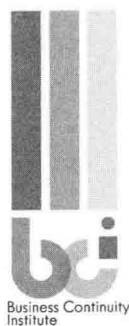
*Henry Ee* 余绍强 FBCI

亚洲区域执行董事 国际业务持续协会

BCP Asia 创始人，执行董事

Henry@bciasia.org

## 序 2



欢迎大家阅读由国际业务持续协会发布的新版《良好实践指南》。自 2002 年这本兼具科普和教育性的指南面世以来,这已经是第五个版本了。尽管有关业务持续的国家标准和国际标准已经相继发布,且有很多关于本指南是否还要存在的疑问,在 2010 版指南的成功基础之上,2013 版指南依然是目前关于业务持续的最全面的著作。

毋庸置疑,本指南已经不再是以业务持续为主题的唯一著作,但是它依然保持着自己对现状的最为独立的观点。它不同于标准,它不仅探讨“做什么”,而且根据业内专家在现实世界中的实践经验,解答“为什么”“如何”以及“何时”等问题。此外,本指南还以在危机管理、事件管理、应急规划、组织弹性及治理、风险和合规的相关领域中提升和实践新兴标准为目标。

诚然,本指南主要是写给业务持续专业人士的,但是它也探讨了关于业务持续的未来趋势、挑战以及那些仍然被更为广泛产业中的从业者们辩论的问题。每个组织都在面对那些他们无法控制的潜在灾难性威胁,特别是

诸如洪水、海啸和地震等自然灾害。确实有一些物理措施可以降低某些可能导致重大损失的事态发生的可能性，但是面对大灾难的威胁，最根本的途径还是采取措施降低其对组织的影响。业务持续就是降低此类事态影响的最有效的方法。

无论如何，很多受助于良好业务持续管理的情况都没那么戏剧性。当一个组织实施业务持续管理方案的时候，它将进行一个业务影响分析(BIA)。业务影响分析的一个交付物就是对组织承担的哪些活动应该被最紧急复原的理解。无论何种起因，这些活动的中断都会对组织产生最为严重和迅速的影响。

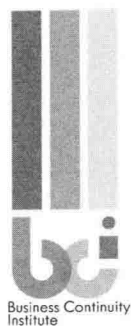
业务持续为组织提供了一个强化其整体弹性的机会，一种不断加强的能够在危急时刻运行业务的生死攸关的特性。

目前《良好实践指南》具有多数世界主要语言的版本，这也是今天业务持续主题如此国际化的另一个体现。对于在亚洲使用中文的读者们，我对你们长久以来对业务持续的积极参与、大力支持表示由衷地感谢，希望你们在阅读《良好实践指南》2013版的时候有所收获。

*Lyndon Bird*

技术总监兼董事  
国际业务持续协会

# 序 3



业务连续性管理(BCM)是识别对组织的潜在威胁以及这些威胁一旦发生可能对业务运行带来的影响的一整套管理过程。该过程为组织建立有效应对威胁的自我恢复能力提供了框架,以保护关键相关方的利益、声誉、品牌和创造价值的活动。随着近年来国内外突发事件频发,BCM作为组织应对突发事件,保障其业务连续的有效方法,在全球范围内被越来越多的组织付诸于实践,随着全球对BCM关注和重视程度的日益加深,BCM将成为一种必然的管理趋势。

近年来,BCM标准化工作发展迅速,2012年5月和12月ISO分别颁布了ISO 22301:2012《公共安全 业务连续性管理体系 要求》和ISO 22313:2012《公共安全 业务连续性管理体系 指南》。在2014年1月召开的ISO/TC 223(公共安全标准化技术委员会)年会上,针对业务连续性又提出了与审核和业务冲击分析有关的多项国际标准提案并获得立项,一系列BCM有关方面标准的集中制定和发布体现了国际标准化组织对BCM的重视及其国际化趋势,随着要求、指南和审核等标准的陆续发



