

BS 25999-1:2006

英国标准

业务连续性管理

第一部分：实用规则

ICS 03.100.01



目 录

前言	5
出版信息	5
本标准的使用	5
表述约定	6
合同义务与法律法规的考虑	6
符合标准本身并不获得法律义务的豁免。	6
1. 范围和适用性	7
2. 术语和定义	8
3. 业务连续性管综述 (BCM)	12
3.1. 什么是 BCM?	12
3.2. BCM 和组织策略	12
3.3. BCM 与风险管理的关系	12
3.4. 为什么组织应该采用 BCM	12
3.5. 有效的 BCM 方案带来的好处	13
3.6. 有效 BCM 方案的输出	13
3.7. 业务连续性管理生命周期要素	13
4. 业务连续性管理方针	15
4.1. 概要	15
4.2. 相关内容	15
4.3. 开发业务连续性方针	15
4.4. BCM 方案的范围	15
4.5. 外包的活动	16
5. BCM 方案管理	17
5.1. 概要	17
5.2. 职责分配 (治理)	17
5.3. 在组织内实施业务连续性	18
5.4. 持续管理	18
5.5. BCM 文件	18

6. 理解组织	20
6.1. 介绍	20
6.2. 业务影响分析(BIA)	20
6.3. 识别关键活动	21
6.4. 确定连续性要求	21
6.5. 评价关键活动的威胁（风险评估）	22
6.6. 确定选项	22
6.7. 签署	23
7. 确定业务连续性策略	24
7.1. 介绍	24
7.2. 策略选项	24
7.3. 人员	25
7.4. 基础设施	25
7.5. 技术设施	26
7.6. 信息	26
7.7. 供给	27
7.8. 相关利益方	27
7.9. 公众紧急事件	28
7.10. 签署	28
8. 开发和实施 BCM 响应措施	29
8.1. 介绍	29
8.2. 事故响应结构	29
8.3. 计划内容	30
8.4. 事故管理计划 (IMP)	32
8.5. 事故管理计划 (IMP) 的内容	32
8.6. 业务连续性计划 [BCP(s)]	34
8.7. BCP 的内容	34
9. BCM 安排演练、维持和评审	37
9.1. 介绍	37
9.2. 演练方案	37
9.3. BCM 安排的演练	38
9.4. 维持 BCP 安排	39

9.5. 评审 BCM 安排	39
10. 在组织文化中融入业务连续性管理	41
10.1. 总则	41
10.2. 意识	41
10.3. 技能培训	42
参考书目	43
标准	43
其他出版物	43

前言

出版信息

本标准由BSI发布, 于2006年11月30日生效。本标准由业务连续性技术委员会BCM/1编写。该委员会的成员组织包括:

Association of British Certification Bodies
Association of British Insurers
Association of Chief Police Officers
Association of Insurance Risk Managers
Business Continuity Institute
Cabinet Office
Chief Fire Officers' Association (CFOA)
Continuity Forum
Coventry University
Department of Trade and Industry
Emergency Planning Society
Federation of Small Businesses
Financial Services Authority
Independent International Organization for Certification
Institute of Directors
Institute of Emergency Management
Institute of Internal Auditors
Institute of Risk Management
Intellect
Metropolitan Police
Securities Industry Business Continuity Management Group (SIBCMG)
Society of Industrial Emergency Services Officers (SIESO)
Survive

本标准由整个业务连续性论坛的从业者, 借鉴其学识、技术和业务连续性管理(BCM)的实践经验开发而成。本标准提供了以业务连续性管理的最佳实践为基础的管理体系。本标准试图为实施业务连续性管理的多数情形提供一个集中参考, 可能用于工业、商业、公共和志愿机构的大型、中型或小型组织。

本标准是BS25999的第一部分。本标准发布时, 规定业务连续性要求的第二部分正在制订中。

本标准的使用

本标准作为实用规则，采用指南和建议的方式。不应该做为规范被引用，并应该特别注意符合性声明没有被误导。

希望任何声称符合本标准的用户能够正确处理与本标准建议的偏差。

表述约定

本标准仅提供建议，在语句中采用“应该（should）”。

条款3不包含任何建议；然而，它提供了有关业务连续性管理的有用的背景信息（虽然本标准并不试图作为业务连续性管理的入门指南）。

“可/可能（may）”用于表达选择性，如，用于表达条款的主要推荐项的可选项。“能够（can）”用于表达可能性，如一个事态或活动的后果。

补充注释、解释和一般性的信息材料，采用楷体字，并且不构成一个标准的要素。

合同义务与法律法规的考虑

本出版物不声称包括一个合同所有必要的规定。用户负责对其进行正确的应用。

符合标准本身并不获得法律义务的豁免。

1. 范围和适用性

本标准提供业务连续性管理（BCM）有关的过程、原则和术语。本标准的目的是为组织理解、开发和实施业务连续性提供一个基础，并为组织与客户和与其他组织进行交易时提供信心。并使组织能够采用一致的、公认的方式，测量其BCM的性能。

本标准提供基于BCM最佳实践的体系。

本标准可用于负责业务运行或提供服务的任何人员，从最高管理层到组织各个层次的员工；从单一地点的组织到全球布局的大型组织，从专营商和小型企业到雇佣数千名员工的组织。因此，本标准适用于任何人所负责的任何运行及运行活动的连续性。

本标准不覆盖关于公众紧急事件的应急计划。

注：最后，不论在在业务连续性管理中付出多大的努力和资源，企业仍有可能面临非预期的事故或系列事故。

2. 术语和定义

下列术语和定义适用于本标准。

2.1. 活动 activity

由组织（或以组织的名义）生产或支持一个或多个产品或服务所履行的过程或过程组。

注：例如，会计、呼叫中心、IT、制造、发送。

2.2. 业务连续性 business continuity

组织对事故和业务中断的规划和响应，使业务可能在预先定义的级别上持续运行的组织策略和战术上的能力。

2.3. 业务连续性管理 business continuity management (BCM)

找出组织有潜在影响的威胁及其对组织业务运行的影响，通过有效响应措施保护组织的利益、信誉、品牌和创造价值的活动，并为组织提供建设恢复能力框架的整体管理过程。

注：业务连续性管理包括组织在面临灾难时对业务活动的恢复和连续性的管理，以及为保证业务连续性的切适当宜所进行的培训、演练和评审而进行的整个方案的管理。

2.4. 业务连续性生命周期 business continuity management lifecycle

业务连续性管理方案所包含的所有方面及各个阶段的的一系列业务连续性活动。

注：图1给出了业务连续性的生命周期的图例。

2.5. 业务连续性管理方案 business continuity management programme

由最高管理层和适当资源支持的持续管理和治理过程，以保证识别潜在损失所造成的影响，维持可行的恢复策略和方案所需的必要步骤能够得以实施，并通过培训、演练、维持和评审以保证产品和服务的连续性。

2.6. 业务连续性计划 business continuity plan (BCP)

为发生事故时，使组织能够在一个预定的可接受的水平上连续提供其关键活动，而开发、编辑和维持就绪的程序和信息文件集。

2.7. 业务连续性策略 business continuity strategy

组织在发生灾难或其他重大事故或业务中断时，保证业务恢复和连续的方法。

2.8. 业务影响分析 business impact analysis (BIA)

分析业务功能以及可能发生的业务中断对业务功能所造成的影响。

2.9. 公众紧急事件 civil emergency

国内发生的严重危机人身、环境或社会安定的事件或情形。

[UK Civil Contingencies Act 2004 (1)]

2.10. 后果 consequence

对组织目标造成影响的结果。

注1: 一个事故可能造成一系列的后果。

注2: 后果可能是确定的或不确定的, 并可能给业务目标带来正面或负面的影响。

2.11. 成本效益分析 cost-benefit analysis

测量、比较一个特定方案的实施成本和收益的财务方法。

注: 收益可能界定在组织的财务、声誉、服务提供、法律法规或其他方面。

2.12. 关键活动 critical activities

组织为提交关键产品或服务以满足其最重要的、时间紧迫的目标所必需执行的活动。

2.13. 中断 disruption

可预期(如罢工、飓风)或不可预期(如停电或地震)的, 导致非计划地与组织目标所期望提交的产品和服务相背离的事件。

2.14. 2.14 公众应急计划 emergency planning

开发和维持已达成一致的程序, 以防止、减少、控制、减轻公共紧急事件或在公共紧急事件中采取其他措施。

2.15. 演练 exercise

业务连续性计划部分或全部预演的活动, 以保证计划包含适当的信息和程序, 使得当计划付诸实施时能够达到预期效果。

注: 演练可能包括启动业务连续性程序, 但更多是模拟一个公告或未公告的业务连续性事故, 通过参与者角色的扮演, 以在真正付诸实施之前评估可能出现的问题。

2.16. 收获 gain

正面的结果。

2.17. 影响 impact

特定输出的评估结果。

2.18. 事故 incident

可能引起或带来业务中断、损失、紧急情况或危机的情形

2.19. 事故管理计划 incident management plan (IMP)

