国际标准ISO

标准22313

第一版2012
年12月15
日

社会安全-业务连续性管理系统-指南

如果这是您的公司——持续经营管理信息系统——指南

参考编号ISO
22313：2012(E)

目录页

前言

国际标准化组织（ISO）是全球性的国家标准机构(ISO成员机构）联盟。国际标准的编制工作通常由国际标准化组织的技术委员会进行。每个对已设立技术委员会的专题感兴趣的成员机构都有权派代表参加该委员会的工作。国际组织，政府和非政府组织也与国际标准化组织联系，参与这项工作。ISO与国际电工委员会（IEC）在所有电工标准化事务上紧密合作。

国际标准是根据ISO/ IEC指令第2部分中给出的规则起草的。

技术委员会的主要任务是编制国际标准。技术委员会通过的国际标准草案将分发给各成员机构进行表决。作为国际标准发布的文件需要至少75%的投票成员机构的批准。

请注意，本文件的一些要素可能是专利权的主题。ISO不负责识别任何或所有此类专利权。

ISO 22313由技术委员会ISO/TC223，社会安全编写。

为了研究的目的，鼓励用户分享他们对ISO22313：2012的看法以及他们对文件未来版本的修改优先级。点击下面的链接参与在线调查：

http:// www .surveymonkey .com/s/22313

介绍

将军

本国际标准在适当情况下，对ISO 22301：2012中规定的要求提供指导，并就这些要求提出建议（“应当”）和许可（“可以”）。本国际标准无意对业务连续性的所有方面提供一般性指导。

本国际标准包括与ISO 22301相同的标题，但不重复业务连续性管理体系及其相关术语和定义的要求。因此，希望了解这些信息的组织必须参考ISO 22301和ISO 22300。

为对关键点作进一步的澄清和解释，本国际标准包含了一些图。所有这些数字仅用于说明，本国际标准正文中的相关文字具有优先权。

业务连续性管理系统（BCMS）强调以下重要性：

一理解组织的需求以及制定业务连续性政策和目标的必要性；

-实施和运行控制措施，以管理组织整体能力，以便管理破坏性事件；

-监测和审查BCMS的绩效和有效性；

一基于客观测量的持续改进。

BCMS与任何其他管理系统一样，包含以下关键组件：

a)政策；

b)具有明确职责的人员；

c)与以下方面相关的管理过程：

1)政策；

2)规划；

3）实施与操作；

4) performanceassessment;

5）管理评审；

6）改进。

d）提供可稽查证据的一套文件；以及

e）与组织相关的任何BCMS流程。

业务连续性通常与一个组织有关，但是它的实施可能对更广泛的社区和其他第三方产生深远的影响。一个组织很可能有它所依赖的外部组织，同时也会有其他组织依赖于它。因此，有效的业务连续性有助于建设一个更有弹性的社会。