布,BCM 已经形成一套从要求到实施到审核的闭环结构,将有效推动 BCM 相关标准在全球的广泛推广。

我国也高度重视 BCM 标准化工作,SAC/TC 351(全国公共安全基础标准化技术委员会)作为 ISO/TC 223 的国内对口单位,一直积极跟踪参与 ISO 业务连续性管理标准的制定工作,并通过等同采用的方式,于 2013 年 12 月发布了我国第一个业务连续性管理国家标准 GB/T 30146—2013《公共安全 业务连续性管理体系 要求》。目前,正在着力推进业务连续性管理相关标准的立项、制定与实施推广工作。

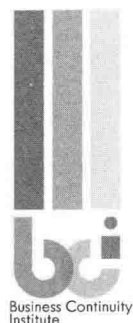
在国际国内业务连续性管理标准化工作迅猛发展的大背景下,《良好实践指南》2013 版的推出可谓正逢其时,它不是一个正式的标准,而是一本遵照 ISO 22301 和 ISO 22313 国际标准,并建立在广泛的 BCM 从业人员的实践经验之上的指导书。该书对推动 GB/T 30146—2013《公共安全 业务连续性管理体系 要求》的实施具有重要的参考价值。

当然,由于业务连续性管理工作在我国方兴未艾,因此该书基于国内企业成功实践经验的分析总结还有所欠缺。我希望作者能够在未来几年内积极收集分析国内企业 BCM 成功案例,继续改进《良好实践指南》,为 BCM 相关标准在中国的实施推广提供强有力的支持。

王金玉

中国标准化研究院

# 目 录

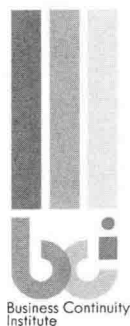


致谢辞 .....	1
<b>《良好实践指南》2013 版介绍 .....</b>	<b>3</b>
我们为什么需要《良好实践指南》? .....	3
与《良好实践指南》2010 版相比有何变化? .....	4
本指南面向哪些读者? .....	4
<b>业务持续和国际业务持续协会的起源 .....</b>	<b>5</b>
<b>常见问题 .....</b>	<b>6</b>
业务持续应用在哪些方面? .....	6
业务持续专业人士有能力审核业务持续管理体系吗? .....	6
业务持续和组织弹性是一回事吗? .....	7
我们需要单独的危机管理职能吗? .....	7
业务持续和风险管理在哪些方面有所重叠? .....	8
业务持续适用于基于风险的正式框架吗? .....	8
业务持续对公司治理有何贡献? .....	9
业务持续和应急管理区别何在? .....	9
国际标准能改变我们对业务持续的认识吗? .....	10
业务持续管理体系标准与其他标准怎样重叠? .....	10



一个业务持续专业人士通常需要什么样的背景? .....	10
必须聘用专职的业务持续专业人士管理业务持续管理方案吗? .....	11
<b>业务持续管理的生命周期 .....</b>	<b>11</b>
<b>国际业务持续协会专业实践</b>	
<b>业务持续——管理实践</b>	
专业实践一:方针和方案管理 .....	13
专业实践二:业务持续的植入 .....	35
<b>业务持续——技术实践</b>	
专业实践三:分析 .....	45
专业实践四:设计 .....	61
专业实践五:实施 .....	73
专业实践六:验证 .....	91
<b>术语表 .....</b>	<b>108</b>

# 致谢辞



这本《良好实践指南》(简称“GPG”)汲取了国际业务持续协会(BCI)各成员在学术、技术和实践层面的丰富经验。

本指南可供那些掌握了有关业务持续的基本原理及其基本原则等应用知识的专业人士、顾问、审核员和监管者使用。它主要不是为初学者提供指南,不过本指南能为他们提供许多卓越的学习材料。建议初学者在有经验的专业人士指导下使用本指南,或参加合适的培训课程。

新版《良好实践指南》的编撰工作始于2012年1月。初稿于2012年6月完成,并在2012年9月底前给予同行审阅,吸取了广泛的意见,并进行了全面的评估。2012年10月,主编通过了最终合订版并提交给国际业务持续协会全球会员委员会审阅和批复。2012年11月至2013年2月间,对本指南进行了翻译,并修改了相应的培训与考试大纲。

负责《良好实践指南》2013版的项目团队成员包括:

主编: Lyndon Bird(国际业务持续协会伙伴级会员,下称“FBCI”)