明确定义和形成文件的行动计划，以为事故发生时所用。通常包括实施事故管理过程所需的关键人员、资源、服务或活动。

2.20. 启动 invocation

组织宣告业务连续性计划需要付诸实施以继续提供关键产品和服务的活动。

2.21. 可能性 likelihood

某些事物发生的机会，可能是明确定义并进行客观或主观测量评估的，或是采用一般性的描述（如罕见的、不大可能的、可能的、几乎肯定的），或利用频率或数学的概率。

注1：可能性可能被表述为定性或定量。

注2：在非英语语言中“probability（概率）”可能和“likelihood（可能性）”通用，但两者并不完全相同。

“probability（概率）”在英语中通常并正式解释为一个数学词汇，本标准使用的“likelihood（可能性）”在广义上可能解释为“probability（概率）”

2.22. 损失 loss

负面后果。

2.23. 最大可忍受中断期限 maximum tolerable period of disruption

该期限过后，如果产品或服务的交付不能恢复，组织生存能力将受到不可恢复的伤害。

2.24. 组织 organization

职责、权限和相互关系得到安排的一组人员和设施。

示例：公司、集团、商行、企事业单位、研究机构、慈善机构、代理商、社团或上述组织的部分或组合。

注1：安排通常是有序的。

注2：组织可能是公众的或私有的。

[BS EN ISO 9000:2005]

2.25. 产品和服务 products and services

组织向其客户、接受人和利益相关方提供的有益成果。如，制品项目、汽车保险、法规遵从和社区护理。

2.26. 恢复时间点目标 recovery time objective

为以下设定时间目标：

- 事故后重续产品或服务的交付；或
- 事故后重续活动的性能；或
- 事故恢复IT系统或应用。

注：恢复时间点目标应小于最大可接受中断时间。

2.27. 健壮度 resilience

组织忍受事故影响的能力。

2.28. 风险 risk

某些事物可能发生并对目标的达成造成影响。

注1: 风险通常被用于不同的方式, 作为名词 (一个“风险”或复数多个“风险”), 动词 (给什么带来“风险”)。作为名词术语“风险”, 风险可能是一个潜在的、导致问题的发生事件或这些事件的后果。明确区分“风险”术语的不同用法对风险管理 (参见条款6.5) 是非常重要的。

注2: 风险是针对特定目标进行定义的; 因此, 任何来源的风险对应几个不同的目标有着多个可能性的测量结果。

注3: 风险的量化通常是以取平均值的方式, 即通过综合后果的加权平均及其可能性所得到的“期望值”。然而, 不管怎样, 需要可能性的分布来表示后果的可能性的量化范围。另外, 在期望值之外可能会用到统计摘要, 如标准偏差。

2.29. 风险偏好

组织在任何时间准备接受、容忍、遭受的风险总和。

2.30. 风险评估 risk assessment

风险识别、风险分析和风险评价的整个过程。

2.31. 风险管理 risk management

结构化的开发和应用管理文化、方针、程序行实践, 以进行风险识别、风险分析、风险评价和控制风险的任务。

2.32. 相关利益方 stakeholders

组织成果的既得利益获得方。

注: 这个一个广泛的术语, 包括但不限于, 内部或“外包”的员工、客户、供应商、合作伙伴、员工、分销商、投资人、保险公司、股东、业主、政府和监管部门。

2.33. 最高管理层 top management

在组织的最高层实施指导和控制的个人或小组。

[BS EN ISO 9000:2005]

注: 最高管理层, 特别是在大型跨国企业, 最高管理层可不直接参与, 但管理者显然需要通过行政管理系统承担责任。在小型组织, 业主或独资经营者可作为最高管理层。

3. 业务连续性管综述 (BCM)

3.1. 什么是BCM?

业务连续性管理是一个由业务所有和业务驱动的、建立符合预定目的的战略和操作框架的过程:

- 预先提高组织抵抗业务中断能力的健壮度,以达成其关键目标;
- 为事故发生后,组织恢复按在商定时间内按商定水平提供其关键产品或服务的能力,提供了一个预演的方法;
- 交付经过证明的管理业务中断的能力,以保护组织的信誉和品牌。

业务连续性的个别过程可能会与随组织的规模、结构、职责而不同,但不论是志愿机构、公共或私有组织,及其规模、范围和复杂程度,基本的原则还是一致的。

3.2. BCM 和组织策略

不论组织的大小,都具有目的和目标,如成长、提供服务或收购其他业务。组织通常通过达成短期、中期和长期目标的策略计划来达到这些目的和目标。组织最高层对BCM的理解,可能保证不会因意外中断而危及组织的目的和目标。

事故的后果可能会有很大的不同。这些后果可能是生命的消失,资产或收入的损失,或无力提供组织策略、信誉、甚至生存所依赖的产品和服务。

BCM必须认知已知利益相关方对策略的重要性。此外,作为业务中断的后果,一些新的利益相关方会浮现,并且可能会给损害的最终范围带来直接的影响。例如,媒体会在组织面对业务中断时,施加压力。所有这些问题都是在组织的策略层面所关心的。

3.3. BCM 与风险管理的关系

BCM是风险管理框架的补充,用于理解组织运行和业务上的风险及其后果。

风险管理寻求管理组织需要交付的关键产品或服务的相关风险。产品和服务的交付可能因多种事故而中断,其中很多事故难以预测和分析原因。

通过集中考虑中断的影响,BCM识别组织赖以生存的产品和服务,以能够识别组织持续承担职责的要求。通过BCM,组织能够认知到,为保护生命、资产、技术、信息、供给、相关利益人和信誉,在事故发生前,所需要完成的事情。

通过以上认知,组织能够对当中断发生时所需要的响应有一个现实的想法;并能够有信心通过管理以达到不会形成服务或产品的不可接受的延迟交付。

3.4. 为什么组织应该采用BCM

BCM构成良好业务管理、服务提供和企业家谨慎的重要元素。

管理层和业主有职责维持组织不中断持续运行的能力。组织经常承诺或有责任交付产品和服务,例如,签订合同和其他方式提供预期。所有组织都有道德和社会上的责任,特别是当他们提供公共紧急响应、

公共或志愿服务时。在某些情形下，组织有法律法规上的职责去执行BCM。

所有都需要面对中断，如技术故障、水灾、电力中断或恐怖活动等。BCM在保护生命安全的同时，提供适当响应业务中断的能力。

BCM应该作为组织的增值计划，而不是一个昂贵的策划过程。

3.5. 有效的BCM方案带来的好处

一个有效的BCM方案给组织带来的好处：

- 能够提前识别一个业务中断带来的影响；
- 具备就绪的有效中断响应措施，使得中断对组织的影响最小；
- 维持对不可保险的风险的管理能力；
- 鼓励不同小组之间的合作；
- 能够通过演练过程展示可信的事故响应；
- 能够提高组织的信誉；
- 通过可证实的维持服务和产品交付的能力，获得竞争优势。

3.6. 有效BCM方案的输出

一个有效BCM方案的输出包括：

- 关键产品和服务被识别和保护，以保证其持续的交付；
- 提供有效响应的事故管理能力；
- 组织对自身及其与其他组织、相关监管机构或政府、当地权威机构关系的理解；以及对应急服务的适当开发、文件化和理解；
- 通过适当演练，培训员工对事故或中断的有效响应；
- 理解利益相关方的要求，并能够被执行；
- 在中断发生时，员工得到适当的支持和沟通；
- 组织的供应链是安全的；
- 组织的信誉得到了保护；
- 使组织符合法律法规的义务。

3.7. 业务连续性管理生命周期要素

BCM生命周期有6个要素组成，如图1所示。这适用于所有组织，不论其规模或性质：公众、私有、非盈利、教育、工厂等。BCP方案的范围和结构可能不同，付出的努力也可根据特定组织进行调整，但基本的要素必须得到履行：

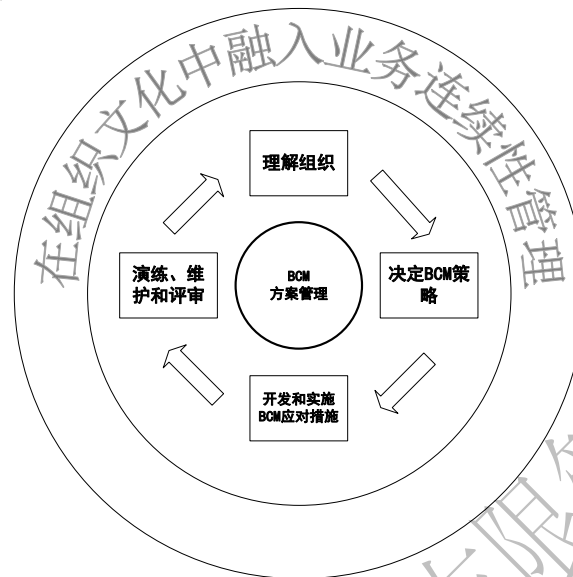
a) BCM 方案管理（参见条款 5）

方案管理使得业务连续性能力得以建立（如果需要），并根据组织的规模和复杂性以合理的方式得到维持。

b) 理解组织（参见条款 6）

与“理解组织”相关的活动提供组织产品和服务区分优先次序, 以及产品和服务必须交付的紧迫性的信息。这为选择适当BCM策略的确定了要求。

图1: 业务连续性生命周期



c) 确定业务连续性策略（参见条款7）

通过对一系列策略的评估, 确定业务连续性策略。这使得每一产品或服务选择了合适的响应方式, 组织因此在中断发生中或发生后能够按以下条件持续交付这些产品和服务:

- 在可接受的运行级别; 并
- 可接受的时间框架内。

选择业务连续性策略时应考虑健壮度以及组织现有措施。

d) 开发和实施BCM响应（参见条款8）

通过开发和实施BCM响应, 建立事故管理和业务连续性、业务恢复计划的管理框架, 以详细描述在事故发生中或发生后维持和恢复运行的步骤。

3.7.d)的注释: 贯穿本标准的术语“事故”体现了事件的延伸性, 包括从小到大可能影响组织的事件。单个或一系列的事故可能给组织承担其义务带来严重的中断影响。如果事故得到了很好的管理, 可能不会发展成为危机。然而, 某些给组织目标带来重大影响的中断, 应立即作为一个危机来考虑。

即使组织对事故的预期损坏程度的应对措施已经进行了仔细研究, 但仍有可能超出预备的范围。这告诫管理层及支持组织结构不要固守现有计划, 需根据当时情形作出调整。业务连续性计划绝不会替代知情和称职管理者的决策。

e) BCM 演练、BCM安排的维持和评审（参见条款9）

BCM的演练、维持、评审和审核使得组织能够:

- 展示业务连续性策略和计划完成、更新和准确的程度;
- 识别改进机会。

f) 在组织文化中融入BCM（参见条款10）;

在组织文化中融入BCM, 使得BCM成为核心价值的一部分, 并让利益相关方对组织应对中断怀有信心。

4. 业务连续性管理方针

4.1. 概要

4.1的注释:

建立业务连续性方针的目的:

- 保证所有BCM活动按照商定的、可控的方式被导入和实施;
- 让业务连续性的能力满足不断变化的业务要求, 并与组织的规模、复杂程度和性质相符合;
- 为持续的BCM设置清晰的已定义的框架。

4.1.1. BCM 策略定义以下过程:

- 为建立业务连续性能力组织活动;
- 业务连续性能力的持续管理和维持。

4.1.2. 结合业务连续性规范、端对端设计、建立、实施和最初演练组织活动。

4.1.3. 在组织日程维持和管理活动中融入业务连续性, 定期演练计划, 并对计划进行更新和沟通, 特别当基础设施、人员、过程、市场、技术或组织结构发生重大变化时。

4.2. 相关内容

组织应该确保 BCM方针与组织的性质、规模、复杂程度、地理位置及其业务活动的危险程度相符, 并反应组织的文化、关联性和运行环境。BCM方针定义过程要求, 以确保业务连续性安排满足组织遭受事故时的需要。方针应该确保业务连续性能力在组织文化内得到提高。BCM能力应该整合到组织的变更管理活动中, 以保证BCM能力随着组织产品和服务一起成长和发展。

4.3. 开发业务连续性方针

组织应开发业务连续性方针, 以阐述组织的BCM目标。最初方针只是一个概要的意图表述, 并随着业务连续性能力的开发和提供逐步被优化和提高。

业务连续性方针应该为组织提供文件化的原则, 并致力于业务连续性能力的测量。BCM策略应该由高层管理者负责, 例如, 董事或推举的代表。

组织在开发BCM策略时, 可考虑以下因素:

- 确定组织内的BCM范围;
- BCM资源的获得;
- 为组织定义BCM原则、指南以及最低标准
- 参考任何必须包括或可能用来作为基准的相关标准、法规或政策。

应在组织需要的基础上, 维持和定期评审BCM策略、计划和解决方案。

BCM策略的范围应该清晰说明适用的例外和限制, 如地理的或产品的排除。

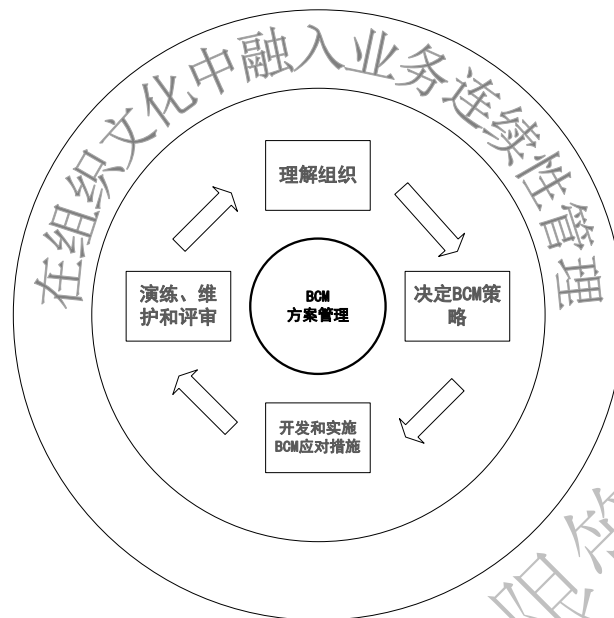
4.4. BCM方案的范围

最高管理层通过识别支持组织目标、义务和法律责任的关键产品和服务，可确定BCM方案的范围。在确定哪些是产品和服务时，应该与条款6.2中描述的业务影响分析相一致。

4.5. 外包的活动

如果产品、服务或活动被外包出去，组织仍需承担该产品、服务或活动的风险责任。从而，组织确保其关键供应商或外包合作伙伴具有就绪的有效的BCM安排。达到上述目的的方式之一是，获得关键供应商生存能力相关的连续性计划以及方案演练和维持的审核证据。

5. BCM 方案管理



方案管理是BCM过程的核心。有效的方案管理建立组织业务连续性的方法。

最高管理层的参与是确保BCM过程正确导入、获得恰当支持和成为组织文化的一部分的关键。

5.1. 概要

BCM方案应该准备就绪，以达到业务连续性方针（参见4.3）中所定义的目标。BCM 方案管理包括以下三个步骤：

- 职责分配（参见5.2）；
- 在组织内实施业务连续性（参见5.3）；
- 业务连续性的持续管理（参见5.4）；

5.2. 职责分配（治理）

5.2.1. 组织的管理层应该：

- 指定或任命一名具有适当资历和权限的人员负责BCM方针及其实施；
- 指定或任命一人或多人实施和维持BCM方案。

注释：

实施和维持业务连续性方案的个别活动，根据组织的规模、范围及复杂程度可能存在于组织的多个领域。然而，具有适当权力的人员（如业主、董事或推举的代表）整体负责BCM，并对保证BCM能力的持续成功负责，是一个基本要素。

5.2.2. 如果组织结构需要，最高管理层可按功能或位置任命跨业务的代表，以协助实施BCM方案。

角色、义务、责任、权力应该与岗位说明和技能要求相结合。

组织的审核过程应对折线职责进行评审。

这些职责可能通过评价、奖励或认可方针等方式来加强。

注释:

在大型组织, 可能需要具有不同角色和责任的业务连续性代表小组。在小型组织, 业务连续性的职责可能分配给单个或多个人员。

5.3. 在组织内实施业务连续性

5.3.1. 实施业务连续性方案的活动应该包括方案的设计、建立和实施。

组织应该:

- 与利益相关方就方案进行沟通;
- 为员工安排或提供适当的培训; 并
- 演练业务连续性能力 (参见条款9)。

5.3.2. 组织可采用经认可的项目管理方法来保证实施得到了有效的管理。

5.4. 持续管理

5.4.1. 概要

持续管理活动应该保证业务连续性融入组织。组织应该对连续性能力的每一组成部份进行定期评审、演练和更新。另外, 当组织的运行环境、人员、过程或技术发生重大变化时, 以及当演练或事故表明 BCM 方案不足时, 应该对业务连续性安排和计划进行评审和更新。

5.4.2. 持续管理

BCM 是非常丰富的, 其活动应基于前期建立和日常运行进行。活动包括:

- 为 BCM 方案定义范围、角色和职责;
- 指定合适的人员和小组来管理持续的 BCM 能力;
- 通过最佳实践, 维持业务连续性方案的适时性;
- 适用时, 扩展业务连续性跨越组织或更大范围;
- 管理演练方案;
- 协调对业务连续性能力的定期评审和更新, 包括风险评估和业务影响分析 (BIAs) 的评审和修订;
- 按组织的规模和复杂性维持文件的适当性 (参见 5.5);
- 监视业务连续性能力的性能;
- 管理与业务连续性能力相关的成本;
- 建立和监视变更管理和后续的管理制度。

5.5. BCM 文件

应该由相应的任务来建立和维持业务连续性文件。BCM 文件可能包括:

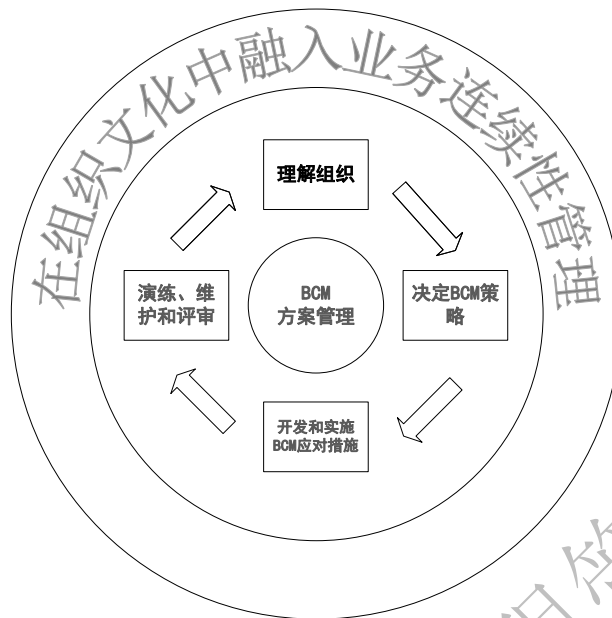
a) BCM 方针:

- BCM 方针的阐述,
- BCM 的职权范围;

b) 业务影响分析 (BIA);

- c) 风险和威胁评估;
- d) BCM 策略;
- e) 提高意识方案;
- f) 培训方案;
- g) 事故管理计划;
- h) 业务连续性计划;
- i) 业务恢复计划;
- j) 演练时间表和报告;
- k) 服务水平协议和合同。

6. 理解组织



BCM生命周期的本要素目的是，通过识别组织的关键产品、服务及用于支持关键产品和服务的关键活动和资源，来理解组织。本要素确保BCM方案与组织的目标、义务和法律责任相一致。

6.1. 介绍

6.1.1. 在业务连续性环境中，从以下方面理解组织：

- 识别组织的目标、利益相关方的义务、法定责任和组织运行的环境；
- 识别活动、资产和资源，包括组织以外支持组织产品和服务交付的活动、资产和资源；
- 活动、资产和资源的失效随时间推移的影响和后果（参见6.2）；
- 识别和评估可能会给组织关键产品、服务，以及支持关键产品和服务的关键活动、资产和资源带来中断的已感知到的威胁（参见6.5）。

6.1.2. 对组织来说，理解以下方面是重要的：

- a) 活动的相互关系；
- b) 对外部组织或其他方的依赖。

6.2. 业务影响分析(BIA)

6.2.1. 组织应确定支持关键产品和服务的活动中断造成的影响，并形成文件。该过程通常被引用为业务影响分析（BIA）。

6.2.2. 在BCM方案范围内，对每一支持关键产品和服务的活动，组织应该：

- a) 评估如果活动中断，随时间推移所造成的影响；
- b) 通过识别以下内容，为每一活动建立最大可忍受期限：
 - 自中断开始，活动需要被恢复的最大期限，
 - 活动需要恢复到的最低水平，
 - 恢复到正常水平的时间跨度；

6.2.2 b) 的注释:

对于中断, 一般影响会随时间推移而加重, 并对每一活动造成不同的影响。影响也会随日期、月份或业务周期点而发生变化。

c) 识别任何相互依赖的活动、资产、用于支持的基础设施和资源, 这些也需要得到持续的维护或随时间进行的恢复。

6.2.3. 在评估影响时, 组织应该考虑与业务目的、目标和相关利益方相关的内容。

这可包括:

- 对员工或公众健康的影响;
- 基础设施、技术或信息损害或丧失所造成的影响;
- 违背法律责任或法律要求的影响;
- 信誉的损害;
- 财政的损害;
- 产品或服务质量的降低;
- 环境损害。

中断所带来的影响的评估方法、发现和结论应形成文档。

6.3. 识别关键活动

组织可能根据恢复的优先级将活动进行排序。在BIA中识别的, 那些活动的丧失将在最短的时间内带来重大影响, 并需要快速恢复的活动, 可被视为“关键活动”。每一关键活动支持一个或多个产品或服务。组织可希望关注关键活动的计划, 但也应该认识到其他活动也需要在中断的最大可忍受期限内恢复, 并需要预先设定安排。

6.3的注释:

根据活动的性质, 最大恢复时间期限可能从几秒钟到几个月不同。时间敏感的活动会需要更高精确的详细说明, 如分钟或小时。低时间敏感的活动精确的要求会较低。

中断的最大可忍受期限在确定BCM策略时(参见条款7), 将影响每一活动的恢复时间点目标。

6.4. 确定连续性要求

组织应该评估每一活动恢复时所需要的资源。这些可能包括:

- a) 员工资源, 包括人数、技能和知识(人员);
- b) 必要的工作场所和设施(基础设施);
- c) 用于支持的技术、厂房和设备(技术设施);
- d) 以前工作或当前工作进展有关信息的提供, 并确保信息的即时更新和精确, 以保证活动在商定的水平上有效持续运行(信息);
- e) 外部服务和供给(供给)。

组织在确定资源水平时, 应考虑相关利益方的需求。

6.4的注释:

在广义上, 技术设施意味着与组织相关的设备使用。技术设施可能包括但不限于, IT 软件和硬件, 通讯设备、车床、食品加工机器、抽真空设备, 或任何制造、生产能力所必要的其他厂房、机器等。

如果记录或工作进展等信息无法获得、不准确、或没有即时更新, 都可能导致妨碍或严重耽搁活动的恢复。在确定BCM策略时, 通常对这些所提供的信息制定合适的备份和记录管理策略。

6.5. 评价关键活动的威胁 (风险评估)

6.5的注释:

咨询组织内或外部的风险注册机构咨询, 可能是有益的。

6.5.1. 在BCM环境中, 应理解风险的级别, 特别是有关组织关键活动及导致关键活动中断的风险。关键活动需要资源的支持, 如人员、设施、技术、信息、供给和利益相关方。组织应理解对这些资源的威胁, 每一资源的脆弱性, 以及当威胁转化为事故并导致业务中断的影响。

6.5.2. 风险评估方法完全是组织自身的决定, 但方法对组织的适用和恰当是很重要的。

6.5.3. BS ISO/IEC 27001 通过描述风险评估过程的必要要素, 为所选择的风险评估方法设定了一个框架。典型要素如下:

- 确定可接受风险准则, 以描述组织倾向于接受风险的情形。
- 定义可接受风险级别。不论组织选择了哪种风险评估方法, 组织都需要定义风险可接受级别。
- 分析风险。组织采用的风险评估方法必须对6.5.4、6.5.5、6.5.6条款中的概念进行处理。

6.5.4. 特定的威胁可能描述为事件, 在某些条件下, 将导致对资源的影响, 如, 火灾、洪水、电力失效、员工短缺、员工矿工、计算机病毒和硬件故障。

6.5.5. 脆弱性可能表现为资源的漏洞, 并在某些条件下被威胁所利用, 如单点失效、不充分的消防防护、电子健壮度、人员配备水平、IT 安全和IT 健壮度。

6.5.6. 影响 (参见6.2.3) 可源自威胁对脆弱性的利用。

6.6. 确定选项

6.6.1. 概要

作为BIA和风险评估的结果, 组织应该识别措施, 以:

- 降低中断的可能性;
- 缩短中断期限;
- 限制对中断组织关键产品和符合的影响。

这些措施被认为是降低损失和风险处理。

降低损失的策略可能结合其他措施, 因为并非所有风险定能够预防或降低到可接受风险级别。组织可包括6.6.2到6.6.5中为每一活动所描述的一个或多个策略。

6.6.2. 业务连续性

如果业务连续定作为关键产品或服务的被选策略, 应建立恢复时间点目标 (RTO), 并对照这一目标对

条款7所描述的连续性策略进行评估。

业务连续性寻求提高组织对中断的健壮度, 保证关键活动按BIA所规定的最低可接受水平和时间框架持续运行或被恢复。

6.6.3. 风险接受

风险可不采取任何进一步的活动, 而被接受。即使是不可接受风险, 但对某些风险能够采取措施的能力有限, 或者采取措施的潜在收益与成本不成比例。在组织的风险偏好内, 如果高层管理人员认为, 风险是可接受的, 在这些情况下, 响应措施可能是忍受现有的风险水平。在某些情形下, 风险的影响可能超出了组织的风险偏好, 但风险发生的可能性较低或风险控制成本不经济, 最高管理层可接受风险。对风险发生的影响处置计划可能作为风险接受的补充。

6.6.4. 风险转移

对于某些风险, 最好的响应方式可能是转移风险。这可通过常规的保险或合同安排来实现风险转移, 或通过向第三方支付费用以其他方式处理风险。该选项对于降低财务风险或资产的风险尤为合适。风险可被转移, 以该组织的减少风险, 或者因为另一个组织是更能够有效地管理风险。注意到某些风险不能(或不能全部)转移; 特别的, 通常不能转移信誉风险, 即使服务交付是外包的。

购买保险可能构成风险处理的一部分, 购买保险可能给部分损失带来一定的财务补偿。但是, 并非所有的损失都是可能保险的(例如, 不确定的事故、品牌或信誉的损失、相关利益如的损失、市场份额的降低或人身后果)。单独的财务处置方法很难如相关利益人所期望的全面保护组织。必要的保险安排通常与一个或多个其它个策略相配套。