计划-执行-检查-行动循环

本国际标准将“计划-执行-检查-行动”（PDCA）循环应用于规划、建立、实施、运行、监控、评审、维护和持续改进组织BCMS的有效性。

图1说明了BCMS如何将利益相关方的需求作为业务连续性管理（BCM）的输入，通过所需的操作和流程，产生业务连续性结果(即。符合这些要求的管理业务连续性)。

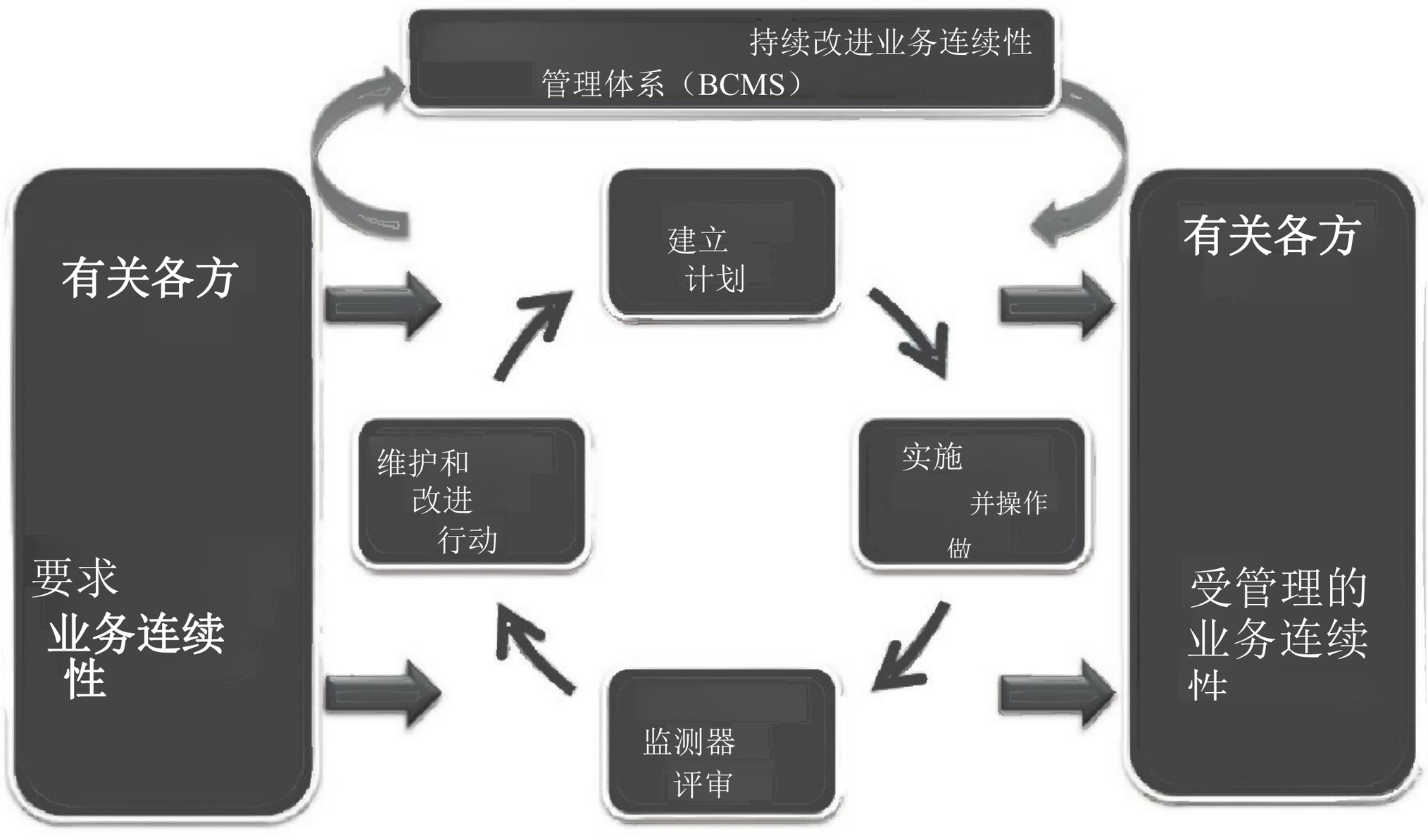

图1-应用于BCMS过程的PDCA模型

表1-PDCA模型说明

计划 （建立）	制定业务连续性政策、目标、控制措施、流程和程序，以改善业务连续性，从而交付符合组织总体政策和目标的结果。
做 （实施和操作）	实施并执行业务连续性政策、控制措施、流程和程序。
勾选 （监测和审查）	监控和审查业务连续性目标和策略的执行情况，向管理层报告结果以供审查，并确定和授权采取补救和改进措施。
行动 （维护和改进）	根据管理评审的结果，对BCMS和业务连续性政策及目标的范围进行重新评估，并采取纠正措施，以维持和改进BCMS。

本国际标准中PDCA的组成

图1的内容与本国际标准的条款之间存在直接关系：

表2-PDCA模型与C子句4至10的关系

PDCA组件	涉及PDCA组件的条款
计划 （建立）	**第4条（组织环境）规定了组织必须采取哪些措施，以确保BCMS符合其要求，同时考虑到所有相关的外部和内部因素，包括：**
	-相关方的需求和期望。
	-它的法律和监管义务。
	-BCMS的要求范围。
	第5条（领导）规定了管理层在示范方面的关键作用 明确承诺，确定政策和建立角色、责任和权限。
	第6条（规划）描述了为BC MS整体建立战略目标和指导原则所需的行动。这些行动为业务影响分析和风险评估（8.2）以及业务连续性策略（8.3）设定了背景。
	第7条（支持）确定了支持BCMS所需的关键要素，即：资源、能力、意识、沟通和文档- 已知信息。
做 （实施和操作）	**第8条（运营）确定了实现业务连续性所需的业务连续性管理（BCM）要素。**
勾选 （监测和审查）	**第9条（绩效评估）为通过衡量和评估BCMS的绩效来改进BCMS提供了依据。**
行动 （维护和改进）	**第10(改进）条涵盖了通过性能评估确定的不合格情况所需的纠正措施。**