助理编辑: Deborah Higgins(国际业务持续协会会员,下称“MBCI”)

编者: Lyndon Bird (FBCI)、Ian Charters (FBCI)、Mel Gosling (MBCI)、Tim Janes (MBCI)、James McAllister (MBCI) 和 Charlie McLean-Bristol (MBCI)

管理者: Jan Gilbert

参与者: Malcolm Brooke (MBCI)、Jim Burtles Hon (FBCI)、Steven Cvetkovic (SBCI)、Gianna Detoni (MBCI)、Stacey Farrow (MBCI)、Debbie Featherstone (MBCI)、Lesley Grimes (MBCI)、Gayle Hedgecock (MBCI)、Simon Kearney (MBCI)、David Lightfoot (MBCI)、Margaret Millett (MBCI)、Norman Powell (MBCI)、Keith Prabhu (MBCI)、Clifford Seow (MBCI)、Brigitte Theuma (MBCI)、Pauline Wilson (MBCI)、John Worthington (MBCI) 和 Anton Wroblewski (MBCI)。

国际业务持续协会在此感谢以上列出的所有人士为了国际业务持续协会和业务持续全球社区而在编撰本指南时积极给予的宝贵时间和专业意见。当然,没有众多国际业务持续协会会员对前一版的贡献,新版指南也无从谈起;因此,国际业务持续协会也在此感谢前一版的所有参与者。本指南的参与者均同意:他们不拥有本指南的个人版权 © 或知识产权 (IP),本指南归 BCI™ 独家所有。

*Lyndon Bird (FBCI)*

主编

国际业务持续协会技术开发总监

## 《良好实践指南》2013 版介绍

自 1994 年国际业务持续协会(简称“BCI”)成立以来,业务持续(简称“BC”)已有许多变化;随着越来越多的人意识到其价值,业务持续还将不断发展。

在目前的形势下,业务持续尤显重要。世界仍未从过去十年的全球经济危机中完全复苏。我们所处的时期具有新的经济和政治秩序,并且亟须应对不断增加的全球威胁,如能源安全、移民潮、网络犯罪和气候变化等。在此背景下,业务持续学科经证明在面对这些重大商业和社会变化时能发挥作用,这着实令人鼓舞。

个人如想成为国际业务持续协会的法定会员,必须在所有六项专业实践中显示自己的能力。BCI 认证考试将考查《良好实践指南》中所有六个专业实践章节的知识。考试合格者将获得及格或优秀两种成绩。在准备参加 BCI 认证考试之前,有必要全面掌握本指南的内容。

如想升级到某一法定会员等级(AMBCI、MBCI 和 FBCI),也必须展示其经验。有关每个等级所需详细经验,请访问 [www.thebci.org](http://www.thebci.org)。

《良好实践指南》2013 版使用了 ISO 22301:2012 推荐使用的术语。

BC	业务持续	一个组织在破坏性事件之后仍能持续以可接受的重新定义的水平交付产品或服务的能力
BCM	业务持续管理	业务持续管理是一个整体的管理过程,它能识别组织面临的潜在威胁,以及这些威胁一旦变成现实可能对业务运营造成的影响,并且为构建组织弹性提供框架,以使组织具备有效应对的能力,从而保护其关键利益相关方的利益、组织声誉、组织品牌以及创造价值的活动
BCMS	业务持续管理体系	综合管理体系中的一部分,旨在建立、实施、运行、监督、评审、维护和改进业务持续

有关《良好实践指南》使用的所有术语,可参见“术语表”。

### 我们为什么需要《良好实践指南》?

在目前存在的各业务持续(BC)国家标准和国际标准中,良好实践指南已有所不同。出版物不再是严肃题材内容的唯一提供者,但它仍然是这一课题中现有最全面和独立思考的观点。对业务持续专业人士来说,它的实际价值在于它不单思考“做什么”(这方面各类标准已经覆盖),而且还思考“为什么”“如何”以及“何时”开展现实世界的专家所撰写的这些实践。它不是一个规范或执行标准。它旨在提升并补充危机管理、事件管理、应急规划、组织弹性,以及治理、风险和合规性(简称“GRC”)的现有标准。

