ICS 13.200
A 90

中华人民共和国国家标准

GB/T 31595—2015/ISO 22313:2012

公共安全　业务连续性管理体系　指南

Societal security—Business continuity management systems—Guidance

(ISO 22313:2012,IDT)

2015-06-02 发布　　2016-01-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准使用翻译法等同采用 ISO 22313:2012《公共安全　业务连续性管理体系　指南》(英文版),仅有编辑性修改。

与本标准中规范性引用的国际文件有一致性关系的我国文件如下:

——GB/T 30146—2013　公共安全　业务连续性管理体系　要求(ISO 22301:2012,IDT)

本标准由全国公共安全基础标准化技术委员会(SAC/TC 351)提出并归口。

本标准起草单位:中国标准化研究院、中国信息安全认证中心、广发银行、招商银行。

本标准主要起草人:王金玉、秦挺鑫、魏军、林德明、董晓媛、高旭磊、邢立强、杨正科、尤其。

引　言

总则

本标准在适当时为 ISO 22301:2012 的要求提供指南，并提供与要求相关的推荐(宜)和允许(可)建议。为业务连续性的各个方面提供通用指南不是本标准的意图。

本标准和 ISO 22301 虽标题相同但并不是重复业务连续性管理体系要求、相关术语和定义。组织希望了解上述内容请参照 ISO 22301 和 ISO 22300。

本标准使用的示图是为了进一步澄清和解释关键点。这些示图只为说明目的，相关内容优先参考标准正文。

业务连续性管理体系(BCMS)强调以下重要性：

——了解组织的需求和建立业务连续性方针与目标的必要性；

——实施和运行控制以及实施和运行措施来管理组织应对中断事件的整体能力；

——监视和评审 BCMS 绩效和有效性；

——基于目标测量的持续改进。

业务连续性管理体系与其他管理体系类似，也包括以下关键因素：

a) 方针；

b) 有明确职责的人员；

c) 与管理过程相关的：

1) 方针；

2) 策划；

3) 实施和运行；

4) 绩效评估；

5) 管理评审；

6) 改进。

d) 一套可提供审核证据的文件；

e) 任何与组织相关的业务连续性管理体系过程。

业务连续性对一个组织而言是特定的，但在执行过程中可能要涉及到其他的群体和第三方。一个组织很可能有他依赖的和依赖他的外部组织，业务连续性有助于构建更具弹性的社会。

策划-实施-检查-改进 PDCA 模型

本标准采用“策划(Plan)-实施(Do)-检查(Check)-改进(Act)”(PDCA)模型来策划，建立，实施，运行，监视，评审，保持和持续改进组织 BCMS 的有效性。

图 1 说明了 BCMS 如何把相关方业务连续性管理要求作为输入，并通过必要的措施和过程，产生满足这些要求的连续性输出(例如受控的业务连续性)。

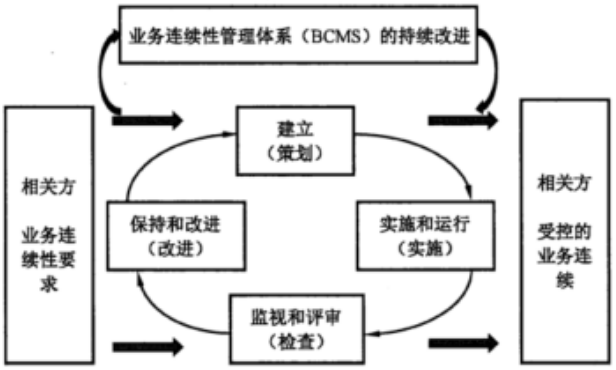

图 1　应用于 BCMS 过程的 PDCA

表 1　PDCA 模型的解释

策划 （建立）	建立与改进业务连续性管理相关的业务连续性方针、目标、控制措施、过程和程序，以提供与组织的总方针和目标相一致的结果
实施 （实施和运行）	实施和运行业务连续性的方针、控制措施、过程和程序
检查 （监视和评审）	对照业务连续性方针和目标，监视和评审业务连续性的绩效，并将结果报告管理者以供评审，确定和授权纠正和改进措施
改进 （保持和改进）	基于管理评审以及重新评审的业务连续性管理体系的范围、方针和目标的结果，采取纠正措施，以持续改进 BCMS

本标准中 PDCA 组成部分

本标准中各章节和图 1 内容间对应关系如下表所示：

表 2　PDCA 模型与第 4 章到第 10 章之间对应关系

PDCA 组成部分	与 PDCA 组成部分对应的章节
策划 （建立）	第 4 章（组织环境）阐述了组织做什么以确保满足 BCMS 要求，并考虑所有相关的外部和内部因素，包括： ——相关方的需求和期望； ——法律法规责任； ——BCMS 所要求的范围
	第 5 章（领导力）阐述了管理者在证明承诺、确定方针、建立角色、职责和权力方面的关键作用
	第 6 章（策划）描述建立整体 BCMS 的战略目标和指导原则所需的措施。为业务影响分析，风险评估（8.2）和业务连续性策略（8.3）建立环境
	第 7 章（支持）识别支持 BCMS 所需的关键要素，即资源，能力，意识，沟通和存档信息
实施 （实施和运行）	第 8 章（实施）识别实现业务连续性所需的业务连续性管理（BCM）要素
检查 （监视和评审）	第 9 章（绩效评估）通过绩效测量和评估提供 BCMS 改进基础
改进 （保持和改进）	第 10 章（改进）包括通过绩效评估识别针对不符合所采取的纠正措施

业务连续性

业务连续性是在中断事件发生后，组织在预先确定的可接受的水平上连续交付产品或提供服务的能力。BCM 是实现业务连续性的过程并使组织准备处理有可能妨碍实现其目标的中断事件。

将 BCM 置于管理体系框架和原则下来建立 BCMS，以使 BCM 可控、可评估和可持续改进。

本标准中，业务一词泛指组织为实现其目标、目的或使命而开展的运营和服务。该词本身适用于大、中、小型的工业、商业、公共和非盈利组织。

任何事件，无论大小、自然的、意外的或蓄意的，都可能会使组织的运营及其交付产品和服务的能力发生严重的中断。因此，只有在中断事件发生前而不是发生后实施业务连续性，才能确保组织在所受影响尚未严重到不可接受之前恢复业务的运行。

BCM 包括：

a) 清楚组织的关键产品和服务，以及交付这些产品和服务的活动；

b) 了解恢复活动的优先级及其所需的资源；

c) 清晰地了解活动所受到的威胁，包括这些活动之间的依赖关系，还要知道如果没有恢复这些活动将会带来的影响；

d) 当中断事件发生时，有准备好的经过测试并可靠的计划来重启活动；

e) 确保这些计划得到定期评审和更新，从而使其在各种情况下都有效。

业务连续性在处理突发中断事件（例如，爆炸）和渐进中断事件（例如，流感大爆发）时都是有效的。

能够造成活动中断的事件非常多，其中许多是难以预测和分析的。由于业务连续性关注中断事件带来的影响而不是其产生的原因，所以业务连续性识别出哪些是组织赖以生存的活动，并使组织确定为履行其责任需确保哪些活动的连续性。通过业务连续性，组织能认识到在中断事件发生前需要做什么准备来保护其资源（例如：人、房屋、技术和信息）、供应链、相关方以及声誉。基于该认识，组织能在中断事件发生时务实地采取可能需要的响应，从而能够自信地管理结果并避免造成不可接受的影响。

做好了适当的业务连续性准备的组织还能将高风险转化为机会。

下面两图（图 2 和图 3）试图从概念上来说明在某种情况下业务连续性是如何有效地减轻影响的。两图中所示的各个阶段之间的相对距离并不表示特定的时间尺度。

通过有效的业务连续性管理减轻中断事件的影响——突发中断

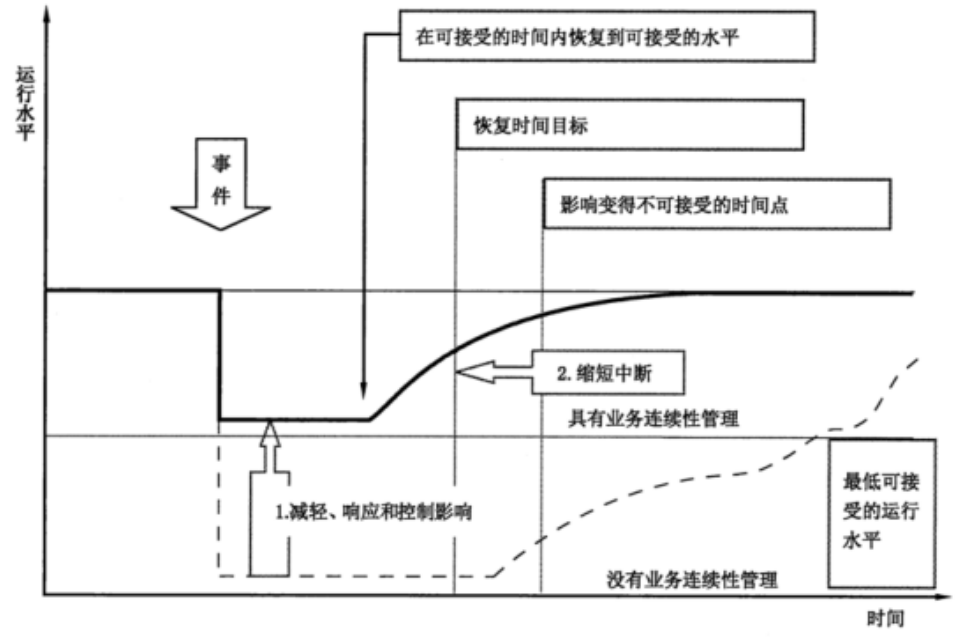

图 2 业务连续性对突发中断有效的图解

通过有效的业务连续性管理减轻中断事件的影响——渐进中断

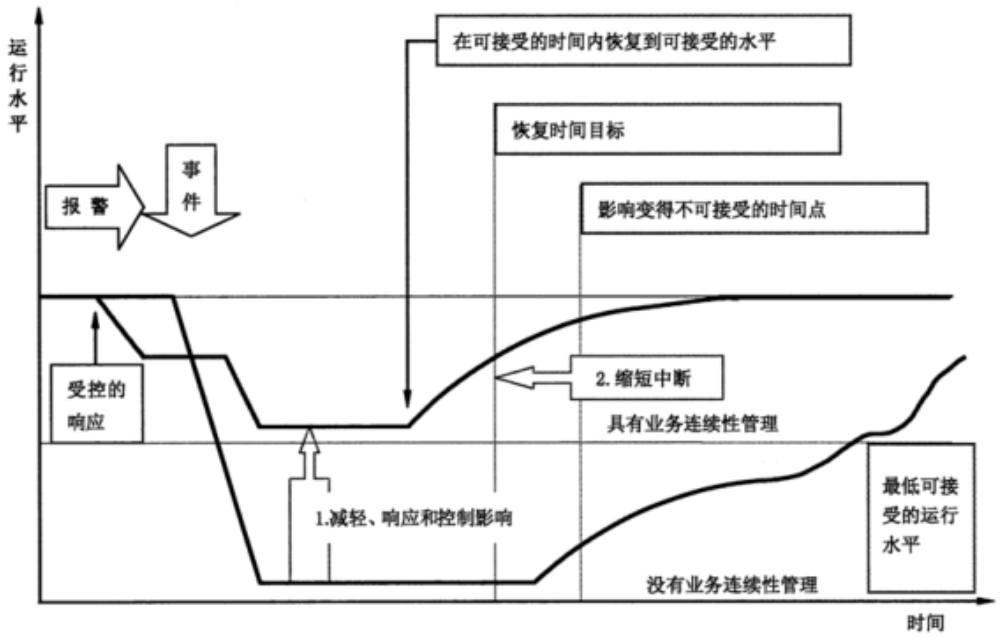

图 3　业务连续性对渐进中断有效的图解

公共安全　业务连续性管理体系　指南

1　范围

本标准基于良好实践，为业务连续性管理体系的策划、建立、实施、运行、监视、评审、保持和持续改进文件化的管理体系提供指南，以使组织能够在中断事件发生时，准备、响应并进行恢复。

本标准目的不是要制定统一的 BCMS 结构，而是为组织设计一个适合组织自身需要和满足其相关方要求的 BCMS。这些需求由法律、法规、组织和行业要求、产品和服务、所采用的过程、运行环境，组织的规模和结构以及相关方的要求等方面构成。