业务连续性

业务连续性是指组织在发生破坏性事件后，继续以可接受的预定水平交付产品或服务的能力。业务连续性管理（BCM）是实现业务连续性的过程，它涉及组织为处理可能妨碍其实现目标的破坏性事件所做的准备。

将BCM置于管理系统框架和学科中，创建一个业务连续性管理系统（BCMS），使BCM能够得到控制、评估和持续改进。

本国际标准中，“业务”一词是用于指代组织为实现其目标、目的或使命而开展的业务和提供的服务，因此，它同样适用于在工业、商业、公共和非营利部门运营的大、中、小组织。

任何事件，无论大小、自然或人为，都有可能对组织的运营及其提供产品和服务的能力造成重大干扰。然而，在破坏性事件发生之前实施业务连续性计划，而不是等待事件发生，将使组织能够在不可接受的影响水平出现之前恢复运营。

BCM包括：

a）明确组织的关键产品和服务以及提供这些产品的活动；

b)了解恢复活动的优先次序和所需资源；

c)对这些活动所面临的威胁，包括其依赖性有明确的认识，并了解不恢复这些活动的影响；

d）在发生破坏性事件后，已制定并信任的安排，以恢复这些活动；以及

e)确保这些安排得到定期审查和更新，以便在所有情况下都有效。

业务连续性在处理突发性破坏事件（e.g.explosions）和渐进性事件（例如：　　流感大流行)。

各种各样的事件会扰乱活动，其中许多事件难以预测或分析。　　通过关注中断的影响而非原因，业务连续性识别了组织赖以生存的活动，并使组织能够确定继续履行其义务所需的内容。通过业务连续性，组织可以在中断事件发生前认识到需要采取哪些措施来保护其resources(e.g.people、场所、技术和信息、供应链、利益相关者和声誉。有了这种认识，组织能够对可能需要的应对措施有一个现实的看法，从而有信心管理后果并避免不可接受的影响。