2013 版主要由业务持续专家撰写。它为这一行业提供了如何实践这一学科的现有知识体系。与管理体系统标准不同的是,本指南在识别从业者仍在热议的未来趋势、挑战和问题方面具有灵活性。与此同时,它还为如何检验专业人士的知识以及学术培训的组成基础提供了公认的基准。

## 与《良好实践指南》2010 版相比有何变化?

《良好实践指南》的各项原则无需大幅修改,因此两个版本的主要组成部分保持一致,但对语言进行了精炼。新版同样涵盖了业务持续管理生命周期的六个阶段,并将它们定义为专业实践(简称“PP”)的内容。六项专业实践被细分为两项管理实践和四项技术实践。我们决定简化各个专业实践的命名,并使用了以下章节标题:

### 管理实践

- 专业实践一:方针和方案管理
- 专业实践二:业务持续的植入

### 技术实践

- 专业实践三:分析
- 专业实践四:设计
- 专业实践五:实施
- 专业实践六:验证

## 本指南面向哪些读者?

《良好实践指南》并不是仅仅针对需要专业证书的人士。作为一个知识体系,它可用作业务持续培训课程的信息源,也可为那些需要更好地了解业务持续的同事提供意识宣传。这里所说的同事既包括公共关系和危机管理方面的专业人士,也包括供应链从业者和人力资源工作者。

业务持续并不局限于任何一个行业。事实上,我们采用了标准产业分类代码对国际业务持续协会的会员组织进行分类,这正好说明了业务持续可用于各行各业。同样地,术语“业务”并不代表业务持续仅适用于商业组织,政府公共部门也可受益于这些实践,公共志愿服务机构亦如是,其中包括志愿者组织和非营利性组织。事实上,许多志愿者组织是公共部门的关键交付合作伙伴。

虽然业务持续管理在大中型组织中的作用明显,但它在小型组织中发挥的作用不尽如人意。业务持续管理本身并非专为“大中型组织”而生,国际业务持续协会意识到它在小型组织中作用不佳是因为鲜有小型企业主能够彻底执行《良好实践指南》,因此协会根据《良好实践指南》,为小型组织编制了更简单的替代材料。这类材料既包括国际业务持续协会发布的指南,也包括了政府机关、其他专业结构以及业务支持团体发布的指南。



## 业务持续和国际业务持续协会的起源

业务持续的准确起源仍有待商榷,不过它的某些发展史是确定的。20世纪70年代晚期,最初的商业灾难恢复站点在美国出现,这使得对第三方顾问的需求应运而生。开始时,这类顾问服务是技术性的,完全旨在处理数据或MIS(管理信息系统),随后被普遍称作“信息通讯技术”(下称“IT”)。

这一课题被称为“灾难恢复规划”(下称“DRP”)。同业者在当时面临的初步问题是很难说服最高管理层为何要在一些可能永远不会发生的事情上进行重大投资。由此引出了一种分析业务和系统可用性中断所导致的影响的方法论。

20世纪80年代中期,这一方法论在美国初步成形,随后被迅速采用并传入欧洲(主要是英国)和澳大利亚。由此可见,业务影响分析(下称“BIA”)模型确实早于范围更广的业务持续的首次应用。此外,也可以证实成功开发出DRP商业方法论的首个顾问来自美国,不过这种方法很快在欧洲确立并得以提升。

关于业务持续是如何逐渐从DRP中独立出来的故事众说纷纭。国际业务持续协会的观点源自众多资深专业人士的普遍认识、经验和回忆。虽然这不足以完整地叙述故事,但它是准确的概述,有益于从事业务持续的新人和未来的专业人士。

1988年,一家名为“Survive”的英国组织成立,旨在满足当时对灾难恢复业界交流经验和知识的论坛的新兴需求。这一组织随后发展成为培训、活动和出版物的商业提供商,不过它最初成为一家社交网络团体的愿景非常成功。它在许多主要讲英语的国家成立了类似的团体。1991年,“Survive”决定更名为“The Business Continuity User Group”(业务持续用户团体)。众多顾问早已开始使用“业务持续”这个术语,但“Survive”的更名在改变外界对这一课题的看法上影响更大。