本标准是通用的并适用于包括大、中、小型从事工业、商业、公共和非盈利等所有规模和类型的组织，以期：

a）　建立、实施、保持和改进 BCMS；

b）　确保与组织的业务连续性方针保持一致；

c）　做出符合本标准的自我声明；

d）　本标准不可用于评估组织的能力是否满足其自身业务连续性要求，也不能用于评估是否满足其客户，法律或者法规的要求。组织可以使用 ISO 22301 的要求向其他组织证明其符合性，或者使其 BCMS 通过获得被认可的第三方认证机构的认证。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

ISO 19011　管理体系审核指南

ISO 22300　公共安全　术语

ISO 22301　公共安全　业务连续性管理体系　要求

ISO 22398　公共安全　演练和测试　指南

3　术语和定义

ISO 22300 和 ISO 22301 中界定的术语和定义适用于本文件。

4　组织环境

4.1　了解组织和组织环境

本部分是关于了解建立和管理 BCMS 相关的组织环境。BCM 的建立和管理是 8.1 中的内容。

组织宜评估和了解与其意图和运行有关的内部和外部因素。组织在建立、实施、保持和改进其 BCMS 时宜考虑这些信息并排列优先级。

适当时，评估组织的外部环境宜包括以下因素：

——国际、国家、地区或本地的政治、法律和监管环境；

——国际、国家、地区或本地的社会文化、金融、科技、经济、自然和竞争环境；

——供应链的承诺和关联关系；

——在考虑对风险的内部研究时，将其他相关的信息管理体系和知识管理中更通用的信息考虑在内；
——影响组织目标和运行的关键驱动和趋势；
——组织外部相关方的关系、观念和价值。

适当时，评估组织内部环境宜包括以下因素：
——产品和服务、活动、资源、供应链以及和相关方的关系；
——能力、资源和知识方面条款的理解（例如资本、时间、人、过程、系统和技术）；
——信息体系、信息流和决策制定过程（正式的和非正式的）；
——组织内部相关方；
——方针和目标，以及实现它们的策略；
——未来机会和业务优先级；
——观念、价值和文化；
——组织采用的标准和参考模型；
——组织架构（例如管理，角色和职责）。

4.2 理解相关方的需求和期望

4.2.1 总则

在建立 BCMS 时，组织宜确保考虑相关方的需求和要求。

组织宜识别与其 BCMS 相关的所有相关方，并基于他们的需要和期望确定他们的要求。识别强制的、阐明的和通常隐含的要求很重要。

注：组织需要知道谁是其相关方，比如媒体、附近公众、竞争对手等。

当策划和实施 BCMS 时，识别相关方适用的措施是很重要的，但是这些措施在不同类型相关方之间应有所差别。例如，在中断事件发生后与所有相关方进行沟通可能是合适的，而建立和管理 BCM（8.1.1）与所有相关方进行沟通也许就不合适。

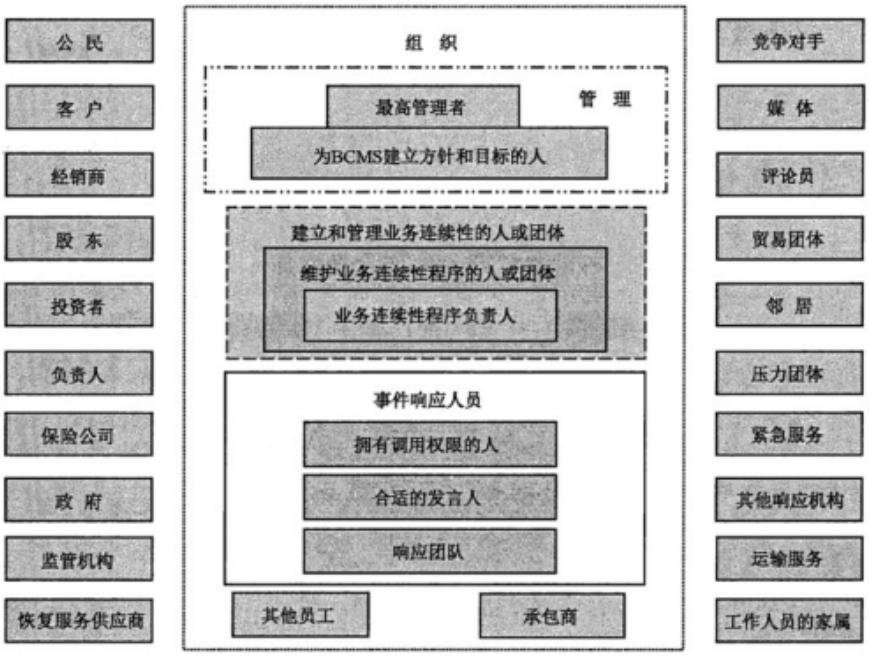

图 4 公共和私有部门需考虑的相关方的示例

4.2.2 法律和法规要求

所有管理体系都宜在组织运行的法律和法规的环境框架下运行。因此，组织宜识别并适应所有与其 BCMS 相关和适用的法律法规要求，这些法律法规是相关方赞成并需要的。

与以上要求相关的信息宜形成文件并保持更新。新的或变更的法律法规和其他要求宜被传达给员工和其他相关方。

在建立、实施和保持 BCMS 时，组织宜考虑适用的法律要求、第三方要求和相关方要求并形成文件。

组织宜确保其 BCMS 能在其法律义务及相关方要求内运行，并支持其法律义务及相关方的要求。

组织宜评审其所在地当前的及待定的法律法规要求，可能包括：

a) 事件响应：包括应急管理、健康、安全和权益法；

b) 连续性：指明方案的范围、响应的程度或速度；

c) 风险：要求定义的风险管理方案的范围和方法；

d) 危害：与危险品存放场所相关的运行要求。

注：多场所经营的组织往往还须满足不同的司法要求。

4.3 确定管理体系的范围

4.3.1 总则

组织宜确定 BCMS 的范围并确保与相关方进行了适当的沟通。特别是，BCMS 的边界和适用性要清晰，同时范围要考虑 4.1 和 4.2 提到的情况。

范围确定了 BCMS 适用的产品、服务、场所、职能、过程和活动。组织所依赖的即使没有明确地识别在范围声明内，也应属于该范围内。例如，如果员工薪酬被指定在该范围内，那么默认情况下，可用资金、管理层批示和给财务部门的支付指示也在该范围内。

组织宜在文件中清晰记录 BCMS 的范围和内容。

4.3.2 BCMS 的范围

组织宜依据其规模、性质和复杂性来确定合适的 BCMS 范围并使之文件化。

范围宜：

a) 识别被包含在 BCMS 内的组织的部分；

b) 在考虑组织的任务、目标、法律责任和内外部义务下，建立 BCMS 的要求；

c) 通过识别所有相关活动、资源和供应链的方式来识别组织的产品和服务；

d) 考虑相关方的需求和利益。

范围还可：

——包括 BCMS 将应对的事件规模和组织风险偏好的说明；

——识别如何使 BCMS 融入组织的全面风险管理战略(如果存在)中。

没有包含在 BCMS 范围内的部分，组织宜记录并阐明原因。

确定范围的目的就是确保覆盖所有相关活动、地点和供应商(8.2.1 图 6)。

4.4 业务连续性管理体系

本节规范性引用 ISO 22301。不提供指南。

5 领导力

5.1 领导力和承诺

整个组织的各级管理者宜证明他们在实现业务连续性方针和目标方面的承诺和领导力。承诺和领导力可以通过激励、鼓励和授权来实现。

5.2 管理承诺

最高管理者宜证明其在 BCMS 方面的承诺。

最高管理者宜对建立和实施 BCMS 并持续改进其有效性所作出的承诺提供证据：

a) 满足适用的法律要求和组织适用的其他要求(4.2.2)；

b) 将 BCMS 过程整合到组织已建立的保持和评审程序；

c) 建立与组织目标、责任和战略方向相一致的业务连续性方针和目标(5.3)；

d) 任命一名或多名具有适当权限和能力的人负责 BCMS 并确保其有效运行(5.4)；

e) 确保建立 BCMS 角色、职责和能力(5.4)；

f) 确保有充足的资源可用，包括适当的资金保障水平(7.1)；

g) 向组织传达满足业务连续性方针和目标的重要性(7.4)；

h) 积极参与演练和测试(8.5)；

i) 确保 BCMS 内部审核被执行(9.2)；

j) 执行有效的 BCMS 管理评审(9.3)；

k) 指导并支持 BCMS 的改进(10)。

也可以通过以下方式证明其管理承诺：

——通过指导组参与运营；

——将业务连续性作为管理会议的常设议题。

5.3 方针

最高管理者宜根据组织的目标和责任确定业务连续性方针并确保：

——符合组织的宗旨(与组织的规模、性质和复杂性相适应并反映组织的文化、依赖关系和运行环境)；

——为目标的制定提供框架；

——包含遵守相关适用要求的明确承诺，包括法律和法规所规定的义务以及 BCMS 的持续改进；

——在组织内部被传达和理解；

——与其他相关的方针相互补；

——管理层批准后，使相关方能够获知。

宜制定适当的规定来审批方针、保存相关存档信息，并定期(如每年度)和当内外部因素发生显著变化时(如最高管理者变更或引入新法规)对方针进行评审。这些规定的适用性取决于组织的规模、复杂性、性质和范围。

方针还宜：

——对组织的业务连续性的范围和边界提供指引，包括纳入管理范围内的和删减的部分；

——识别权力和授权要求，包括负责组织 BCMS 的人员；

——建立被追踪的事件类型和规模的准则；

——包括参考的标准、准则、规则或者 BCMS 宜考虑或遵从的方针。

业务连续性方针可能包括以下内容：

——关键术语；

——资金承诺；

——所参考的其他相关方针；

——实施业务连续性的要求；

——演练和保持业务连续性的承诺。

5.4 组织的角色、职责和权力

最高管理者宜确保在 BCMS 内对职责和权限进行分配和传达。

最高管理者中宜有一人对 BCMS 全权负责。

组织的最高管理者宜任命一名或多名特定的管理者代表，不管该代表是否有其他职责，都宜明确其角色、责任和权力以：

——确保 BCM 的建立、执行和保持与业务连续性方针相一致；

——向最高管理者汇报 BCM 的绩效以便于评审并作为改进的基础；

——在整个组织中提升业务连续性意识；

——确保建立的事件响应程序有效，但未必需要在事件期间参与该程序的实施。

该管理者代表可以：

——被称为“业务连续性经理”；

——在组织中还负有其他职责；

——根据组织的大小、规模和复杂性，归属于组织不同的领域。

可指派来自于组织每个职能部门或区域的代表来协助实施 BCMS。他们的角色、义务、责任和权力宜写入其工作职责描述中，并通过将其纳入组织的评估、奖励和表彰政策而得到加强。

最高管理者可任命其他组织，如指导委员会，来全程监督并持续监控业务连续性管理的实施。

BCM 的所有角色、责任和权力都宜明确、存档并可被审核。

6 策划

6.1 应对风险和机会的措施

组织宜决定如何应对 4.1 提到的因素和 4.2 提到的要求。

宜包括评估需求以策划措施来：

——防止非预期的输出；

——利用一切机会改进 BCMS。

如果有必要还宜包括：

——将这些措施在 BCMS 的过程中进行整合和实施(8.1)；

——如果措施有效，确保存档信息可用以评估(7.5)。

6.2 业务连续性目标和实现计划

宜制定一个建立和管理 BCM 的计划(如第 8 章中所设)，该计划宜包括明确责任并设定恰当和务实的目标，从而完成任务。该计划宜基于组织内部已经设定好的并和相关的职能和层次已沟通过的连续性目标。宜监控并存档计划的进展程序。