一个有适当业务连续性的组织也可以利用那些可能被认为风险过高的机会。

下图（图2和图3）旨在从概念上说明业务连续性在某些情况下如何有效缓解影响。　　两个图中所描绘阶段之间的相对距离并不意味着特定的时间尺度。

通过有效的业务连续性缓解影响—突然中断

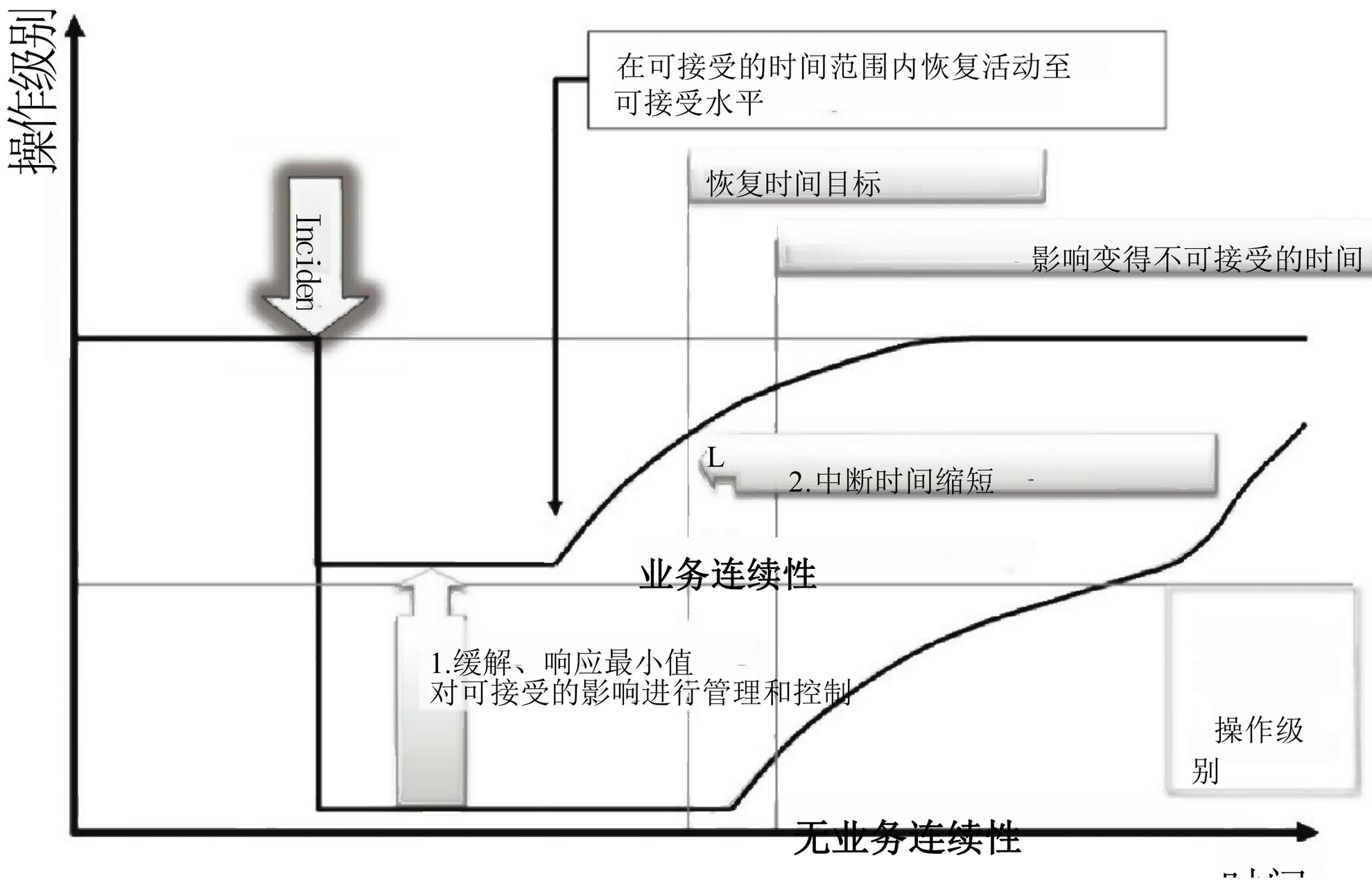

图2-业务连续性在突发中断时有效性的说明

通过有效的业务连续性逐步中断来减轻影响

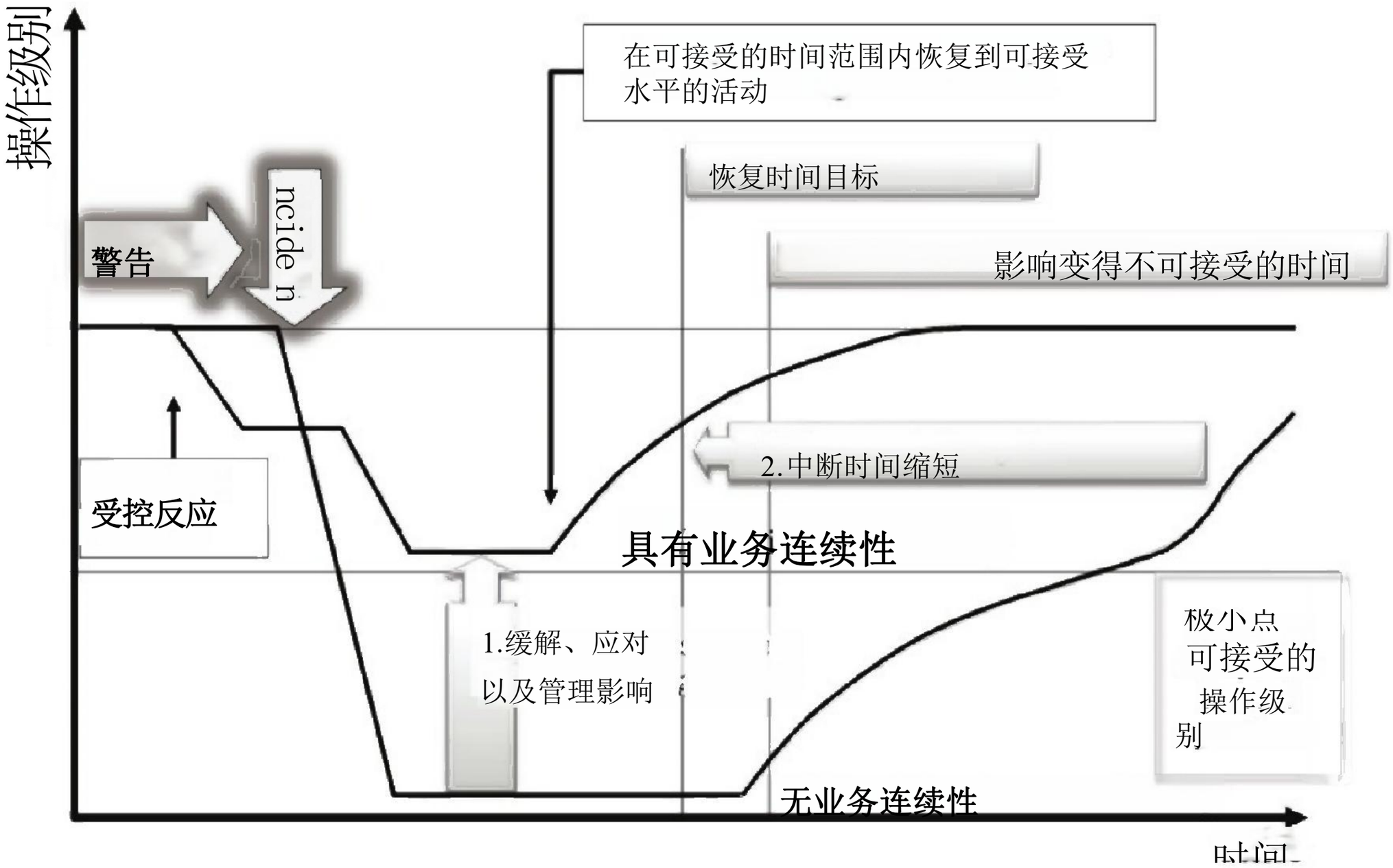

图3-业务连续性对渐进式中断的有效性说明
(e.g.接近大流行)

社会安全-业务连续性管理系统-指南

1范围

本国际标准为业务连续性管理系统提供了基于良好国际惯例的指导，用于规划、建立、实施、运行、监控、评审、维护和持续改进一个文件化的管理系统，使组织能够为发生破坏性事件时做好准备、做出响应并进行恢复。

本国际标准无意暗示BC MS结构的统一性，而是希望组织设计出符合自身需求并满足相关方要求的BC MS。这些需求由法律、法规、组织和行业要求，产品和服务，所采用的流程，其运营环境，组织的规模和结构以及相关方的要求所塑造。

本国际标准是通用的，适用于所有规模和类型的组织，包括在工业、商业、公共和非营利部门运营的大、中、小组织，这些组织希望：

a）建立、实施、保持和改进aBCMS；

b）确保符合组织的业务连续性政策；或

c）做出符合本国际标准的自我决定和自我声明。

本国际标准不能用于评估组织满足自身业务连续性需求的能力，也不能用于评估客户、法律或监管需求。希望进行此类评估的组织可以使用ISO 22301要求来证明符合其他组织的要求，或寻求由认可的第三方认证机构对其BCMS进行认证。