6.6.5. 变更、延缓或停止

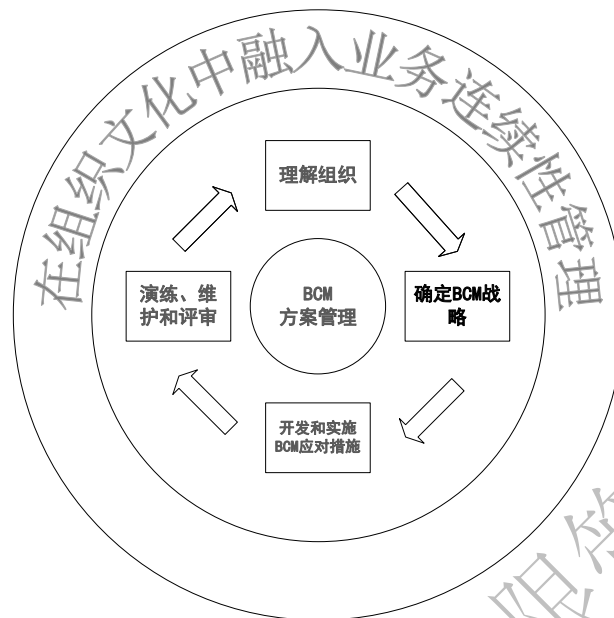
在某些情形, 变更、延缓或停止服务、产品、活动、功能或过程, 可能是合适的方法。该选项应只在与组织目标、法律法规符合性以及利益相关方的期望不发生冲突时考虑。该方法通常对具有有限预期使用期限的服务、产品、活动、功能或过程等时考虑。

注: 以上四项, 有时用“4T”模型予以描述: “Treat”降低风险(业务连续性), “Tolerate”接受风险(接受风险), “Transfer”转移风险以及“Terminate”规避风险。

6.7. 签署

最高管理层应签署关键产品和服务、业务影响分析和风险评估的相关文档, 以保证工作的适当性并反应组织的真实现状。

7. 确定业务连续性策略



“确定业务连续性策略”是BCM生命周期中“理解组织”的后续元素。作为前面分析的结果，组织能够选择合适的连续性策略，使其能够达成目标。

7.1. 介绍

组织用于确定BCM策略的方法应该：

- 实施合适的措施以降低事故发生的可能性或降低这些事故的潜在影响；
- 考虑健壮度和缓解措施；
- 事故中以及事故后为关键活动提供持续性；
- 考虑未被识别为关键活动的其他活动。

注释：

条款7及随后的所有条款都是业务连续性关键产品和服务的选定项。对于其他情形（如中止、终止或风险接受），没有被BC方法所覆盖的服务或产品，将不能视为符合本标准。

7.2. 策略选项

7.2.1. 组织应考虑关键活动的策略选项以及每一活动恢复所需的资源。最为合适的策略将基于一系列的因素，如。

- 关键活动中断的最大可容忍期限；
- 策略实施的成本
- 不采取行动的后果

7.2.2. 策略可能需要以下资源：

- 人员（参见7.3）；

- 基础设施（参见 7.4）；
- 技术设施（参见 7.5）；
- 信息（参见 7.6）；
- 供给（参见 7.7）；
- 利益相关方（参见 7.8）。

对于所有情形，组织在实施业务连续性解决方案是，都应该将同一事故导致业务中断的影响降到最小。

7.3. 人员

组织应识别管理核心技能和知识的合适策略。分析应该从员工扩展到合同工以及其他拥有广泛特殊技能和知识的利益相关方。保护或提供这些技能的策略可能包括：

- a) 关键活动运行方式的文档；
- b) 员工和合同工多种技能的培训；
- c) 分离关键技能，以防止风险集中（这可能是必要的拥有核心技能员工的物理分离或保证超过一人拥有核心技能）；
- d) 利用第三方；
- e) 后续计划；和
- f) 知识的维持和管理。

7.4. 基础设施

组织应该计划降低其正常工作地点不可用所造成的影响的策略。这可包括以下一项或多项：

- a) 组织内的备用场所（地点），包括其他活动的转移；
- b) 由其他组织提供的备用基础设施（不管是否是互为备份）；
- c) 第三方专门机构提供的备用基础设施；
- d) 家庭或远程办公；
- e) 其他商定的合适基础设施；
- f) 在已确定的场所使用备用人力。

7.4的注释：

工作场所策略可能会有很大的不同，并且有很大范围的选项可以选择。不同类型的事故或威胁可能需要实施不同或多个场所的选项。正确的策略是基于组织的规模、行业、活动的范围，基于利益相关方，基于地理位置。例如，政府当局需要在社区提供一线的服务。

注1：如果员工需要转移到备用场所，这些场所不能太远，以使员工愿意并能够到达，并考虑任何因事故可能带来的困难。然而，备用场所也不能太近，而受到同一事故的影响。

注2：应该明确阐明用于连续性目的的备用场所是否只为组织所用。如果备用场所与其他组织共用，应制定减轻这些场所不可用的文件化的计划。

注3：可能转移工作比转移员工更合适，如转移生产线和转移呼叫中心的工作。

7.5. 技术设施

7.5.1. 技术设施策略依赖于组织利用技术设施的性质及技术设施与关键活动的关系，但通常由以下一个或几个方面构成：

- 由组织内部制作提供；
- 交付给组织的服务；
- 由外部第三方提供的服务。

7.5.1的注释：

技术设施策略依据组织的规模、性质、业务的复杂程度有很大的不同。组织应该为交付时间较长的特定或定制技术设施开发特定的策略，以用于保护、替换或恢复技术设施。

组织可能需要在技术服务完全恢复前，采用手工操作方式。

7.5.2. 技术设施策略可能包括：

- 技术设施的物理扩展，如，在不受同一业务中断影响的不同地点维持相同的技术；
- 保留旧设备用于紧急替换或作为备件；
- 为单一或交货时间长的技术设施采取额外减轻风险的措施。

7.5.3. 信息技术（IT）服务通常需要复杂的连续性策略。在需要这些策略时，应该考虑：

- 支持BIA所识别关键活动的系统或应用的恢复时间目标（RTO）；
- 技术设施场所的位置和之间的距离；
- 技术设施场所的数量；
- 远程访问；
- 对应有人工作场所的无人工作场所；
- 通讯的连通性和冗余路由；
- “失效”的性质（需要人工干预以启用备用IT系统，还是自动启用）
- 第三方的连通性和外部连接。

注1：如果采用从一个地点转移到另一个地点的“容错”机制，需要认真考虑两个场所之间的网络路径距离，因为两个地点的物理距离会给IT系统的运行带来负面的影响。

注2：当组织采用多个场所用户存放IT设施，可能需要互融的IT恢复策略，使得每个地点的系统、网络、存储的容量能够应付自身负荷外附加来的流量和工作。

注3：安排人员到备用场所的另一解决方案是通过拨号、通过Internet使用虚拟局域网（VPN）或类似技术提供远程访问。

注4：有关IT和通讯硬件的业务连续性的进一步指南可以参考PAS 77、BS ISO/IEC 27001和BS ISO/IEC 20000（两部分）。

7.6. 信息

信息策略应该保证对组织运行至关重要的信息受到保护，并能按照BIA所描述的时间表得以恢复。

注1：BS ISO/IEC 27001 提供了进一步的指南。信息的保存和恢复必须符合相关法律法规的要求。

交付组织关键活动所需要的任何信息应该具有适当的:

- 保密性;
- 完整性;
- 可用性;
- 流通性

信息策略应该对没有拷贝或备份到安全地点的信息的恢复形成文件。信息策略应扩展到:

- 物理(硬拷贝)格式;
- 虚拟(电子)格式。

注2: 信息需要及时恢复到某一状态点的所有情形, 应告知最高管理层并获得认可。可采用多者不同的拷贝方法, 如电子或磁带备份、胶片、影印、在生产时制作多个拷贝等等。已知恢复点通常是指“恢复状态点目标”

7.7. 供给

7.7的注释: 在办公室环境, 供给可能是支票等。其他的行业可能是库存货、及时(just-in-time)供给, 或交通工具燃料。

7.7.1. 组织应该识别和维持支持关键活动的核心供给的库存。供给的策略可包括:

- 在其他地点存储额外的供给;
- 与第三方达成短时通知交付的协议;
- 转移及时(just-in-time)交付到其他地点;
- 在仓库或运输点保存原材料;
- 将部分运作转移到具备供给的备用场所;
- 识别备用或替代供给。

7.7.2. 当关键活动依赖于特点供给时, 组织应识别关键供应商和单一供应渠道。管理供应连续性策略可能包括:

- 增加供应商数量;
- 鼓励或要求供应商具备有效的业务连续性能力;
- 与供应商签订合同和(或)服务水平协议;
- 识别备选合格供应商。

7.8. 相关利益方

7.8.1. 当确定合适的BCM策略时, 组织应该考虑和保护其关键利益相关方的利益。这些策略应该考虑相关社会和文化的影响。

7.8.2. 组织应该识别合适的策略来管理与关键相关利益方、业务或服务合作伙伴及承包方的关系。每一组可能需要特别考虑。保护关键利益相关方利益的策略可能包括保证利益相关方人身的特定要求, 如, 残疾、疾病或怀孕。

7.8.3. 组织应识别发生事故时, 因人身问题放弃职责的人员。

7.9. 公众紧急事件

7.9.1. 组织应在确定、实施或验证事故管理或业务连续性管理策略的早期, 了解当地官方紧急事件响应机构。这些当地紧急事件响应机构承担其辖区内的公共紧急事件的预计、评估、预防、准备、响应和符合活动。

注释: 在英国, 这些机构可能被认为是当地安防协会。

7.9.2. 关键响应机构将在紧急事件发生发布官方公告, 并提供:

- 事故前或事故后的建议 (如风险评估);
- 警告或告知程序;
- 公共紧急事件发生后的社会恢复安排。

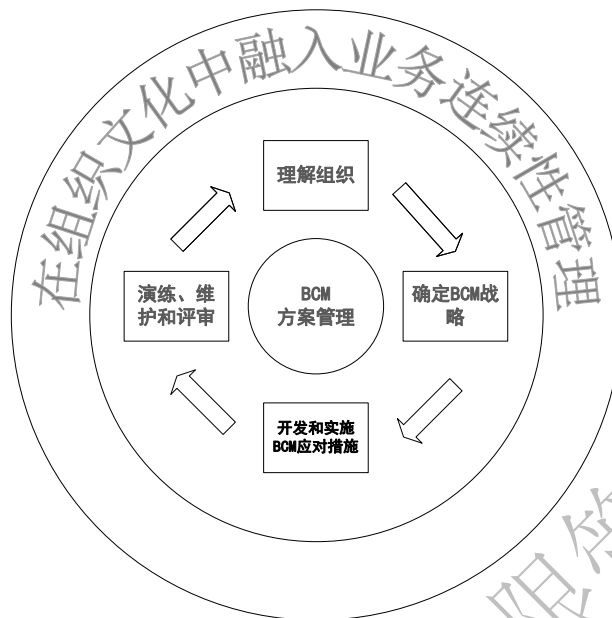
注1: 公共紧急事件可能导致死亡或身体伤害; 将给个人或社区带来心理、社会和经济服务的重大的、长期的影响。紧急事件可能很快导致公众交通、通讯网络、公共设施以及物品、服务和供给的畅通运转的中断。依照中断的潜在可能, 组织应该熟悉当地响应机构的安排计划。

注2: 根据英国公众紧急事件法案 (2004), 当地响应机构在其权限范围内, 应依法向商业和志愿组织提供业务连续性建议和指南。

7.10. 签署

最高管理层应该签署文件化的策略, 以确认连续性策略的确定是合适并与适合中断发生的可能和后果, 而且在组织的风险偏好内, 所选择的策略对满足组织的目标是合适的。

8. 开发和实施BCM响应措施



本BCM生命周期要素是关于开发和实施合适的计划和安排，以保证关键活动的连续性和管理事故。

8.1. 介绍

条款6和条款7阐明了组织应该怎样：

- 识别其关键活动；
- 评估关键活动的威胁；
- 选择合适策略以降低事故的可能性和后果；
- 选择为关键活动提供连续性或恢复的合适策略。

将要计划的威胁范围应该由组织的风险偏好所决定。

8.2. 事故响应结构

8.2的注释：

在小型组织，事故和业务连续性管理的职责可能都单个人承担。大型组织可采用分层的方法，并可建立不同的小组来关注事故管理、业务连续性和业务恢复问题。在某些情形，这些小组可由其他具有相应职责的小组来支持，如媒体沟通和人员问题。

8.2.1. 组织应该定义一个事故响应结构，使组织能够有效响应中断并从中断中恢复。

8.2.2. 任何事故情形，组织都应该有一个简单和快速形成的组织结构，以使组织能够：

- 确认事故的性质和程度，
- 控制事态，
- 处理事故，
- 与相关利益方沟通。

该组织结构应该启动合适的业务连续性响应措施。该组织结构可被称为事故管理小组（IMT）或应急管

- 特定场所;
- 或特定情形,

8.3.2. 目的和范围

每一个特定计划都应该定义目的和范围, 获得最高管理层的认可, 并获得计划实施人员的理解。对组织内所有相关的其他相关计划或文档的引用应该清晰, 并描述获得和访问这些计划的方法。

事故管理、业务连续性和业务恢复计划应该按以下内容进行优先级排序:

- 将被恢复的关键活动;
- 恢复时间表;
- 每一关键活动的恢复水平;
- 每一计划可以被利用的情形。

8.3.2 的注释: 每一计划可以阐明不打算达成的内容和为什么。

8.3.3. 角色和责任

事故发生时或发生后, 具备相应权力的人员和小组的角色和责任 (包括决策和权力的使用) 应该清晰的形成文件。

应该清晰定义计划所覆盖的人员和小组。

8.3.3 的注释: 在适当时, 计划也可以包括支持事故后评审过程的程序和检查表。

8.3.4. 计划的启动

启动事故管理、业务连续性或业务恢复计划的方法应清晰的形成文件。该过程应该使得业务中断发生后, 在尽可能短的时间启动相关计划或计划的相关部分。

组织应该建立在什么样的条件下、谁有权启动计划的清晰指南和准则, 并形成文件。

启动过程可需要立即动员组织资源。计划应包括对以下内容的清晰、准确地描述:

- 怎样动员队伍;
- 立即集合的地点;
- 后续队伍的汇合地点和其他任何替代汇合地点的详细细节 (在大型组织, 这些汇合地点可能是指事故管理或指挥中心)。

组织应该对事故结束并且业务恢复正常后队伍的撤离形成文件化的清晰过程。

8.3.4 的注释:

事故响应中时机的丧失是不可弥补的。抓住时机尽早控制事故并防止扩大, 总是比动员响应队伍然后撤离要好。

组织可要考虑其他专业组织专业指南中所定义的、或国际间达成一致的逐级上报步骤, 如负责流行性疾病的世界卫生组织 (WHO)。

8.3.5. 文件的所有人和维持人员

组织应任命计划的主要责任人, 识别按计划的时间间隔进行评审、修订和更新的人员, 并形成文件。

应该引入版本控制体系, 变更应正式通知到正式计划分发的维持和更新记录中的所有相关方。

8.3.6. 具体的联系方式

每一计划都应该包含或提供所有关键利益相关方的具体的基本联系方式。

8.3.6的注释:

联系记录可能包括“非工作时间”的具体联系方式。当然,提供这些细节的计划,应该首先考虑到数据保护。

8.4. 事故管理计划 (IMP)

事故管理计划(IMP)的目的是为组织对事故早期(爆发时)的管理。

事故管理计划(IMP)应该:

- a) 是灵活、可行和相关的;
- b) 易于阅读和理解;
- c) 为所有可能问题的提供基本的信息,包括在利益相关方和外部问题、事故中组织所面对的问题。

事故管理计划(IMP)还应该:

- 1) 获得最高管理层的知识,适用时包括董事会的支持;
- 2) 具有开发、维持和培训所需的合适资金预算的支持。

8.5. 事故管理计划(IMP)的内容

8.5.1. 总则

在8.3所建议内容之外,事故管理计划(IMP)还应包括8.5.2到8.5.8的信息。

8.5.2. 任务和活动清单

IMP应该包含任务清单和检查表,以管理业务中断的直接后果。这些任务应该:

- 首先处理人员安全;
- 基于组织BIA的结果;
- 按组织选定的策略和战术措施(如条款7所描述)来组织;
- 并帮助防止进一步的损失,或防止关键活动及条款7中所定义的支持资源的损失或不可用。

8.5.3. 应急联系方式

应该包括在什么样的情形下,组织怎样与员工,或其家属、朋友进行沟通,以及紧急联系的方式。在某些情况下,将这些信息放在一个单独的文档中,可能是合适的。

所有人员的亲属或紧急联系信息应维持更新和可用,以备随时所需。

8.5.3的注释:

根据组织的规模和事故的大小,可能需要一定数量的、具有相应能力和经过培训的人员以应对有关事故的电话查询。

8.5.4. 人员活动

IMP应该满足因事故后果可能危及人身安全的人的利益,并考虑社会和文化因素(参见条款7.8.2)。

IMP应识别在事故发生后因人身安全放弃其职责(参见7.8.3)的人员,包括:

- a) 地点的撤离(包括内部“掩体”);
- b) 负责安全、急救或撤离的小组的动员;
- c) 定位和计算现场或现场附近的人员;

d) 持续的雇员/客户的沟通以及安全简报。

组织应安排具备合适权限的人员负责与紧急服务的联络。

注：紧急服务在紧急事故的生命安全保护和伤亡救援方面承担主要任务。因此，组织尽可能早的与一线响应和急救服务机构联络、预先计划和实施事故协调，以提供事故相应的效率。

组织应提供在事故后听取受影响员工汇报和建议的服务渠道。服务可能是外包到组织外部或是延伸现有职业健康和员工救助方案。

8.5.4的注释：

当事故对生命、民生和健康带来直接威胁的，组织对保护员工、合同工、房客和客户生命保护负有直接的责任。

对于残疾人员或有其他特殊要求的人员（如怀孕、因伤而暂时丧失活动能力）应予以特别的关注。满足这些要求的预先计划可以降低风险和消除影响。

不能低估事故的长期影响。开发合适的保护人员健康的策略，可以直接有助于生理和心理的恢复。

8.5.5. 媒体回应

在IMP中应该就媒体回应形成文件，包括：

- a) 事故沟通策略；
- b) 媒体的组织首选窗口；
- c) 事故后尽可能在早期提供给媒体声明的指南和模板；
- d) 任命和授权合适数量的、经过培训的、具有相应能力的发言人，以向媒体发布信息；
- e) 合适时，应建立适当的场所以支持与媒体或其他利益相关团体的沟通。