随着 BCMS 的发展，该计划宜被审核和定期更新。

以下是业务连续性目标的示例，他们可能在特定的环境下满足 ISO 22301 中提出的要求：

——按期建立符合 ISO 22301 要求的 BCMS；

——按期通过 ISO 22301 认证；

——我们将按期建立符合关键客户合约的业务连续性；

——按期建立 BCM 以保护关键产品和服务。

7 支持

7.1 资源

7.1.1 总则

组织宜确定并提供 BCMS 所需的资源，这将：

a) 实现其业务连续性方针和目标；

b) 满足组织变化要求；

c) 能就业务连续性管理体系有关方面进行有效的内外部沟通；

d) 为业务连续性管理体系的持续运行和持续改进提供支撑。

这些资源宜以一种及时和有效的方式提供。

7.1.2 BCMS 资源

当识别 BCMS 要求的资源时，组织宜提供适当的：

a) 人员以及与人相关的资源，包括：

1) 达到 BCMS 角色和职责所需的时间；

2) 培训、教育、意识和演练；

3) BCMS 人员的管理。

b) 设施，包括适当的工作场所和基础设施；

c) 信息通信技术(ICT)，包括支持有效和高效方案管理的应用程序；

d) 对所有形式的存档信息的管理和控制；

e) 与相关方进行沟通(见图 4)；

f) 财务和资金。

资源及其分配宜定期评审以确保资源充足。该评审最好有最高管理者的参与。

7.1.3 事件响应人员

组织宜任命具有必要责任、权力和能力的事件响应人员来管理事件。

事件响应人员宜形成团队来负责管理任何对组织有显著影响或潜在显著影响的中断事件。

根据这些人员已被证实的处理不同方面的事件响应的能力将他们分组，例如：

——事件管理/战略管理(8.4.4.3.1)；

——沟通(8.4.4.3.2)；

——安全和权益(8.4.4.3.3)；

——挽救和安保(8.4.4.3.4)；

——恢复活动(8.4.4.3.5)；

——ICT 的恢复(8.4.4.3.6)。

宜清晰地确定这些团队中的所有人员在事前、事中和事后所具有的责任和权力。

7.2 能力

组织宜建立一个适当和有效的体系来管理在该体系控制下承担 BCMS 工作的人员的能力。管理层宜确定所有 BCMS 角色和责任的能力要求以及需要达到的意识、知识、理解力、技能和经验。在组织内被分派角色的所有人员宜证明其具有所要求的能力并且提供了培训、教育、发展和其他所需的支持。这可被称作能力发展方案，该方案可包括：

——对所承担的角色进行能力评估；

——建立个人发展方案以确定达到能力所需的培训、教育、发展和其他支持；

——包括挑选适当的方法和资源在内的培训和指导规定；

——知识分享；

——工作分担；

——雇佣有能力的人或与其签订工作合同；

——目标团队的培训；

——对所接受的培训形成文档并监督；

——根据培训需求和要求对所接受的培训进行评估以证明与 BCMS 培训要求相一致；

——根据需要对发展方案进行改进。

组织宜有一套过程来识别和交付所有参与者的业务连续性培训要求，并对其所交付的培训效果进行评估。

适合于具体角色的培训类型可能如下：

a) 建立并管理 BCMS：

1) BCM 的建立和管理；

2) 指导业务影响分析；

3) 风险评估；

4) 沟通技能；

5) 开发和实施业务连续性文档；

6) 运行演练方案。

b) 事件响应和业务恢复：

1) 事件评估；

2) 疏散和就地避难的管理，包括用以清点员工人数的签到过程；

3) 后备工作场所的安排；

4) 处理媒体询问。

组织的响应技能和能力宜通过实际的培训来建立，包括实际参与演练。

响应和恢复小组宜接受与其责任和义务有关的教育和培训，包括与急救人员和其他相关方进行合作。这些小组宜以固定周期接受培训(至少每年一次)，并且宜对纳入响应机制的新成员进行培训。这些小组还宜接受培训来防止事件升级为危机。

商业环境和运营方式的改变会影响业务连续性活动的策划、设计和实施的方式和方法。组织可以通过一定的方法来证明其对业务连续性管理发展趋势的认识，例如实际参与行业 BCM 活动，这些活动可能包括：

——作为行业利益团体成员；

——作为会议筹办委员会成员；

——在会议和研讨会上进行发言；

——参加本地或国际 BCM 会议。

实质性参与可以通过以下一种或多种方式进行证明：

——作为会议或研讨会筹办委员会成员；

——在会议和研讨会上做报告。

通过以下方式可以加强其能力：

——将 BCMS 成就纳入到组织的奖励和认可过程；

——将 BCMS 成就纳入组织的绩效和评价过程；

——将 BCMS 的角色、义务、责任和权力纳入组织的职位描述和技能要求；

——业务操作者和最高管理者要积极参与演习、演练和测试。

组织宜为可能受中断事件影响的所有现有员工建立培训和意识方案，并要求那些为组织工作的承包方证明在其管理下工作的人员具备 BCMS 所要求的能力并能胜任他们所履行的响应角色。

7.3 意识

在组织管理下工作的人员宜对 BCMS 有适当的意识。

这些人员可能包括员工、承包方、供应商。他们宜了解业务连续性方针，并且了解：

——他们与事件预防、检查、缓解、自我保护、疏散、响应、连续性和恢复方面相关的角色和责任；

——遵守业务连续性方针和程序的重要性；

——组织运营的变化所带来的影响；

——他们在 BCMS 有效性方面的贡献，包括改进 BCM 绩效所带来的好处；

——他们在实现其要求中的角色和责任。

组织宜在组织内部建立、推动和融入一种文化，从而：

——使 BCM 成为组织核心价值观和管理的一部分；

——使相关方了解业务连续性方针以及他们在相关程序中的角色。

一个具有积极的业务连续性文化的组织将：

——更有效率地开展业务连续性活动；

——使相关方(尤其是员工和客户)逐渐相信组织有能力处理中断事件；

——通过确保在各级决策中都考虑了业务连续性理念来增强组织的弹性；

——使中断发生的可能性和影响降到最低。

建立业务连续性文化要依靠：

——组织所有人员的参与；

——在整个组织中传播领导力；

——责任分配；

——基于绩效指标的衡量；

——将业务连续性融入组织日常管理实践；

——意识提升；

——技能培训；

——对业务连续性计划进行演练。

意识方案可以包括：

——与组织中所有员工就关于 BCM 建立和管理问题进行讨论的过程；

——在组织内部的通讯、简报、介绍方案或刊物(包括新员工入职培训)中讨论业务连续性；

——将业务连续性纳入相关网页；

——将业务连续性管理纳入员工和管理团队会议的议题；

——对事后报告的选择性公开发布；

——向最高管理者做简报；

——参观选定的备用地点(如一处恢复场所)；

——向关键供应商和经销商简要介绍组织的业务连续性的安排。

7.4 沟通

建立和管理 BCMS 时，组织宜具有与相关方进行信息交换的有效的沟通和协商程序。

该程序宜包括以下所有方面：

a) 相关方之间的内部沟通，包括组织的员工；

b) 与客户、供应商、当地社区和包括媒体在内的其他相关方的外部沟通；

c) 接收、记录并响应来自于所有相关方的沟通信息；

d) 适当时，采用国家或区域的威胁预警系统或其他具有相同作用的系统，并将其纳入到组织的策划和运营中；

e) 确保在中断事件发生期间沟通方式可用；

f) 确保组织能够与外部机构进行沟通，并且适当时，确保与其他组织和人员能相互沟通；

g) 操作并测试通讯能力，为正常通讯中断时使用做准备。

组织可能会邀请可能会参与响应的任何外部资源，如消防、警察、公共卫生和第三方服务商，来与管理层一起评审与其相关的业务连续性程序。

在供应商和客户的通讯和简报里，组织也可以对其 BCMS 和业务连续性的安排进行介绍。

组织宜将有效的外部沟通作为其意识方案的一部分(7.3)，并在事件进展过程中提供有效的外部沟通(8.4)。

7.5 存档信息

7.5.1 总则

存档信息可做为满足要求以及管理体系有效运行的证据。

“程序”一词是指完成某项活动或过程的具体方法。“文件化程序”是指在任何媒介中建立和维护该程序。单个文档也许可以解决一个或多个文件化程序的要求，同时要求的文件化程序可能包括多个文档。

本标准所要求的存档信息包括：

——组织的环境(4.1)；

——法律、法规和其他要求以及符合性证据(4.2.2)；

——BCMS 的范围和与范围有关的任何删减(4.3.2)；

——业务连续性方针(5.3)；

——业务连续性目标(6.2)；

——能力(7.2)；

——业务影响分析和风险评估过程(8.2)；

——业务连续性策略(8.3)，包括供考虑的所有候选策略；

——连续性，事件管理和恢复程序(8.4)；

——事后演练报告(8.5)；

——BCMS 的监视(9.1)；

——内部审核(9.2)；

——管理评审(9.3)；

——不符合和纠正措施(10.1)。

此外，为确保 BCMS 的有效性，存档信息包含以下可能要求的信息：

——客户协议和服务等级；

——业务影响分析的结果；
——风险评估的结果；
——业务连续性策略的确定和选择；
——事件响应概述；
——意识方案；
——与员工和相关方就 BCMS 及事件进行的沟通，如通讯、会议纪要和警报；
——组织和个人的培训方案；
——演练进度表；
——与供应商的合同和服务级别协议；
——承包商和供应商的通知和响应程序；
——检查、保持和校正的证据；
——对已发生的事件和未遂事件的报告；
——BCMS 评审会议记录。

7.5.2 创建和更新

为了满足创建和更新存档信息的要求：
——所有的存档信息宜包括其识别信息和描述信息(如标题、名称、日期、作者、数量、修订说明等)；
——宜指定可接受的格式(如语言、软件版本、图形)并宜清晰描述存档信息的获取和展示媒介(如纸质、电子)；
——所有的存档信息都宜被充分评审和批准。

存档信息的获取和展示宜包括所使用的形式(如语言、软件版本和图形)以及所使用的媒介(如纸质、电子文档)。

BCMS 存档信息的范围可能会根据组织的以下因素而有所不同：
——组织的规模、产品和服务以及所从事的活动类型；
——活动的复杂性及其相互依赖关系；
——人员的能力。

7.5.3 存档信息的控制

所有要求的存档信息都宜受到控制。

控制文档的目的是要确保组织以一种适当并充分的实施和运行 BCMS 的方式创建、维护和保护文件。关注的重点宜为该目的而不是建立一个复杂的文件控制系统。

保护的例子包括防止文件在没有适当授权的情况下被损坏、修改和意外删除。

可以设置不同的访问等级和组合，如只读、读写以及限制阅读。

宜建立一个文件化的程序来确定需要的控制措施以：

a) 分发存档信息；
b) 提供存档信息访问(访问包括，例如，批准和授权查看或更改存档信息)；
c) 在信息发布之前得到充分的批准；
d) 评审以及必要时进行更新和再次批准文件；
e) 确保文件的变更内容及其当前的修改状态得到确认；
f) 确保适用的文件相关版本在使用时的可用性；
g) 确保文件的清晰和易读；
h) 确保组织确定的为策划和运行 BCMS 所必须的来自外部的文件得到识别，并且这些文件的分发受到控制；

i) 避免过期文件的意外使用，并且如果这些文件因为某种原因需要加以保留的话则宜提供适当的识别方法；

j) 设置文件保存和归档的编号；

k) 确保对机密信息的保护和保密。

组织宜确保存档信息的完整性，防止对其进行篡改，进行安全备份，仅限授权人员接触，并谨防损坏、变质和丢失。

组织宜充分满足所有与存档信息保存有关的法律和法规要求，并宜建立、实施和保持满足合规性所要求的过程。

8 实施

8.1 实施的策划和控制

组织宜确定、策划、实施和控制所需的措施，以达成业务连续性方针和目标，并满足适用的需求和要求。

这些措施可能包含建立一个方案，以确保组织的业务连续性得到恰当的管理和有效的保持。

组织宜在该方案中建立控制机制，包括：

a) 决定如何确定、策划、实施和控制这些措施，例如：通过建立一个实施计划并就实施 BCM 的方法论达成一致；

b) 确保这些控制措施按照所做的决定得到实施，例如：设置项目里程碑并明确要求的交付物；

c) 保留存档信息以证明这些过程已按策划得到实施。

组织宜确保策划内的变更受到控制，策划外的变更被审核，并且采取了适当的措施。

8.1.1 BCM 的要素

BCM 包括以下要素，如图 5 所示：

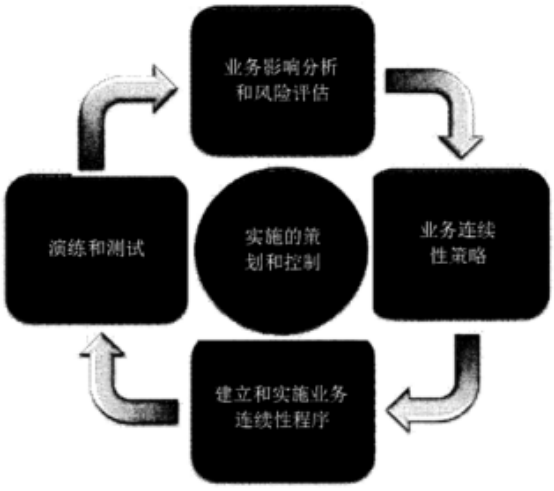

图 5 业务连续性管理(BCM)的要素

这些要素及其在本标准中的位置如下：

a) 实施的策划和控制(8.1)