2规范性引用文件

下列引用文件对于本文件的应用是必不可少的。 对于有日期的参考文献，只适用所引用的版本。 对于未注明日期的参考文件，适用最新版本的参考文件（包括任何修订）。

ISO 22300，社会安全术语

ISO 22301，社会安全-业务连续性管理系统-要求

3术语和定义

在本文件中，ISO 22300和ISO 22301中给出的术语和定义适用。

4、组织背景

4.1对组织及其环境的理解

本节介绍组织的背景，以及与设置和管理BCMS有关的内容。BCM的设置和管理在第8.1节中介绍。

组织应评估和了解与其目的和运作相关的内部和外部事实，这些信息应在制定、实施、保持和改进组织的BCMS以及分配优先级时加以考虑。

评估组织的外部环境时，应包括以下因素：

——国际、国家、地区或地方的政治、法律和监管环境；

——社会文化、金融、技术、经济、自然和竞争环境，无论是国际、国家、地区还是地方的；

一供应链承诺和关系；

-考虑内部研究的风险，同时考虑其他相关信息

管理系统以及更广泛的知识管理信息；

-对组织目标和运作产生影响的关键驱动因素和趋势；以及

——与组织外利益相关方的关系以及对他们的看法和价值观。

在评估组织内部环境时，应包括以下相关因素：

-产品和服务、活动、资源、供应链以及与利益相关方的关系；

-能力，从资源和知识的角度来理解(例如。资本、时间、人员、流程、系统和技术)；

信息系统、信息流和决策过程（正式和非正式）；

一组织内部的利益相关方；

一政策和目标，以及为实现这些政策和目标而制定的战略；

一未来机遇和业务优先事项；

一感知、价值观和文化；

-组织采用的标准和参考模型；以及

一结构(e. g. gover财务、职责和责任）。

4.2了解相关方的需求和期望

4.2.1概述

在建立其BCMS时，组织应确保考虑相关方的需求和要求。

组织应确定与BCMS相关的所有利益相关方，并根据其需求和期望，确定其要求。
重要的是不仅要确定义务性和明示的要求，而且还要确定任何暗示的要求。

注：组织需要了解所有对组织有利益关系的人，如媒体、附近的公众、竞争对手等。

在规划和实施BCMS时，重要的是要确定与相关方相关的适当行动，并区分不同的类别。例如，在发生破坏性事件后，可能需要与所有相关方沟通，但在建立和管理BCM（8.1.1）时，则不一定需要与所有相关方沟通。