差不多同一时间,两家美国最大的灾难恢复公司也改变了他们的定位,认为“持续”传递的信息比“恢复”更积极。一些观点认为这使得业务持续仅仅变成DRP的另一种说法,并可能阻碍业务持续作为一门新学科的发展,尤其是在北美的发展。

另一个关键发展是英国信息安全标准的推出,它很快演变成为ISO标准,即ISO 17799。这些标准的核心原则包括了对业务持续的要求,并根据数据可用性定义了业务持续。这使得对业务持续概念的讨论更加纷繁复杂,并使许多IT从业者宣称业务持续仅只是信息安全的一个分支。这种观点在那些当时还未形成业务持续观念的国家获得了许多支持,例如在亚洲和中欧。

1993年,“Survive”成立了一个工作小组,调查有关业务持续专业人士的培训和认证问题。当时存在一种认知,要将技能娴熟的业务持续专业人士和一般顾问(通常是IT背景的顾问)区分开来。类似的讨论较先在美国展开,并使得灾难恢复协会于1988年成立。该协会从业内热门期刊《灾难恢复杂志》(The Disaster Recovery Journal)独立出来,主要提供培训和认证。

国际业务持续协会于1994年成立,是“Survive”工作小组建议下的直接产物。在国际业务持续协会的推出和发展过程中,有必要为那些寻求认可或资质的人明确衡量和判断其能力的技能标准。最初拟定了13或14种技能,但最终削减至十种能力标准。



这些专业能力标准是在国际业务持续协会和国际灾难恢复协会(现在的 DRII)的共同努力下制定和同意的。

到 20 世纪末,兴起了一种整体的端对端的方法。在整个业务运营中提供保护和弹性的需求在当时更加突出。尽管“过分渲染”了千年虫的问题,但大型公司在全球的严阵以待确实证明了其对单个供应商和其他单点故障的高度依赖。虽然这样的思考已被概括在多年前提出的业务持续的首个概念中,但这个概念还是用了十多年才赢得广泛的认可。它使得诸如 BS 25999 和其他国家层面的业务持续管理体系标准等举措更可行,因为这些举措具备了坚实的概念框架。

21 世纪,业界决心沿着“质量、信息安全和环境服务”已铺就的道路梳理业务持续并将其归为管理体系标准的一部分。这项工作开始时参考了一系列的指导标准,如英国的 BS 25999-1,美国的 NFPA 1600,以及澳大利亚和亚洲的各种指南。包括英国金融服务管理局、澳大利亚审慎监管局(APRA)和美联储在内的各监管机构也开始积极参与这一领域,尤其是在纽约世贸中心被毁之后。现在,已有多个国家推出了正式的国家标准;并且自 2012 年起,ISO 也出台了业务持续管理体系标准(ISO 22301)和单独的指导标准(ISO 22313)。

## 常见问题

常有人请国际业务持续协会就业务持续及其补充学科的各类话题表明观点。由于许多此类话题在业务持续界仍无定论,我们认为必须明确以下几点。这些观点并不是最终定论,但能对业界的讨论有所贡献。以下是最常见的问题:

### 业务持续应用在哪些方面?

广泛的观点认为业务持续只是处理影响大且可能性小的事态。目前更为普遍地意识到业务持续作为“日常运营”的一部分,能改善组织弹性。业务持续这个概念还可用于解决非实体事态,如供应商不能履约和负面媒体关注引起的商业危机。

成功应用业务持续可增强组织弹性,从而带来更好的公司业绩。一般来说,弹性的定义是一个组织消化和应对中断的能力,以及从中断中恢复的能力。业务持续为理解价值是如何在组织内创造出并加以维护的,以及在这些价值同交付该价值所存在的依赖性 or 脆弱性之间如何建立直接关系提供了独特的框架。

从根本上看,弹性并不能第一时间停止或预防中断发生。由于大部分中断性事件从本质上是无法预计的,单凭提供全面保护的预防措施将不可避免地造成盲目自信。

### 业务持续专业人士有能力审核业务持续管理体系吗?

业务持续专业人士应精通所有六项专业实践,但这些实践是其自己的协会和认证机构凭借其自身建立的专业职能,因此对于成为一个合格的业务持续管理体系审核员