有效地实施策划和控制是业务连续性管理的核心，它宜由最高管理者任命的责任人来领导。

b) 业务影响分析和风险评估(8.2)

通过业务影响分析(BIA)和风险评估(RA)对业务连续性的优先级和要求达成理解并取得一致。BIA 使组织能确定支持其产品或服务的活动的恢复优先级。风险评估能够提升对优先活动及其从属活动的风险和中断事件的潜在结果的理解。对以上内容的理解使组织能够选取合适的业务连续性策略。

c) 业务连续性策略(8.3)

识别和评估业务连续性策略选择的范围使组织能够选择合适的方法来预防优先活动的中断并处理发生的任何中断。选取的业务连续性策略将能使业务在认可的时间范围内恢复到可接受的程度。所选的业务连续性策略可以在可接受的运行级别和允许的时间范围内为活动的恢复做准备。

注：所选的策略需考虑组织内已有的任何风险处置。

d) 建立和实施业务连续性程序(8.4)

实施业务连续性的安排会建立事件响应机制(8.4.2)、产生监测和响应事件的方法(8.4.3)、产生业务连续性计划(8.4.4)以及恢复到正常业务的程序(8.4.5)。

e) 演练和测试(8.5)

演练和测试为组织提供机会以：

——提升个人意识并发展能力；

——确保业务连续性和业务连续性程序是完整的、最新的和合适的；

——识别机会以改进其业务连续性。

8.1.2 管理 BCM 的环境

对 BCM 环境的有效管理包括：

a) 确保业务连续性的范围、角色和职责持续相关；

b) 适当时，在组织和其他相关方内促进和融入连续性；

c) 管理与业务连续性相关的花费；

d) 在业务连续性管理体系内建立和监视变更管理和继任管理制度；

e) 安排或提供适当的员工培训和意识宣贯；

f) 保持方案文件与组织的规模和复杂度相适宜。

组织 BCM 的安排的每个组成部分，包括文档都宜定期进行评审、演练和更新。当组织的运营环境、架构、场所、人员、过程或技术发生显著变化，或者当某次演练或事件凸显不足时，这些安排也宜被评审和更新。

组织可以采取公认的项目管理方法来确保 BCM 方案得到有效的管理。

8.1.3 保持业务连续性

保持有效的业务连续性宜包括：

a) 通过最佳实践来保持 BCM 的更新；

b) 管理演练方案；

c) 统筹业务连续性计划的定期检查和更新，包括评审或改写一个或多个业务影响分析(BIAs)和风险评估；

d) 确保业务连续性程序的保持适合响应团队的需求。

8.1.4 测量有效性

测量有效性需解决以下两方面：

a) 监视业务连续性的绩效；

b) 监视和评审对外包活动的业务连续性的安排和供应商的 BCM 能力。

可用于测量有效性指标的示例包括：

——活动和资源在其规定的恢复时间目标内是可恢复的并将信息恢复到当前所要求的(恢复点目标);
——用以恢复和重新开始活动的备用地点的场所和设备是可用的;
——证明具备要求的在规定的恢复时间目标内重启优先活动的能力;
——证明具备要求的响应和管理事件的能力。

8.1.5 输出

有效 BCM 的输出指标可包括以下方面:

a) 具有事件管理能力并提供有效的响应;
b) 适当地发展、文件化和理解对组织自身的认识以及与其他组织、相关监管机构或政府部门、本地权力部门和应急服务部门之间的关系;
c) 定期演练以确保受训后的员工能对事件或中断进行有效响应;
d) 相关方的要求被理解并能被交付;
e) 在中断事态中,员工能够得到足够的支持和沟通;
f) 组织的声誉得到保护;
g) 组织符合法律法规要求;
h) 在事件期间,维持财务控制。

8.2 业务影响分析和风险评估

8.2.1 总则

组织宜建立、实施和保持一个正式和文件化的业务影响分析(BIA)和风险评估过程。通过 BIA 和风险评估来了解组织,对组织的了解为有效的业务连续性提供了基础。

组织通过向客户交付产品和服务来达成其目的。因此,认识到这些产品和服务(及相关活动)随着中断时间对组织的目标和运行产生的负面影响是非常重要的。理解相互关系和支持产品和服务的活动的资源要求以及它们所受的威胁也是很重要的。

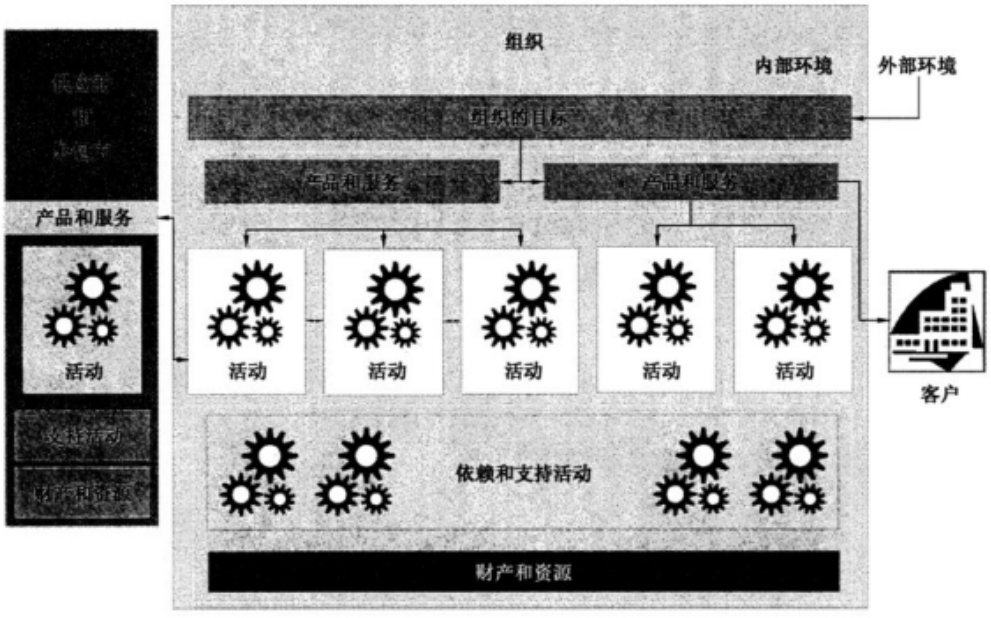

图 6 了解组织

通过了解，组织能确保其业务连续性计划符合其自身意图、法定责任和其对相关方的义务。对组织的了解可以通过业务影响分析和风险评估过程来实现。这些过程可以提供组织确定和选择业务连续性策略(8.3.1)所需要的信息。

BIA 和风险评估宜使组织能够识别措施：

a) 限制中断对组织的影响；

b) 缩短中断的时间；

c) 减小中断的可能性。

宜事先确定并对 BIA 和风险评估的输出格式和评估准则达成一致。宜定期评审所收集的信息，特别是在发生变更期间。

8.2.2 业务影响分析

组织宜建立正式的评估过程以确定连续性、恢复优先级和目标。

BIA 的目的是：

——了解组织的关键产品和服务以及交付这些产品和服务的活动；

——为恢复活动确定优先级和时间；

——识别为了业务连续性和恢复有可能需要的关键资源；

——识别相互依赖关系(包括内部和外部)。

业务影响分析宜包括：

a) 识别支持组织交付关键产品和服务的活动——“关键”意味着这些产品和服务包含在 BCMS 的范围之内；

b) 评估由不受控的非特定事件导致的中断随着时间推移给这些活动带来的潜在影响。评估影响时，组织宜主要考虑那些与业务目标和相关方有关的影响，可能包括：

1) 对员工或公众权益的不利影响；

2) 未尽到法律义务或未满足法规要求而产生的后果；

3) 声誉的损害；

4) 降低财务能力；

5) 产品和服务质量的下降；

6) 环境破坏。

注 1：活动的中断可能会导致产品和服务的交付间接中断。例如，失去为供应商付款的能力可损害组织的声誉，导致供应商拒绝供货，阻止产品生产或服务的交付。

注 2：活动通常都有其日常变化和自然循环。它们通常会随季节变化，也可能会受周末、月末、年末或项目交付日期所带来的高峰期影响。假设中断发生在这些循环期间的最坏时间段，要确保最大可能的影响得到评估。

c) 估算多久与组织活动中断相关的影响变的不可接受；

注 3：影响达到不可接受程度的时间可是几秒钟到几个月，这取决于活动的性质。对于具有时间敏感性的活动需要特定的准确度，如分钟或小时。对于时间敏感性较低的活动可以降低其精确性。

注 4：影响时间变成不可接受可称为“最大可容忍中断时间”、“最大可容忍时间”或“最长可接受中断时间”。组织可接受的最低级别的产品或服务可被称为最小业务连续性目标(MBCO)。

d) 基于对潜在影响的评估，并考虑其他相关因素，在设定的最小可接受级别，为重新开始这些活动设定优先时间；

e) 识别活动间的依赖关系；

f) 识别每个活动所依赖的支持资源，包括供应商和其他相关方。

活动恢复的优先顺序时间表可被称为恢复时间目标(RTO)。RTO 可能需要考虑相关活动之间的相互关系和在活动不能恢复的影响变得不可接受的时间(参照上文 C 部分)。

注 5：在本标准中从现在开始，将采用术语“恢复时间目标”或其缩写“RTO”来代替“优先时间”。

业务影响分析的输出宜被文件化并包括识别：

——产品、服务和活动；

——恢复优先级；

——重要依赖关系和支持资源。

业务影响分析所用的信息可能来自：

——访谈；

——调查问卷；

——研讨会；

——其他内外部来源。

8.2.3 风险评估

组织宜建立一个正式的风险评估过程，对组织优先活动和支撑这些活动的过程、体系、信息、人员、资产、供应商和其他资源中断的风险进行系统的识别、分析和评估。

在决定所要求的进一步处置之前，风险评估在结果和可能性方面为风险分析提供了一个结构性过程。该结构化过程试图解答一些基本问题：

a) 什么可能发生以及为什么会发生(风险识别)？

b) 可产生什么结果？

c) 它们发生的可能性是什么？

d) 是否有办法可能减缓结果或降低其可能性？

该过程需要考虑财务、治理和社会责任。

组织宜了解其活动所要求的资源的威胁和脆弱性，特别是那些：

——高优先级活动要求的；

——具有重要替代的交付时间的。

组织宜选择适当的方法识别、分析和评估可能导致中断的风险。ISO 31000 列出了风险管理的原则和相关指南，本标准宜包含的典型要素如下：

——识别风险：识别组织优先活动和支持这些活动的过程、体系、信息、人员、资产、供应商和其他资源。这些风险可能来自于：

i) 特定的威胁，可被描述为在一些点上中断活动或资源的事态或活动(例如：火灾、洪灾、电力中断、员工损伤、员工缺勤、电脑病毒和硬件故障等)；

ii) 中断事件，可产生于资源脆弱性(如单点故障、消防防护不充分、缺乏后备电力、人员配备水平不足，IT 安全水平和弹性低下)。

——风险评估：评估哪些与中断有关的风险需要处置，宜关注高优先级或重要替代交付时间的活动所要求的资源。

——处置识别：识别可实现业务连续性目标并应符合组织风险偏好的处置(4.1)。

注：如果组织或外部机构已经从事过任何其他的风险分析，这些风险分析将能提供与风险评估有关的信息。

社会需要或监管责任可能会要求组织与部分相关方分享部分风险评估结果。

8.3 业务连续性策略

8.3.1 确定和选择

8.3.1.1 总则

确定业务连续性策略就是从 BIA 和风险评估的发现来识别需要采取的措施，并以某种方式满足组织的业务连续性目标。该措施可能在中断事件之前、之中及之后都需要，例如，可能包括：

——将一条制造生产线拆分到两个地点；

——安装发电机；

——通过缩短中断时间和降低其程度至可接受级别的业务连续性的安排来降低中断事件的总体影响。

业务连续性策略的确定与选择宜基于业务影响分析和风险评估的结果(8.2)。

组织宜确定适当的策略选项来：

——保护优先活动；

——稳定、持续、重启和恢复优先活动；

——缓解、响应及控制影响。

组织宜准备一个机制来评审和批准所推荐的方案。

8.3.1.2 保护优先活动

保护优先活动的目的可能是：

——减少该活动的风险；

——将该活动转给第三方(但责任仍归组织)；

——如有切实可行的替代，终止或改变该活动。

保护优先活动的选项宜根据以下内容来选择：

——已发觉的活动的脆弱性；

——措施的成本与预期收益的比较；

——该活动的紧迫性—由于只有较少的时间来解决问题(可选择的)；

——选项整体的可行性和适用性。

当组织估计一个威胁基本不可能发生或保护优先活动的成本非常昂贵时，组织可选择接受风险，并作为持续的 BCMS 绩效评估中的一部分对该风险进行重新评估(第 10 章)。