在某些情形，可适合：

- 在一个独立文件中提供有关支持细节；
- 建立合适数量、经过培训的、有相应能力的人员来回答出版机构的电话询问；
- 准备有关组织和组织运作的背景材料（这些准备发布的信息应该预先商定）；
- 确保所有媒体信息没有不必要的延误。

8.5.5的注释：

预先准备的信息在事故的早期将特别有用。它使得组织在有关事故的详细信息还在建立时，能够提供有关组织及其业务的信息。

组织在事故中或事故后可以利用所有可用的渠道来发布信息。这些渠道可能包括网站、发言人、新闻资源、一般性的公司简报。

8.5.6. 相关利益方的管理

应该包括对其他关键利益相关方沟通的识别和排序程序。可能需要建立一个独立的利益相关方的管理计划，来提供有关排序的准则，并每一（或组）利益相关方分派人员。

8.5.6的注释：

还应考虑来自权利和影响超越组织的团体的压力和社会活动。

8.5.7. 事故管理场所

组织应定义完备的、预先确定用于事故管理的场所、房间或空间。一旦确定, 该场所应该成为组织响应的中心。应该在其他位置确定一个备用场所, 以备主场所不可用之需。每一场所都应该可以使用合适的资源, 以使事故管理小组无延迟的有效启动事故管理活动。

所选择的场所应满足预定的目的, 并包括:

- a) 有效的主、备通讯方式;
- b) 获取和共享信息的设施, 包括对新闻媒体的跟踪。

8.5.7的注释:

事故管理场所提供一个为大家所知的事事故管理中心。获取和共享关键信息, 并设定目标、分配任务、管理资源、识别和跟踪问题、做出明智决策是非常重要的。良好的沟通是基础。使用集合点以克服电话网络的超载。

场所可以很简单, 如宾馆的房间或员工的房子。也可以很复杂, 如专用的“指挥中心”, 并配备有PCs、视频会议系统和多个电话。

最初, 可能需要举行一个虚拟或非现场会议, 例如, 通过电话、电话会议或视频会议, 以尽可能早的作出决定。

8.5.8. 补充

IMP应该包括及时更新的, 联系和动员支持组织响应策略的相关机构、组织和资源的有关细节。IMP应该包括有关事故的日志或重要信息的记录格式, 如事故时间表、人员伤亡的细节、作出的决定、花费、破坏情况估计、沟通问题和组织事故后评审所需的其他基本信息。

IMP还可以包括或引用:

- a) 地图、图表、计划、照片以及其他与事故发生相关的信息;
- b) 如果适用, 包括与第三方(合作方、合同方、供应商等)商定的响应策略的文件;
- c) 设备保存和集结场所的细节;
- d) 场所进入计划;
- e) 索赔管理程序, 确保组织提出的保险或法律索赔符合法律和合同要求。

8.6. 业务连续性计划 [BCP(s)]

业务连续性管理计划(BCP)的目的是使得组织能够在正常业务运作中段时恢复或维持其活动。

BCP被激活(启动)来支持达成组织目标的关键活动。在事故响应的不同阶段, 可能启动整个或部分业务连续性计划。

8.6的注释:

BCP的组成和内容可能随组织不同而不同, 并且内容的详细程度也随组织的规模、环境、文化和技术复杂性不同而不同。

大型组织可能需要针对每一关键活动的独立文件, 而小型组织可能用单一文档覆盖其所有关键活动。

8.7. BCP的内容

8.7.1. 总则

在条款8.3建议之外, BCP还应该包含8.7.2到8.7.5规定的要素。

8.7.2. 活动计划/任务清单

活动计划应该包括结构化的活动检查表以及活动的优先次序, 并列明:

- a) 怎样启动BCP;
- b) 负责启动业务连续性计划的人员;
- c) 决定启动业务连续性计划的人员所有遵循的程序;
- d) 作出启动业务连续性计划决定之前应该咨询的人员;
- e) 一旦决定启动业务连续性计划, 应该被通知的人员;
- f) 谁需要去哪里, 什么时候去;
- g) 可以利用哪些服务, 在什么地方、什么时候可以利用; 包括组织怎样动员外部和第三方资源;
- h) 怎样和合适进行信息的沟通;
- i) 如果需要, 采用人工应对方式的具体步骤和系统恢复等。

8.7.2的注释:

以上内容应符合Civil Contingencies Act (公众紧急法案) 的6.20条款。

计划应参考在策略阶段(参见条款7)所识别的人员、基础设施、技术设施、信息、供给和利益相关方。应该包括任何假定情形和实施计划所需要资源的具体内容。如果因服务或资源缺乏导致计划目标无法达到, 应该有清晰定义的逐级上报程序。

8.7.3. 资源需求

业务连续性和业务恢复所需要的资源应该在不同时间点及时识别。这可能包括:

- a) 人员, 可能包括:
 - 安保,
 - 后勤运输,
 - 必要的福利,
 - 紧急花费;
- b) 基础设施;
- c) 技术设施, 包括通讯;
- d) 信息, 可能包括:
 - 具体的财务信息(如, 薪水册),
 - 客户账号记录,
 - 供应商和利益相关方的相关信息,
 - 法律文件(如合同、保险单、所有权证书等),
 - 其他服务文件(如服务水平协议);
- e) 供给;
- f) 相关利益方的管理和沟通。

8.7.4. 责任人

组织应该识别被任命来管理业务连续性和中断阶段业务恢复的人员。

注释:

在很多情形下, 组织可能愿意任命在事故管理计划中确定的人员来直接管理较长时间内的相关问题。

8.7.5. 格式和附录

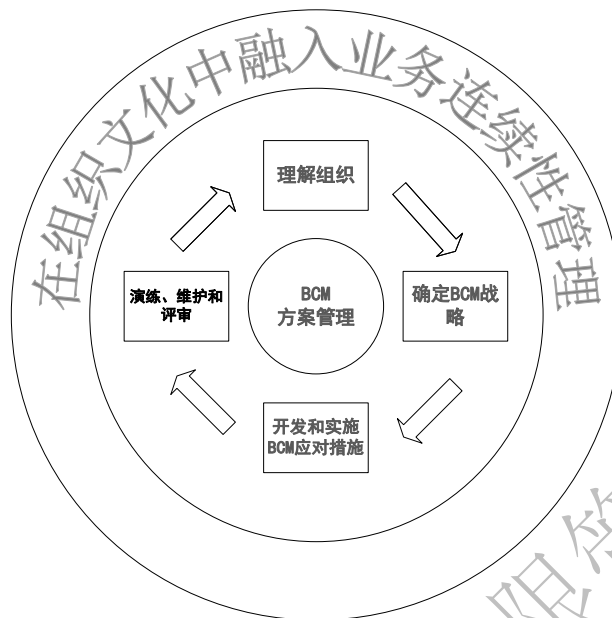
如果适用, BCP 应包括及时更新的、支持组织所内部部相关机构、组织和供应商的具体联系方式。

业务连续性计划应该包括事故的日志或格式, 以记录重要信息, 特别是有关决策的出台。

注释:

计划可能还包括记录管理性数据的格式, 如, 资源的使用、花费的记录材料、地图、图纸以及地点或办公室计划, 特别是与任何备用设施相关的内容, 如工作场所的恢复区和仓储地点。

9. BCM安排演练、维持和评审



BCM生命周期的本要素通过演练、评审确保组织的BCM安排的有效性和及时更新。

9.1. 介绍

除非经过演练并实施维持，否则组织的业务连续性和事故管理安排不能认为是可靠的。演练核心是开发团队合作、能力、信心和知识，这在发生事故时是非常重要的。

9.2. 演练方案

演练方案应与业务连续性计划的范围相一致，并关注相关的法律法规的要求。演练可能：

- 得到预期的结果，如预先的计划和范围；或
- 使组织开发创新的解决方案。

演练方案应在一段时间后，再次规划以确保BCP能按预期工作。方案应该：

- 对BCP技术上的、后勤的、行政的、程序的以及其他系统的运行进行演练；
- 对BC的安排和基础设施进行演练（包括角色、责任，以及任何事故管理地点和工作区域等）；
- 对技术设施和通讯的恢复进行验证，包括可用性和员工的重新安置；

另外，可通过以下来提高BCM能力：

- 从事故恢复中锻炼组织的能力；
- 验证BCP综合了组织的所有关键活动及其相关支持，并按优先级排序；
- 标注有疑问的假定；
- 向演练参与者灌输信心；
- 通过演练的宣传，提高业务连续性意识；
- 确认关键活动恢复的有效性和时间表；
- 证实主响应团队及替补团队的能力。

9.2的注释:

演练为业务连续性和事故管理能力提供可证实的证据。通过BCP 演练时间和资源的消耗证明BCM策略满足预定目的的能力。

不管BCPM策略或BCP看起来是怎样的精心设计和慎重考虑,一系列强有力的和现实的演习将查明需要修订的领域。

9.3. BCM 安排的演练

9.3.1. 演练应该是实际的、经过周密的计划,并获得利益相关方的认可,以使演练过程中业务中断的风险最小。演练应经过计划,以使得因演练直接导致事故的风险最小。

9.3.2. 每次演练都应清晰定义目的和目标。演练后的简报和分析应考虑目的和目标的达成。演练后应该形成包含建议及实施时间表的报告。

9.3.3. 演练的规模和复杂程度应该与组织的恢复目标相适应。

9.3.4. 业务连续性或事故管理计划应该进行演练,以保证其能够得以正确执行,并包含合适的细节和指南。

9.3.4 的注释:

演练所表明的BCP中的不足和错误,在纠正措施完成之后,应该重新测试。

表1列出了BCM策略演练的一系列方法。

表1 BCM策略的演练方式和方法

复杂程度	演练	过程	变更	最佳频次 ^{A)}
简单	桌面检查	内容的评审和修订 质询BCP的内容	更新/确证 审计/验证	至少每年一次 每年
中等	逐步浏览计划	质询BCP的内容	包括互动和确认参与者角色	每年
	模拟	使用“虚拟”情形来确认BCP 包含成功恢复所必要的和充分的信息	与相关计划整合	每年或一年两次
	演练关键活动	启动一个可控的、不会危及业务正常运作的情形	定义一段时间内在备用场所的运作	每年或更低
复杂	全面演练BCP, 包括事故管理	大楼/园区/不包括区域范围的演练		每年或更低

^{A)} 演练的频次应该依据组织的需求、其运行的环境、相关利益方的要求。然而,演练方案应该是灵活的、并考虑组织的变化和以前演练的结果。以上的方法可用于计划的组成部分、单个或多个计划。

9.3.5. 演练方案应该考虑所有参与方的角色,包括关键第三方供应商、外包合作伙伴和被期望参与到恢复活动的其他各方。组织可在其演练中包括以上各方。

9.4. 维持BCP安排

应建立清晰定义和文件化的BCM维持方案。该方案应该保证对任何影响组织的变更（内部的或外部的）及其与BCM的关连性进行评审。还应该识别需要包括到BCM维持方案中的新产品、服务及其所依赖的活动。

作为BCM维持方案的结果，组织应该：

- 评审和质询整个组织BCM任何部分所作出的假定；
- 通过正式的变更控制过程向关键人员分发、更新、修订或变更BCM方针、策略、解决方案和计划。

注：如果有重大的业务变更，则需要修订BIA。BCM方案的其他部分也应进行修订以考虑这些变更。

BCM维持过程的输出，应该包括：

- 组织业务连续性方案预先管理和治理的文件化的证据；
- 验证实施BCM策略和计划的关键人员得到了培训，并具备相应的能力；
- 验证组织所面临风险的跟踪和控制；
- 组织结构、产品和服务、活动、意图、员工和目标的实质变化已经整合到组织的业务连续性和应急管理计划中的文件化的证据。

9.4 的注释：

BCM管理过程的目的是保证组织的BCM能力维持有效、满足预定目的和持续更新。

当策略、解决方案和业务过程发生重大变化时，应该改变现有的演练进度。

9.5. 评审BCM 安排

9.5.1. 组织的最高管理层应该在合适的时间间隔评审组织的BCM能力，以保证组织的连续性的适宜、充分和有效。评审应形成文件。

9.5.2. 评审应验证BCM方针的符合性，以保证符合适用的法律、标准、策略、框架和最佳实践的指南。

9.5.3. 评审应处理依据演练结果所需要的方针、策略、目标和BCM管理体系其他要素的变更，环境变化的以及保证持续改进所需要的任何可能的变更。

9.5.3的注释：

在持续改进的环境下，组织可能获取BCM相关的新技术和实践，包括新工具和技巧。需要对这些新技术和实践进行评估，以使组织获益。

9.5.4. 评审可以采用内部或外部审核，以及自我评估的方式。频次和时间的选择可能依据组织的规模、性质和法律地位，因法律法规的要求而变化；也可能受利益相关方要求的影响。

组织的BCM方案的审核或自我评估应该验证：

- 组织BCM策略内的所有产品和服务及其支持的关键活动和资源得到了识别；
- 组织的BCM方针、策略、框架和计划准确反映了优先次序和要求（组织的目标）；
- 组织的BCM能力是有效的，满足预定目的，并能够管理、指挥、控制和协调事故；
- 组织的BCM解决方案是有效的，更新及时，满足预定目的，并适合于组织所面临的风险；
- 组织的BCM维持和演练方案得到了有效的实施；

- BCM策略和计划整合了事故、演练和方案维持中识别的改进措施;
- 组织具有BCM培训和提高意识的持续方案;
- 就BCM程序与相关员工进行了有效沟通, 并且这些员工理解其自身的角色和职责;
- 设置有变更控制过程, 且运行有效。

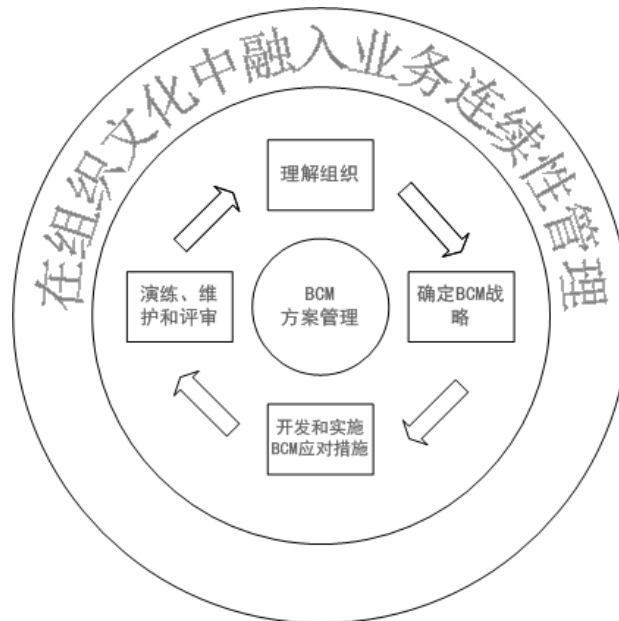
9.5.5. 审核

组织应对其BCM能力进行独立审核, 以识别当前和潜在的缺陷。组织应建立、实施和维持审核的过程。不管是内部审核, 还是外部审核, 独立审核都应该由具有相应能力的人员实施。

9.5.6. 自我评估

BCM 自我评估过程承担保证组织具备健壮、有效和满足预定目的的BCM能力的任务。它为组织从事故中恢复的能力提供定性的验证。自我评估应针对组织的目标进行, 并考虑相关的行业标准和最佳实践。

10. 在组织文化中融入业务连续性管理



要取得成功，业务连续性必须成为组织的一部分，不论规模大小或行业。在BCM过程的每一个阶段，都存在引入和提供组织的BCM文化。

10.1. 总则

在组织内建立、改进和融入BCM文化，使其成为组织的核心价值和有效管理的一部分。

具有积极BCM文化的组织会：

- 更有效的开发BCM方案；
- 向其利益相关方（特别是员工和顾客）灌输组织处理业务中断能力的信心；
- 通过确保各个级别的决策中对BCM影响的考虑，随着时间其健壮度得到提升；
- 使中断的可能性和后果降到最低。

通过以下发展BCM文化：

- 组织高层人员的领导；
- 职责的分配（参见5.2）；
- 意识的提高；
- 技能培训；
- 演练计划。

10.1的注释

在组织内建立和融入BCM的文化，可能是一个漫长而艰难的过程，其中可能会遇到一定程度的没有预期到的阻力。

理解组织的现有文化将有助于发展合适的BCM文化方案。

所有员工都必须理解BCM对组织是一个重要问题，他们在维持向客户和顾客提供产品和服务中发挥重要作用。

10.2. 意识

该组织应该有一个过程，识别和传达BCM意识的要求，并评价传达的有效性。

BCM员工应该让自身了解外部BCM信息。可通过配合从紧急服务机构、地方当局和监管机构寻求指导来达到。

组织应该通过维持一个面向所有员工的持续BCM教育和通报方案来提高、强化和维持意识。

方案可包括：

- 在整个组织内就有关BCM方案的实施，与员工的咨询过程；
- 组织内讨论BCM的通讯、简报、归纳方案或期刊；
- 在相关网页或内部互联网上包含BCM内容；
- 从内、外部事故中学习；
- BCM作为小组会议的一项；
- 在备用地点（如恢复地点）演练连续性计划；
- 参观任何指定的备用地点（如恢复地点）。

组织可将其BCM意识延伸到其供应商和其他利益相关方。

10.2的注释：

提高和维持所有组织员工的BCM意识对员工理解BCM对组织为什么重要是很重要的。需要向员工表明这是一个持续主动的过程，并得到最高管理层的支持。

10.3. 技能培训

组织应该有一个过程来识别和交付相关参与方的培训需求，并评估培训交付的有效性。

组织应该承担的培训：

a) BCM员工的任务，如：

- BCM方案管理，
- 执行业务影响分析，
- 开发和实施BCP，
- 运行BCP演练方案，
- 风险和威胁评估，
- 媒体沟通；

b) 非BCM员工在事故响应或业务恢复中所要完成的指定任务。

应该通过实用的培训，包括在演练中积极参与，在全组织内发展响应技巧和能力。

参考书目

标准

BS EN ISO 9000, *Quality management systems – Fundamentals and vocabulary*

BS ISO/IEC 20000 (both parts), *Information technology – Service management*

BS ISO/IEC 27001, *Information technology – Security techniques – Information security management systems – Requirements*

PAS77, *IT Service Continuity Management*

其他出版物

The Civil Contingencies Act 2004, London: TSO