8.3.1.3 稳定、连续、重启和恢复优先活动

稳定、连续、重启和恢复优先活动还宜关注其所依赖和支持资源；

业务连续性策略选项可包括：

a) 活动迁移：一些或所有活动转移到组织内部的其他部分，或者转移给组织外的第三方，可以独立进行也可以通过互惠互助协议来进行；

b) 资源迁移或再分配：包括员工在内的资源转移到组织内的另一处地址或另一个活动，或转给外部第三方；

c) 替代过程和备用能力：建立替代过程或在过程和/或库存上创建冗余/备用能力；

d) 资源和技能代替：提升人员能力，包括对重要员工的多技能培训或者通过外包来获得额外的人员能力。替代资源是通过第三方或组织远距离的库存来提供或与外部组织和关键相关方达成双方互助协议来提供临时使用的额外能力；

e) 临时应对方案：某些活动可能会采取不同的工作方式，为在有限时间提供可接受的结果。临时应对方案可能更加费时和/或费力(例如，手工操作不同于自动系统)。因此，临时应对方案通常仅适用于短期或延缓返回正常业务的情况；

f) 考虑活动重启的地点时，业务连续性选项宜包括受损/受影响的地点和未受损的备用地点。

为确保活动可以在其恢复时间目标内重启，还应该为其所依赖和支持资源设定恢复时间目标。设定这些恢复时间目标可能需要考虑：

——在实现全面恢复前的临时阶段提供最小服务的可能性；

——可延缓重启对支持资源的依赖的应对方案(如手工过程);

——恢复丢失数据所需的备用物和时间;

——恢复要求的复杂度和规模,或交付时间长的专业设备的需要。

组织宜评估所有策略选项来确定这些措施是否会带来新的风险。

为稳定、持续、重启和恢复优先活动所选的业务连续性策略通常不能太昂贵。当组织估计该费用太昂贵时,就宜要么选择可接受的替代策略并满足其业务连续性目标,要么将受影响的产品和服务剔除出BCMS的范围作为处置,参照4.3.2。

8.3.1.4 减缓、响应及控制影响

减缓事件的影响和持续时间的选项可包括:

a) 保险:保险的购买可为部分损失提供经济上的补偿,但不能弥补全部损失(例如,未投保事件、商标、声誉、相关方的价值、市场份额和对人力的影响)。仅靠财务清算并不能完全保护组织并满足相关方的期望。保险更多可能会跟其他一种或几种其他策略联用;

b) 资产恢复:与专业的资产清理或修复公司签订在资产损坏后的后备服务合同;

c) 声誉管理:开发有效的预警和沟通能力(8.4.3),并建立有效的沟通程序(8.4.4.3.2)。

8.3.1.5 供应商的业务连续性

组织宜确保供应商业务连续性被评估,组织可能更关注那些如不能交付将立即中断组织优先活动的供应商。方法可包括:

——标书和合同中要求的技术参数;

——供应商计划的定期审核;

——联合进行业务连续性演练。

8.3.2 建立资源要求

8.3.2.1 总则

组织宜确定资源要求来实施所选策略的选项。

组织宜建立:

a) 具有适当权力的合适的团队或个人(对小规模组织而言)来监管事件的准备、响应和恢复;

b) 为服务、人员、资源、材料、生产或捐赠的设施进行定位、获取、存储、分配、维护、测试及记账的后勤保障能力和程序以支持BCMS;

c) 财务、后勤和行政的程序来支持在事件发生前、中、后的业务连续性的安排;

程序宜:

1) 确保财务决策可迅速做出;

2) 与已建立的权限等级、治理和会计原则相一致。

d) 响应时间、人员、设备、培训、设施、基金、保险、债务控制、专业知识、材料的资源管理目标,以及需要从组织资源库和任何供应商那里获取每种资源的时间表;

e) 与相关方的协助、沟通、战略联盟和互助程序。

8.3.2.2 人员

组织宜识别适当的措施来维护、扩充核心技能和知识的可用性,以应对由事件导致员工可用性减少的事态。这些措施宜包括掌握大量专业技术和知识的员工、承包方和其他相关方。保护或提升这些技能的方法可包括:

——后备技术专家的名单及召集计划；
——员工和承包方的多技能培训；
——分散核心能力以减少事件的影响，包括把掌握核心技能的员工分配在多个地点；
——第三方的使用；
——继任计划；
——知识保留和管理的文档过程和其他形式。

事件发生后对员工进行重新安置的程序需考虑：
——员工到另一地点的交通。
——员工在备用站点的需求，如：
i) 住宿；
ii) 餐饮设施；
iii) 个人和家庭义务；
iiii) 不同设备的培训。
——家庭办公带来的挑战。

专家角色可包括：
——安保；
——交通后勤；
——权益和应急。

8.3.2.3 信息和数据

宜保护对组织运营至关重要的信息，并确保其能在业务影响分析中识别的时间表内得到恢复。数据的存储和恢复宜符合相关立法。

注 1：更多确保电子数据传输的指南请参照 ISO/IEC 27031。ISO/IEC 27002 提供了确保数据的持续保密性、完整性和可用性的指南。

组织响应和恢复所要求的任何信息都宜有适当的：
——保密性：例如，活动迁移至另一地点；
——可靠性：信息可靠、可信；
——可用性：活动要求的信息可尽快获取。响应期间所需的信息可能要求立即获得，但其他数据可能在事件发生后一段时间内不需要；
——时效性：按要求及时更新数据，以使活动运行——尽管因事件丢失的数据可能需要重新创建。

所有情况下，活动所要求的信息都宜适当地更新。该时效性通常可被称为恢复点目标(RPO)。数据复制可以采取各种不同的方法，包括电子备份或磁带备份、缩影胶片、影印以及生产时就创建双份。

为了恢复尚未复制或备份至安全地点的信息，信息策略宜文档化。

信息策略宜扩展为包括：
——物理(硬拷贝)形式；
——虚拟(电子)形式等。

注 2：如果备份信息与原信息存储得太近，中断事件可能会影响其可靠性或妨碍数据获取。但是，当该数据需要时，距离远可能会影响其可用性。应有书面的证据表明上述冲突是如何解决的。

与本节有关的信息可能包括：
——联系信息；
——供应商、相关方和相关方的详细信息；
——法律文件(例如合同、保单、所有权证书)；
——其他服务文件(例如合同、服务水平协议)。

8.3.2.4 建筑、工作环境和相关公共设施

工作场所策略的差别可能很大，选择范围也很广。不同类型的事件或威胁可能要求实施不同或多个工作场所选项。恰当的战术部分取决于组织的规模、行业和活动范围，以及相关方和地理位置。例如，公共机构需要维护其在所管辖社区里的一线服务交付，而某些组织却可以在不同的国家或地区进行运营。

组织宜设计策略来降低正常场所不能使用所带来的影响。这一策略可能包括以下一种或几种：

a) 组织内部的备用场所(地点)，包括取代其他活动；

b) 其他组织提供的备用场所(不论其是否属于互助协议)；

c) 应急控制中心；

d) 第三方专业机构提供的备用场所；

e) 家庭办公或远程办公；

f) 其他商定的适宜的场所；

g) 在已建立的场所中使用备用人力。

备用场所宜认真选择，考虑地理位置是否可能会受到同一事件的影响。事件，如自然灾害，可能会导致大范围地区的损毁，影响基础服务，如电力、燃气、供水和通讯。如果存在这种风险，备用场所就宜远离这种可能受影响的区域。

如果员工也要转移到备用场所，这些场所就应足够近，从而使员工愿意并且能够到达那里，还要考虑该事件可能造成的任何困难。但是，备用场所不应太近，以免有可能受到同一事件的影响。

为了连续性目的使用备用场所时，应对备用场所内要求的资源是否属于该组织所独享进行明确的说明。如果备用场所是与其他组织共享，那么组织就应制定并编写相关计划以应对这些场所不可用的情况。

在某些情况下(例如，生产线或呼叫中心)，转移工作任务也许比转移员工合适。这可能会要求备用站点具有备用容量或额外的员工(不管是通过加班或者招募)，以及可用的其他资源。

8.3.2.5 设施、设备和易耗品

组织宜识别和维护支持其优先活动的核心供给品的库存。

某些设施和机器由于非常昂贵(需要很长时间来批准)或者交付时间很长，可能难以获取。提供这类资源的解决方案需要将这些问题考虑在内。改变商业惯例，例如库存控制或建筑管理，也许能提供解决方法。

提供这些的方法可能包括：

——在另一地点存储额外供给品；

——与第三方签订协议，确保可在短期内供货；

——将零库存交付产品分散到其他地点；

——在仓库或货运站存储物资；

——把部件装配业务转移到有物资供给的备用地点；

——确定备用或替代供给品；

——确认各阶段所需的设施和设备，并制定多种备选供货方案。

如果某些活动需依赖专门的供给品，组织宜识别关键供应商和单一货源的供给品。管理供给连续性的策略可包括：

——增加供应商的数量；

——鼓励或要求供应商具备业务连续性能力；

——与关键供应商签订合同或服务等级协议；

——识别有能力的备选供应商。

如果业务活动改换到备用地点，宜确认供应商可以高效地把他们的产品和服务送到备用地点。

8.3.2.6 信息通信技术(ICT)系统

在许多组织内，没有信息通信技术系统业务活动就无法完成，在业务活动重启之前，信息通信技术系统需要先得到恢复。在可能的实际情况下，在进行信息通信技术服务恢复期间，组织也许需要进行手工运行。

技术恢复策略取决于所用技术的性质及其与业务之间的关系，但基本上是下列的一种或多种组合：

——组织内部自建；

——第三方提供给组织的服务；

——组织购买的外部服务。

提供优先活动所需信息通信技术系统的方法可能包括：

——在地理上将它们分散布局，例如，在不会受到同一中断事件影响的不同地点维持同样的技术；

——保留较老的设备，作为紧急情况下的替代品或备用品；

——签署供应设备或恢复服务的合同。

由于所用支持技术的复杂性，信息通信技术系统经常需要复杂的技术方案来确保其得到及时的恢复。因此宜考虑以下事项：

——设置 ICT 系统的恢复时间目标(RTO)，以使优先活动能在其 RTO 范围内重启；

——特别关注各技术站点的位置以及它们之间的距离；

——跨越多个分离站点的分布式技术；

——为远程访问用户的增加提供足够的设施；

——设置无人(暗)站点及有人站点；

——改进通讯的连通性并提高冗余路由的等级；

——采用自动“故障切换”替代要求的人工干预来转移到 ICT 备用系统；

——适应于 ICT 的升级和更新；

——提供额外的第三方通信线路和外部链接。

如果从一个站点到另一个站点之间采用了“故障切换”技术，就需要考虑这两个站点之间的网络通信距离。如果这两个站点之间的距离很远，就可能会降低该系统的响应速度，并导致 ICT 系统失效。

如果组织在不止一个站点拥有 ICT 系统，那就可能有机会实施互备 ICT 策略，其中每一站点的规模应可容纳多个 ICT 合并后的容量要求。

如果组织使用了交付时间较长的特殊或定制的技术，就可能需要考虑通过做好专门进行替换或修复的预先准备来加强其 ICT 的保护。

注：有关 ICT 连续性的更多指导可以参照 ISO/IEC 27031、ISO/IEC 27001 和 ISO/IEC 20000(包括 ISO/IEC 2000-1 和 ISO/IEC 2000-2)。

8.3.2.7 交通运输

事件发生后，需为员工提供交通运输服务：

——当员工平时所乘交通工具不可用时，送员工回家；

——将员工迁移到备用工作地点；

——运送各地所需资源。

组织宜预先决定提供备用交通运输工具的策略，这些交通运输工具在中断事件发生后可能需要用到。它们可能包括：

——识别直接由事件或异常情况引起物流中断的可能情景；

——充分考虑交通条件、运输方式和其他物流网络，保障备用物流方式和路线；

——与交通运输服务商签署服务协议。

8.3.2.8 财务

组织宜确定能确保在中断事件发生期间及发生后仍可提供必要财务服务的策略，可包括：

——提供紧急采购资金，例如食物、住所、设施、消耗品及交通工具；

——员工费用补贴；

——主要费用，例如，租赁或购买办公楼和设备。

为防范滥用保险或促进保险索赔，组织可能有必要通过提供在中断事件发生期间以及发生之后所有花费的正式记录来证明其具备有效的财务控制措施。

8.3.2.9 供应商

如果组织已经将某产品、服务或活动外包，但为该产品、服务和活动所需承担的风险责任却仍然属于该组织。因此，组织宜确保其所选关键供应商已具备有效的业务连续性措施。实现此目标的方法之一就是获取证据来表明关键供应商具备可行的业务连续性计划及演练和保持方案。参见 8.3.1.5。

8.3.3 保护和缓解

对于已确认需要处理的风险，根据组织处理风险的一贯主张，组织宜采取方法减少业务中断发生的可能性、缩短业务中断的时间和限制业务中断的影响。

8.4 建立和实施业务连续性程序

8.4.1 总则

组织宜制定和编写程序来对中断事件的响应进行全面的控制并在恢复时间目标内重启活动。这些业务连续性程序宜建立适当的内外部沟通协议，并且宜是：

a) 具体的——业务中断发生时，宜立即采取的步骤；

b) 灵活的——以便这些程序可用来应对那些未曾预料到的威胁场景和多变的内外条件；

c) 专注的——这些程序宜明确地与那些可能会造成运行中断的事件所带来的影响有关，并且应基于事先声明的前提假设和互依赖性分析来开发这些程序；

d) 有效的——通过实施适当的缓解策略，最大限度地减轻事件所造成的后果。

8.4.2 事件响应机制

组织宜制定程序和一套管理机制来为缓解和有效应对中断事件做好准备。

响应机制宜能：

——确定影响阈值，从而判断是否应启动正式响应；

——评估中断事件的性质和程度，或其可能造成的影响；

——制定措施来提供受影响员工的权益；

——启动适当的响应来应对中断事件；

——为这些响应的启动、运行、协调和沟通制定相关过程和程序；

——获得资源来支持那些用来控制中断事件并把其影响降至最小的过程和程序；

——与相关方，特别是政府机构和媒体进行沟通。

响应机制宜简单，可快速形成。确定该机制时，宜考虑：

——有一名或多名胜任的人员来确定事件的波及面，并评估事件产生的影响或潜在影响及其影响的时间范围；

——能调动团队来进行控制，包括控制事件以及启动适当的响应程序；

——具备适当的资源，包括员工、承包方、设备和资金。

较大的或复杂的组织可使用分级的方式来进行事件响应，可建立不同的团队来专注于事件响应、事件管理、沟通、员工权益及业务恢复。而在较小的组织中，事件响应的所有事务可能仅由一个团队来处理，但决不能只由一个人来承担责任。

每个小组都宜有相关程序来管理其行动，并且需要有一个具有必要的责任、权力和能力的人来负责。个人和小组的能力能通过培训和演练来证明。

8.4.3 预警和沟通

8.4.3.1 总则

组织宜制定、实施和保持用于预警和沟通的程序。这些程序宜包括：

a) 监测事件，并向响应人员发出报警；
b) 对事件持续监控；
c) 在组织内部不同层级和部门之间进行的内部沟通；
d) 与相关方进行的外部沟通；
e) 对来自其他相关方的沟通信息进行接收、记录和响应；
f) 对任何来自国家或地区的风险通告系统或类似系统发出的信息进行接收、记录和响应；
g) 向可能会受到已发生的事件或即将发生的事件影响的相关方发出报警；
h) 确保中断事件发生期间通信方式的可用性；
i) 建立与应急响应部门进行沟通的机制；
j) 确保多个响应部门和人员之间的协调性；
k) 记录有关事件、所采取措施和所做决定的重要信息；
l) 通信设施的运行。

关于预警和沟通程序，组织可能需要决定是否要包含与外部相关方的沟通以及在什么时候进行沟通的内容。在做此决定时，生命安全宜是首先考虑的问题。为此所做的决定及其理由都宜进行书面记录。

例如，一个从事可能会威胁到邻居的危险作业的组织可能需要确保让其邻居知道潜在的危险。这就意味着他们需要知道如何发布警报以及如何进行响应。

组织宜具备有效的程序和设施来发布预警、警报，以及快速地与外部通信。可能需要采取特别的措施与有特殊需要的相关方进行沟通，例如，老人和残疾人。预警和通信系统宜定期进行演练。关于演练的指导可参考 8.5 节。

8.4.3.2 事件沟通程序

在可能的事件发生之前，组织宜建立事件沟通程序，从而能够：

——对来自任何国家或地区的风险通告系统或类似系统发出的信息进行接收、记录和响应；这些信息可能反映了该地区的公共威胁——例如海啸、地震或台风预警；
——向可能会受到已发生事件或者即将发生事件影响的相关方发出警报——该组织有责任或义务进行此报警。

一旦事件已发生，组织宜制定程序来确保：

——对事件进行持续监视，通过现场观察或远程监视，并将新进展传达给相关响应人员；
——建立与应急响应人员进行沟通的机制；
——建立多个响应机构和人员之间的协调性，这也是组织的责任；
——为不同的响应团队和组织之间提供沟通条件；

——与员工或其他负责照顾来访者及承包方的人员进行定期沟通——在疏散开始时，到家或到备用地点后可能都需要进行这一沟通；

——记录与事件、采取的措施和所做的决定等相关的重要信息——记录工作由做出这些决定的人员或者各团队指定的记录员来负责。

这些程序还需促进相关方(例如客户)与媒体之间有效的双向沟通。

组织宜与这些相关方保持沟通，直到业务恢复到正常运营，此时进行一个标志事件结束的沟通是比较恰当的。

8.4.3.3 事件通信设施

可能需要使用某种专用的或特殊的通信设施来辅助这些沟通程序。该设施宜位于离受影响地点足够远的地方，以免该事件影响其运行。该设施也许在同一地点还可以作为其他事件的响应设施。宜确认事件对现有通信设备的正常通信性能可能产生的影响，因此可能需要准备好备用设备，例如：

——扩音器或有线广播；

——备用手机；

——对讲机。

8.4.4 业务连续性计划

8.4.4.1 总则

组织宜制定书面程序，从而使组织能够应对事件，妥善处理其业务活动的重启和恢复。

这些程序宜解决对事件进行响应的所有问题，特别是生命安全问题，以及满足程序使用人员的相关要求。为确定这些要求，可采取以下做法：

——让程序使用人员参与程序的制定；

——利用演练中的反馈结果及从中断事件中吸取的经验教训。

宜根据业务影响分析(参照 8.2.2)所收集的信息来确定恢复时间和性能等级，并选择业务连续性策略(参照 8.3)。

每个计划宜明确以下信息：

——目的和范围；

——优先活动的恢复目标和成功的方法；

——启动的准则和程序；

——实施程序；

——角色、职责和权力；

——沟通的要求和程序；

——内部和外部的依赖关系和相互作用；

——资源的要求；

——信息流和存档过程。

当处理中断事件时，需要考虑很多措施。这些措施都宜包括在书面程序中(参照 8.4.4.2 和 8.4.4.3)，它们包括：

a) 响应并评估事件；

1) 发生了什么事，以及如何发生的？

2) 组织的哪些部分和哪些相关方已经或可能受到影响？

3) 事件预计要持续多长时间及其影响是什么？

4) 常规管理措施能否解决该事件？

b) 评判根据每一程序的启动准则进行事件评估所得到的结果；
c) 当满足启动准则时，宣布事件的发生并启动程序；
d) 稳定事态、连续性、重启和恢复等活动；
e) 建立和运营事件管理场所；
f) 管理事件及其影响时，应对所要完成的事项和活动按重要性进行排序；
g) 控制和协调所有已启动的程序；
h) 启用或建立备用场所，以便用于恢复 IT 系统或其他基础设施，以及用于组织业务活动的临时运行；
i) 监视事件的进展；
j) 根据情况的变化评审和调整计划；
k) 运营能力恢复之后，应逐步停止计划和恢复日常管理；
l) 进行讨论总结并吸取经验教训；
m) 要严格管理、核对和保护事件管理和恢复过程中产生的文件及记录。

为了能让组织交付产品和服务的能力得到及时恢复，恢复每项业务活动的书面程序宜：

——满足支持产品或服务的业务活动的恢复时间目标；

——足够可靠。

这可以通过以下措施来实现：

——拥有或掌控执行这些程序的方法和资源；

——与第三方签订合同、协议或服务等级承诺。

组织可采取预防措施，以确保这些程序的运行不会受到同一中断的影响，例如，将人员和信息通信技术(ICT)分散到多个场所。但是，对所有规模和类型的事件完全进行分散是不可能的，最高管理者宜清楚并同意这一限制。这种限制可以表现为距离远、人员少或情况严重等，这也许可以由处理严重或大范围事件的政府响应机构来决定。

8.4.4.2 业务连续性计划的内容

业务连续性计划可能是一个单一的书面程序，也可能是包含了业务连续性管理体系全部要求并覆盖了业务连续性管理体系所有范围的多个书面程序。

每个书面程序的目的、范围和目标都宜定义清晰，以便程序使用人员能够理解。宜明确这些程序与组织其他要求或相关书面程序和文档的关系，并说明获取和访问它们的方法。

在业务连续性计划中宜明确以下事项(同时参照 8.4.4.3)：

a) 角色和职责
   1) 为使用业务连续性计划的人员或团队定义角色、职责和权力。如果业务连续性计划包含多个书面程序，则每个程序都宜定义角色、职责和权限；
   2) 对于谁有权启动以及什么情况下启动程序，都应有相关准则和标准予以明确——这可以安排在确定事件升级阶段之后。
b) 启动和停止
   1) 在每个程序内，应明确启动组织响应中断事件的过程，以及它的启动准则和程序。还需要考虑程序启动是在工作时间内还是非工作时间内；
   2) 明确事件过后解散各响应团队的过程；
   3) 确定事件发生时的集合场地及备用集合场地。
c) 事件管理

1) 包括管理直接受中断事件影响人员(包括团队成员)的权益问题,管理中断事件的响应措施(这可能包括战略、战术和执行等层级的措施),以及管理防止优先活动进一步损失或不可用;
2) 在每个书面程序里,宜有:
——用来识别需要执行的措施和任务的实施程序,特别是那些关系到在预定时间内组织应如何继续或恢复其优先活动的程序;
——与书面程序有关的资源要求(参照 8.3.2);
——记录关于事件、采取的措施和所做的决定等关键信息的方法。

d) 每个书面程序中的人员联系信息
1) 明确团队成员和其他承担任务和责任的人员的详细联系信息——详细联系信息宜符合当地数据保护法的有关规定;
2) 明确那些可能需要的相关机构、组织和资源的详细联系信息和调动方式。

e) 沟通(参照 8.4.3)
1) 组织如何以及在何种情况下与员工及其亲属、关键相关方以及紧急联络人进行沟通的详细信息;
2) 事件发生后,组织应对媒体的详细说明,包括沟通策略、首选的媒体、起草媒体声明的方针或模板,以及合适的发言人。

8.4.4.3 程序的具体类型

8.4.4.3.1 事件管理/战略管理程序

事件管理的目的是确保组织在战略层面对中断事件的响应是有效的。

事件管理程序宜包括组织在事件中管理可能面临的所有问题的基本内容,包括与相关方有关的问题。

组织宜识别管理事件所需的地点、房间或空间。该地点一旦建立,宜成为组织应对事件的中心。宜在不同地方安排备用会议中心,以防主地点无法使用。每个地点都宜可获得适当的资源,以使事件管理团队可以立即有效地开展事件管理活动。

该地点可采用简易的地方,如酒店房间或者某小组成员的住宅等。该地点也可采用复杂的地方,如配置有个人电脑、视频会议和多方通话的专用指挥中心。起初,可能需要通过电话、远程会议或视频会议的方式召开虚拟或非现场会议,以便迅速作出关键决策。

选定的地点宜符合使用目的并可包括:

——可容纳所需人数的空间;

——有效的主通信和备用通信工具;

——用于访问和共享信息的设施,包括新闻媒体的监控工具。

其他响应团队可能需要类似的设施。

8.4.4.3.2 沟通程序

沟通程序可包括在事件管理响应程序中,也可在适当时由独立团队单独使用。

事件发生期间,有必要主动地管理和协调众多需要发出和接收的沟通信息。该程序宜包括:

a) 如何以及在何种情况下组织需要与员工及其亲属、紧急联络人和其他相关方进行沟通的详细说明;
b) 事件发生后组织的媒体响应的详细说明,包括:

1) 事件沟通策略；

2) 首选媒体；

3) 起草媒体声明的指南或模板；

4) 授权一定数量经过训练、能力胜任的发言人向媒体发布信息。

在事件发生早期，提前准备好相关信息可能会特别有用。在事件详情确定过程中，这些信息可以提供有关组织自身及其业务的相关细节信息。

以下行为可能是适当的：

——建立合适的场所，以便支持组织与媒体或其他相关方进行联系；

——任命一定数量能力胜任的、经过训练的人员来接受媒体的电话采访；

——使用所有对组织开放的沟通渠道，包括社交媒体；

——准备关于组织及其业务的背景材料(此类信息公开前宜获得批准)。

还需要考虑组织可能会承受的压力或那些对组织有较大影响力的社会团体。

另外，还需要包括一个过程来识别需要与其他关键相关方进行的沟通并排列优先次序。可能有必要制定一个单独的程序来管理相关方，提供设定优先次序的标准，并预先为每个相关方或利益相关方团体分配人员。

8.4.4.3.3 安全和权益程序

当事件对生命、生活和权益造成直接危害时，组织对保护员工、承包方、访客和客户的权益负有直接责任，对伤残人士或其他有特殊需求的群体(如孕妇、因受伤而暂时伤残的人士)需给予特别的关注。提前做好规划来满足这些需求可以降低风险，并可使受影响的人安心。事件所带来的长期影响不能低估。制定适当的策略支持人员的权益可直接促进组织内部员工的生理和心理康复，并且这些策略还宜考虑相关的社会和文化因素。

权益响应的要素宜包括：

——现场疏散(包括内部就地避难活动)及集合点；

——调动安全、急救或疏散协助小组；

——找出并清点现场或附近的人员。

还可能包括：

——翻译服务；

——交通帮助，包括所需的指引；

——指定的联络人以及应急服务、相关机构和应急人员的联络信息；

——寻找替岗人员或承包方；

——管理电话救助热线；

——康复及咨询服务(生理和心理)。

事件发生后，组织可能需要保持一种方式来询问和向受影响的员工进行咨询服务并提供长期的支持。这些服务可以外包，或作为已有的职业健康和员工帮扶方案的补充。

组织宜指定具有适当权力级别的人员来负责联系相关的应急服务。在紧急情况下，应急服务在保护生命和减缓伤害方面发挥主要作用。因此，组织事先与急救人员和应急服务部门建立联系，提前进行规划并建立实时协调机制，可以提高事件响应效率。

宜明确识别所有要求的资源。资源宜及时提供并满足其预期功能。宜考虑资源使用的限制，使用资源不宜比未能使用资源带来更多的责任。资源的成本不宜超过收益。

权益响应可能需要的资源包括但不限于以下方面：

——设备的地点、数量、可获得性、可操作性和维护(如重型装备,防护设备,运输设备,监控设备,净化设备,响应设备,个人保护设备);
——供给(如医药,个人保健,消耗品,勤务,冰块);
——能源供给(如电力、燃料);
——紧急电力设备(发电机);
——通讯系统;
——食物和水;
——技术信息;
——衣服和避难所;
——专业人员(如医生,宗教人员,志愿者组织,灾难/应急管理人员,公共事业工作人员、殡葬人员以及私人签约者);
——专业志愿团体(如业余无线电协会,宗教救济组织,慈善机构);
——志愿者,社区和应急响应支持;
——外部的国际、国家、省、部族、区域及本地机构。

8.4.4.3.4 挽救和安保程序

组织可以准备文档化程序来处理挽救和安保。该程序可包括以下方面的指南:
——设施、设备和文档信息的挽救优先级;
——应急服务部门移交工作场所管理权后的安保;
——组织可在事发前指定专门进行挽救工作的承包方。设施、设备和文档信息的有效挽救可以限制事件造成的影响,并能更快地恢复到正常工作。

8.4.4.3.5 恢复业务活动的程序

每个程序宜详细说明:
——需要恢复的优先活动;
——重启的时间段;
——每一项已划分恢复优先级的活动所需的恢复水平;
——该程序适用的情形。
在适宜的情况下,每个程序宜详细说明为实现目标在不同时间点所需的资源。这可包括:
——资源数量;
——技能与资格;
——技术设备;
——通讯设施;
——通过签订互助协议可利用的资源,或其他可能获得的资源。
如果因服务或资源的缺失威胁恢复活动的开展,则宜采取额外的措施。这些措施可以包括:
——调动外部和第三方资源;
——恢复措施之间的沟通;
——实施手工作业、系统恢复或其他备用过程等的程序。
资源要求宜文件化并可包括:
——重要记录(硬拷贝或电子记录);
——操作和程序手册;

——IT 技术恢复计划和程序；
——组织所使用的异地存储设施所在地；
——后备场所；
——应急费用支付的授权；
——作业部门所需的专业技能员工名单；
——IT 基础设施及应用程序文档；
——通信支持的来源；
——办公室及专业设备供货源；
——公共设施(水、电等)联络名单。

8.4.4.3.6 信息通信技术(ICT)系统的恢复

恢复活动的程序宜识别恢复所依赖的 ICT 系统，这涉及到任何现有的 ICT 连续性程序。

如果有 ICT 连续性程序，那么它至少宜解决：

——ICT 响应和恢复程序的启用及 ICT 人员的部署；
——访问备份数据并获取备用服务资源；
——数据、信息服务、通信和支持资源的重建；
——ICT 达到业务连续性程序中所规定的可用性和能力要求的时间表，以使业务活动的恢复满足其恢复时间目标。

注：更多指引详见 ISO 27031。

8.4.5 恢复

组织宜制定书面程序来恢复并将业务运行从事件发生后所采用的临时性措施返回到支持正常的业务要求。并宜满足相关的审核和企业治理要求。

恢复的目的是在事件发生后重建业务活动，以支持正常的业务要求。可通过以下措施来实现返回到正常运行：

——修复事件造成的损害；
——将业务运行从临时场所迁回至修复后的主业务场所；
——转移至新建场所。

决定如何最佳地“返回到正常运行”取决于事件所造成损害的严重程度以及重建必需的设施预计所需的时间。

这些文件化的程序宜提供对事态及其影响的详细评估，以及为了恢复所确定的任务和步骤。在恢复期间，组织可能需要：

a) 建立恢复资源和基础设施；
b) 运转恢复设施；
c) 修复已损坏的设施；
d) 保障紧急采购和资金；
e) 挽救受损设施中的设备；
f) 根据已有保单进行索赔；
g) 增加额外人力来支持恢复工作；
h) 选择重建和返回正常业务运行的方案；
i) 将业务迁回到已恢复的设施中运行；

j) 恢复已丢失的文档信息；

k) 以适当的频次与相关的相关方进行沟通；

l) 在已修复的设施中进行正常运行；

m) 开展恢复后的评审；

n) 根据审核和公司治理要求进行尽职调查。

这些文件化的恢复程序宜包括全部业务活动恢复的条款，并不仅限于已确认的优先活动。这表明那些较低优先级的业务活动也需要在某个时间点得到重启并且也有相关的资源要求(8.3.2)。

8.5 演练和测试

8.5.1 总则

组织的业务连续性程序和在通过演练之前不能被认为是可靠的，除非其得到了及时的维护。演练对于确保充分准备好策略、方针、计划和程序并满足业务连续性目标是必不可少的。演练有助于加强团队协作、能力、自信和知识，并且宜包括那些将要使用这些程序的人。

8.5.2 演练方案

无论业务连续性程序看起来设计得多么好、考虑得多么周到，经过一系列严格而真实的演练后，都会识别出需要改进的地方。

演练方案应与业务连续性程序的范围保持一致，并充分考虑所有相关的法律和法规。

宜定期设计演练方案来证明业务连续性程序和措施在需要时能实现预期的目标。方案宜：

a) 演练业务连续性程序的技术、后勤保障、行政管理、流程和其他运行系统；

b) 演练业务连续性程序中承担责任的所有人员；

c) 演练业务连续性的安排和基础设施(例如，包括事件管理场地和工作区域)；

d) 验证技术和通信的恢复能力，包括人员的可用性及重新安置。

演练的规模和复杂度宜与组织的业务连续性目标相适应。

宜制定演练时间表，其频度宜取决于组织的需要、进行演练的环境及相关方的要求。但是，演练方案宜具有灵活性，需要考虑组织的变化和前期演练的结果。组织发生重大变化时可能会启动演练计划，以检查改变后的措施。

演练方案宜考虑所有参与者的职责，包括关键的第三方服务商、供货商以及其他预计要参与恢复活动的人员。组织安排的演练可以包含上述各方，同时也可以参加由他们所组织的演练。

宜根据组织的经验、资源和能力，使演练方案的范围和具体内容成熟化。因此在成熟度的初期阶段，演练和测试可能限于采用列表检查、训练和意识培训。随着演练方案的成熟，就可以扩展为包括桌面演练和全面真实的模拟演练。

8.5.3 演练业务连续性计划

演练是经过设计的一系列活动，用来检验组织面临特定中断情景时进行响应、恢复和持续有效地完成指定业务功能的能力。组织宜利用演练及演练的记录结果来确保业务连续性计划的有效性并做好准备。

每次演练和测试都宜确定清晰的目的和目标，并通过合适的场景来满足这些要求。

演练可以：

——预设一个预期的输出，例如事先进行演练设计并确定其范围；

——允许组织开发创新的解决方案。

演练宜是真实的，需要认真设计并获得相关参与方的认可，从而使得由该演练直接导致事件发生并

造成业务过程中断的风险降到最小。为实现该要求，在不破坏测试目标的完整性的前提下，可以在受控和隔离的环境中进行演练。

组织宜设计满足演练目标的演练场景，可以利用风险评估中所确认的威胁或其他适当的事件。

业务连续性某些方面的有效性要求特定的人员或担任特定职位的人员具有特定的知识、技能和意识，这些都宜在演练前准备就绪，从而使参与者可以将其应用于相关的场景和模拟中。

演练的设计和执行宜完成以下一种或几种任务：

a) 验证恢复时间目标是可实现的(8.3.1)；

b) 确信业务活动所需的信息得到了适当的更新(8.3.2.3)；

c) 增加对所依赖的供应商和其他相关方的业务连续性的了解；

d) 提高关于组织背景及优先级的意识；

e) 提高对于业务连续性程序的内容及其使用的理解；

f) 提高对事件进行响应的信心；

g) 作为改进组织能力的机会；

h) 评估业务连续性策略的效用及其适用性；

i) 评估已有的能力和配备的资源是否充分；

j) 识别在管理事件和中断的过程中，所用到的以前没有记录在案的要求和惯例；

k) 识别所编写的业务连续性程序及其贯彻执行中存在的不足之处；

l) 保证业务连续性程序在需要的时候是能够执行的；

m) 提高相关方对组织所做准备工作的信心；

n) 作为一种履行法规、合同及组织治理要求的方法。

演练可以有很多不同的形式。演练类型的适用性取决于业务连续性管理的环境、演练的目标、预算和参与者的参与程度，以及组织对举行演练所造成的运营中断的容忍度。

演练的主要类型详见 ISO 22398(公共安全-演练和测试　指南)

作为演练的一部分，应该安排时间让所有的参与人员对业务连续性程序进行评审，讨论存在的问题和经验教训。该评审信息宜被记录在案并按评审结果的要求对程序进行更新。

组织宜在演练后进行总结和分析，评估演练目的和目标的达成情况。演练总结报告宜包括改进建议及执行时间表。

从演练和经历的真实事件中得到的经验教训宜在以后的演练中再次得到检验。那些发现了严重缺陷和差错的演练，宜在纠正行动完成后再次进行演练。

演练和测试的好处包括：

——验证业务连续性计划的范围、假设和策略；

——确保技术设施和资源正确有效；

——确保备用设施的能力；

——提高效率，减少完成过程所需的时间(例如，通过重复训练来缩短响应时间)；

——提高相关方的意识；

——提高演练参与者的能力和意识。

9 绩效评估

9.1 监视、测量、分析和评价

9.1.1 总则

BCMS 的绩效和有效性程序宜包括设定绩效指标、优先活动保护的评估、确认遵守要求、检查历史

证据;并使用存档信息以帮助后续的纠正措施。这些程序也宜参考业务连续性方针和业务连续性目标。

用于监视绩效的程序宜包括以下方面:

a) 设定适合组织需求的绩效指标,包括定量和定性测量指标;

b) 监视满足组织的业务连续性方针和目标的程度;

c) 识别宜何时进行监视和测量;

d) 评估保护优先活动的过程、程序和职能的绩效;

e) 主动进行绩效测量来监视 BCMS 是否符合适用的法律、法规和监管要求;

f) 被动测量监视失效、事件、不符合(包括未遂事件和错误警报)和其他说明 BCMS 存在缺陷的历史证据的绩效;

g) 记录监视和测量的数据和结果,以帮助后续纠正措施的分析。

这些程序宜定期对组织的业务连续性进行系统的测量、监视和评估。组织宜制定一套绩效指标来测量管理体系及其输出。测量可以是定量的也可以是定性的。绩效指标可以是管理方面的、运营方面的,或经济方面的指标。这些指标宜提供有用信息以识别哪些环节绩效良好而哪些环节需要更正和改进。

BCMS 宜提供监视与测量数据,以识别绩效考核模式,并获取绩效信息。宜应用这些数据确保组织的方针和目标能够得以实现,以及识别纠正措施和改进环节。

组织宜能证明其已经识别、评估并遵守了法律要求及承诺遵守的其他要求。

宜保持所有定期评估及其结果的记录。

组织宜分析,并定期评估监视和测量的输出。

9.1.2 业务连续性程序的评价

组织宜对其业务连续性程序进行评估,以确保其持续的适用性、充分性和有效性。

宜通过演练的结果、事件发生后的回顾、环境的变化以及持续改进的承诺的评估,指出 BCMS 的方针、目标、策略及其他 BCMS 要素可能的变更需求。

评估工作可采用内部审核、外部审核或自我评估的形式。评审的频率和时间间隔可能会受到法律法规的影响,并取决于组织的规模、性质和法律责任。还可能会受到相关方要求的影响。

组织的业务连续性程序的评估工作宜验证:

a) 所有的关键产品和服务,以及支撑这些产品和服务的活动和资源都已得到识别,并被包含在组织的业务连续性策略中;

b) 组织的业务连续性方针、策略、框架和业务连续性程序能够准确地反应组织的优先级和要求(组织的目标);

c) 人员的能力和组织的业务连续性是有效并与其目的相适应的,能使组织在响应中断事件时完成管理、指挥、控制和协调工作;

d) 组织的业务连续性解决方案是有效的、得到及时更新的、与其目的相适应的,并与组织面临的风险等级相适应;

e) 组织的业务连续性维护和演练方案已经被有效地实施;

f) 业务连续性策略和程序包含了在事件和演练中以及在维护方案的过程中确认的改进措施;

g) 组织具有持续开展业务连续性培训和意识方案;

h) 已与相关员工就业务连续性程序进行了有效的沟通,并使那些员工已理解他们的角色和责任;

i) 已具备变更控制过程并得到了有效地运行。

组织宜建立一个清晰定义和文件化的维护方案,该方案宜:

——确保任何影响组织的与 BCM 有关的变化(内部的或外部的)都进行了评审;

——识别任何新产品、新服务以及它们所依赖的需要包含在 BCMS 中的业务活动;

——确保组织的业务连续性持续有效、与目标相适应并得到及时更新;

——在任何业务连续性策略或相关业务过程出现显著变化时,使已有的演练进度表得到修订。

注:评估主要业务变化影响的一个有效方式,就是组织尽早评审业务影响分析(8.2.2),并基于输出改变 BCM 的其他要素。

维护过程的输出宜包括:

——对组织的 BCM 进行主动管理和治理的书面证据;

——验证执行业务连续性策略和程序的关键人员经过了培训,并能够胜任;

——验证 BCM 的执行计划和控制;

——证据表明组织已评估其业务连续性程序的合规性;

——证据表明组织在架构、产品、服务、活动等方面的重大变化已经及时反映在组织的业务连续性程序中。

当事件中断了组织优先活动或要求事件响应时,宜进行事后评审。该评审可包括:

——识别事件的性质和原因;

——评估管理层是否对事件进行了充分地响应;

——评估组织是否有效地满足了恢复时间目标;

——评估针对以上事件保障业务连续的人员安排的充分性;

——识别业务连续性的安排需要作出改进的地方;

——将业务实际受到的影响与业务影响分析过程中分析的影响进行比较;

——获取相关方及参与事件响应的各方的反馈。

在不断改进的过程中,组织可能需要学习新业务连续性管理技术和实践方面的知识,包括新的工具和技能。宜对这些新的技能和知识进行评估,以确定它们给组织带来的潜在收益。

所有与定期评估及其结果相关的书面信息都要保持完整,作为评估的证据。

9.2 内部审核

组织宜定期开展内部审核工作,确保 BCMS 满足组织自身的要求及本标准的要求。对 BCMS 开展内部审核工作至关重要,以确保通过内部审核来实现其目标,符合策划安排并已被正确实施和维护,以识别改进的机会。BCMS 的内部审核工作宜定期进行,从而为最高管理者决定 BCMS 适宜性和有效性提供信息,也为 BCMS 绩效的不断改进的目标设定提供依据。

组织宜建立审核方案(参照 ISO 19011)来指导审核工作的计划和实施,并识别要完成审核目标需要哪些审核工作。审核方案宜根据组织业务的性质、风险评估和影响分析、以往的审核结果及其他相关因素来确定。

内部审核方案宜基于 BCMS 的全部范围,但是,每次审核不必覆盖整个体系。审核工作可以分成几个较小部分,只要审核方案能够确保所有组织的单位、功能、活动和体系要素及 BCMS 的全部范围都在组织规定的审核周期之内完成审核工作即可。

BCMS 内部审核的结果可以报告的形式来提供,可用于改正或预防具体的不符合,并为开展管理评审提供输入。

BCMS 的内部审核可以由组织内部的人员来开展,也可以由组织选定的外部人员来执行。不论哪种情况,开展审核工作的人员必须能胜任该审核工作,并能保证公证客观。在较小型的组织里,审核的独立性可以表现为审核人员并不负责所审核的业务活动。

9.3 管理评审

最高管理者宜定期评审组织的BCMS,从而保持其适用性、充分性和有效性,包括使其业务连续性程序和能力能有效地运行。

管理评审时宜对以下内容进行评价:

——前期评审后所需采取行动的执行状态;

——业务连续性管理体系的绩效,包括不符合及其纠正措施、监视和测量结果、以及审核结果的执行情况;

——可能影响业务连续性管理体系的组织及组织环境(4.1)的变更;

——持续改进的机会。

管理评审为最高管理层提供了机会来评估业务连续性管理体系是否能够不断地保持其适用性、充分性和有效性。管理评审应覆盖BCMS的范围,但不必在一次审查中包括所有要素,审查过程可以在一段期间内进行。

最高管理层宜定期开展并评估对BCMS的执行情况和输出的评审。虽然可以持续不断地进行体系评审,但正式的评审还是宜精心地组织和安排,需要准备好适当的书面材料,并根据情况恰当地安排时间。涉及BCMS实施及资源分配的人员宜参与管理评审。

除了定期的管理体系评审之外,以下因素也可能触发评审需求,在安排好审查计划时间表后,宜对这些因素进行检查:

a) 领域/行业发展趋势:领域/行业内有重大创新举措时,应开展一次BCMS的评审工作。在领域/行业以及业务/运营连续性规划技能方面的发展趋势和最佳实践可能被用来制定评价标准。

b) 监管要求:新的监管要求可能需要对BCMS进行一次评审。

c) 事件经历:对一个中断事件进行响应后,不论是否启动了响应程序,都应该进行一次评审。如果启动了响应程序,评审工作就需要考虑响应程序的历史情况、它工作的效果如何、以及为什么要启动响应程序等。如果没有启动响应程序,评审工作就需要检查为什么不启动响应程序以及这一决定是否合适。

管理评审宜促进BCMS效率和性能的提升,并可能会导致以下变化:

——业务连续性管理体系范围的改变;

——业务连续性管理体系有效性的提升;

——业务连续性程序的更新;

——控制措施及其有效性测量方式的改变。

组织宜保存书面记录信息作为管理评审结果的证据,并宜:

——就管理评审结果与相关方进行沟通;

——针对评审结果,采取适当的行动。

10 改进

10.1 不符合和纠正措施

组织宜识别不符合,采取措施进行控制、遏制和纠正,处理后果并评估消除原因需要的措施。

组织宜建立有效的程序以确保未被执行的要求和策划方法以及与BCMS相关的薄弱环节被识别,并及时沟通防止该情况进一步发展,同时,识别并消除根本原因。该程序宜能进行持续地检查、分析和

消除不符合的实际原因及潜在原因。

组织宜及时识别不符合并采取纠正措施。纠正措施可源于明确的不符合声明，该声明清晰地阐述了存在的问题并能被理解。

在识别不符合后，根本原因的调查宜被实施，并立即制定解决该问题的纠正措施计划。该措施计划宜缓解不符合所导致的后果，识别为纠正局面而做出的改变，恢复正常运营和消除原因以防止问题重复出现。纠正行动的性质和时间安排宜与不符合的性质、规模及其潜在后果相适应。

潜在的问题也许会被识别出但没有实际不符合发生。潜在问题可能从针对实际不符合的纠正措施中推断出来，也可以在内部 BCMS 审核过程中或对行业趋势和事件的分析过程中得到识别。识别潜在的不符合也可成为人们日常工作的一部分，并让大家意识到关注及沟通潜在或实际问题的重要性。

建立解决实际或潜在不符合的程序，并持续地采取纠正措施，以助于确保 BCMS 的可靠性和有效性。这些程序宜定义在策划和实施纠正措施时的责任、权力和步骤。最高管理者宜确保纠正措施得以实施，并有系统的定期复查来评估其有效性。

10.2 持续改进

组织宜持续改进 BCMS 的有效性。

PDCA 循环中各层次都实施持续改进，并宜由业务连续性方针和目标、审核结果、监控事件分析、纠正措施和管理评审来驱动。

产生于纠正措施的变更宜反映在 BCMS 文档中。

持续改进要求一个过程来适当地识别问题和不符合，并解决它们。该过程宜能判定问题的性质和问题所在的环境，并且包括改变环境以使问题不再重发。每一步都宜在前一步的基础上建立并改进，从而使改进覆盖更多方面而不仅仅是原来发现的问题，并对组织有更广泛、更有力的影响。

纠正措施的实施宜确认有效。每项措施都宜有预期完成日期。到期后，组织宜确保规定的措施完成并有效。如果评审显示措施没有达到预期效果，则宜设定新的实施日期。

持续改进过程宜遵循与纠正措施相同的基本过程并包括以下方面：

——识别需要解决什么问题及其现状(不符合)；

——识别当前的过程和控制措施(根本原因)；

——决定做出什么变化(纠正措施)。

纠正措施解决 BCMS 的缺陷，以使 BCMS 能发挥其预定的作用，而持续改进是把 BCMS 的效率和效益提升到更高水平。

参 考 文 献

[1] ISO 19011:2011,Guidelines for auditing management systems.

[2] ISO 20000 (all parts),Information technology—Service management.

[3] ISO 22398,Societal security—Guidelines for exercises.

[4] ISO/PAS 22399: 2007, Societal security—Guideline for incident preparedness and operational continuity management.

[5] ISO 27002:2005,Information technology—Security techniques—Code of practice for information security management.

[6] ISO 27031:2011,Information technology—Security techniques—Guidelines for information and communication technology readiness for business continuity.

[7] ISO 31000:2009,Risk management—Principles and guidelines.

[8] BSI 25999-1:2006,Business continuity managemen—Code of practice.

[9] BSI 25999-2:2007,Business continuity management—Pecification.

[10] HB 221:2004,Business continuity management,Standards Australia/Standards New Zealand,ISBN 0-7337-6250-6.

[11] SI 24001:2007,Security and continuity management systems—Requirements and guidance for use,Standards Institution of Israel.

[12] NFPA. 1600:2007,Standard on disaster/emergency management and business continuity programs,National Fire Protection Association (USA).

[13] Business Continuity Plan Drafting Guideline. Ministry of Economy,Trade and Industry,Japan,2005.

[14] Business Continuity Guideline,Central Disaster Management Council,Cabinet Office,Government of Japan,2005.

[15] ANSI/ASIS SPC.1:2009,Organizational Resilience:Security,Preparedness,and Continuity Managements Systems—Requirements with Guidance for Use.

[16] ANSI/ASIS/BSI BCM.01:2010,Business Continuity Management Systems:Requirements with Guidance for Use.

[17] SS 540:2008,Singapore Standard for Business Continuity Management.