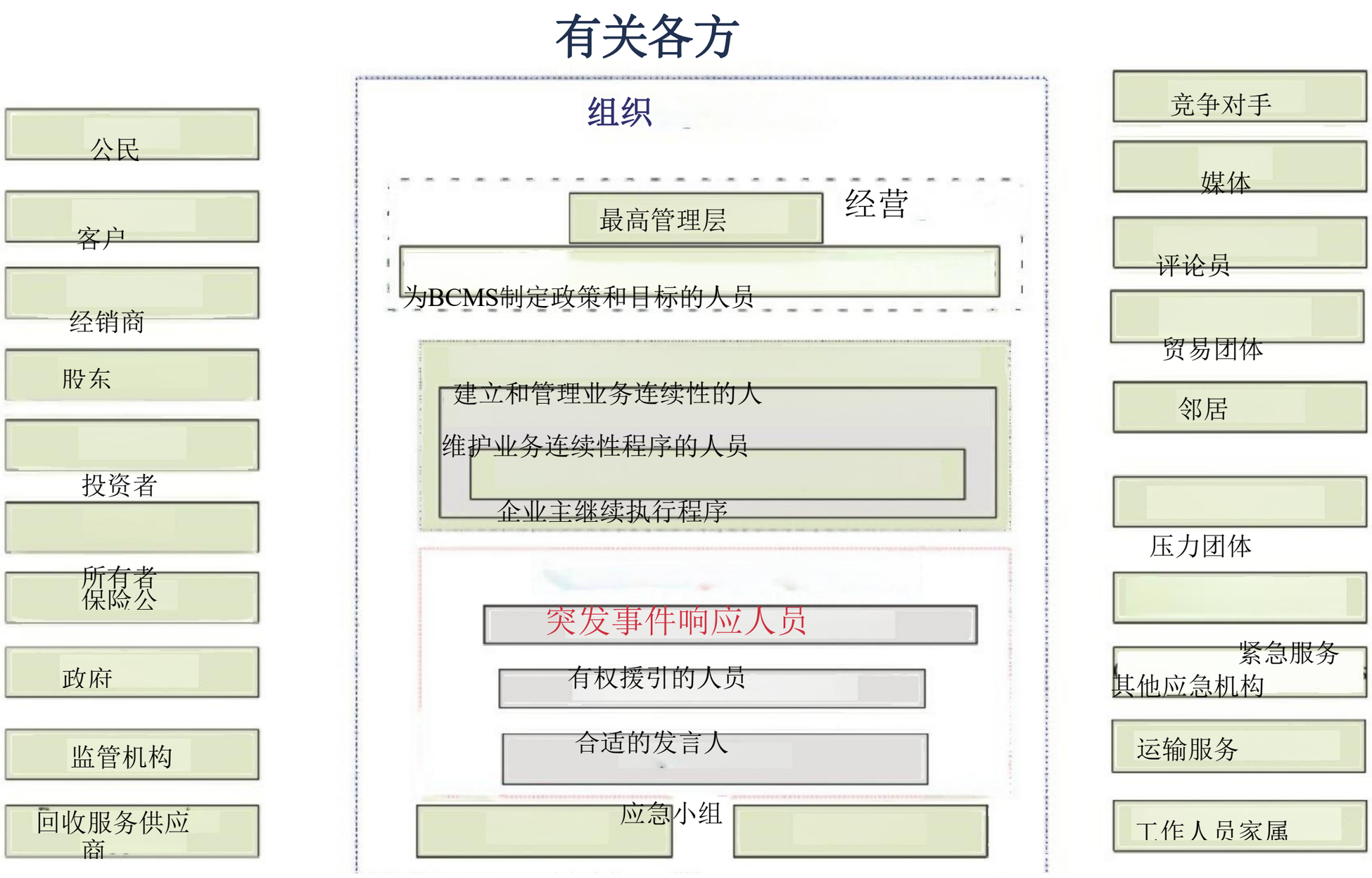

图4—公共和私营部门应考虑的利益相关方示例

4.2.2法律法规要求

所有管理体系均应在组织运营的法律和监管环境框架内运行。 因此，组织应确定并纳入其BCMS中所有相关的和适用的法律和法规要求，这些要求是组织所遵守的并且是相关方需要的。

应记录有关这些要求的信息，并保持其最新状态。 应将法律、法规和其他要求的新变化告知受影响的员工和其他相关方。

在建立、实施和维护BCMS时，组织应考虑并记录适用的法律要求、其遵守的其他要求以及相关方的需求。

组织应确保其BCMS在法律义务和相关利益方要求的范围内开展工作并为其提供支持。

组织应审查其所在地的现行和待定法规和监管要求，包括：

a）突发事件响应：包括应急管理以及健康、安全和福利立法；b）连续性：可能规定计划的范围或响应的程度或速度；c）风险：定义风险管理计划的范围或方法的要求；以及

d）危险：与存放于该地点的危险材料有关的操作要求。

注：在多个地点运营的组织通常必须满足不同地点的要求。

司法权

4.3确定管理体系范围

4.3.1概述

组织应确定BCMS的范围，并确保能够适当地向相关方传达。 BCMS的界限和适用性必须清晰明了，其范围必须考虑到Claus e 4.1和第4.2条中确定的问题。

范围确定了BCMS适用的产品和服务、地点、功能、过程和活动。 由此可知，即使在范围声明中没有明确标识，所有依赖项都将处于范围内。例如，如果在范围内指定了“员工薪酬”，则默认情况下，资金可用性、管理层批准和向金融机构发出付款指令也将处于范围内。

组织应清楚地记录BCMS的范围和上下文。

4.3.2 BCMS范围

组织应以适合于其规模、性质和复杂性的适当方式和术语，定义并记录BCMS的范围。

该范围应包括：

a)确定组织中包含在BCMS中的部分；

b）根据组织的使命、目标、法律责任和内外义务，确定组织的BCMS要求；

c)以一种能够识别所有相关活动、资源和供应链的方式，确定组织的产品和服务；以及

d)考虑到有关各方的需要和利益。

范围还可能包括：

-包括说明BCMS将处理的事件规模和组织的风险偏好；以及
—确定BCMS如何融入组织的总体风险管理战略（如果存在）。

如果组织的某个部分被排除在其BCMS范围之外，该组织应记录并解释该排除。

定义范围的目的是确保涵盖所有相关活动、地点和供应商(8.2.1，图6）。

4.4业务连续性管理系统

这是ISO22301：2012的规范性参考，该标准规定了BCMS的要求。 没有提供指导。

5领导力

5.1领导和承诺

组织内各级相关管理人员应表现出对执行业务连续性政策和目标的承诺和领导作用。示范可以通过激励、参与和授权来实现。

5.2管理　　信奉

最高管理层应表明其对BCMS的承诺。

最高管理层应通过以下方式提供其致力于BCMS的制定和实施并持续改进其有效性的证据：

a）遵守适用的法律要求和组织签署的其他要求（4.2.2）；

b)将BCMS流程整合到组织已建立的维护和审查程序中；

c)根据组织的目标、义务和战略方向制定业务连续性政策和目标（5.3）；

d）任命具有适当权力和能力的一名或多名人员负责BCMS并对其有效运作负责（5.4）；

e）确保确立BCMS角色、责任和能力（5.4）；

f)确保有足够的资源，包括适当的供资水平（7.1）；

g）向组织传达履行业务连续性政策和目标的重要性（7.4）；

h）积极参加锻炼和测试（8.5）；

i）确保进行内部BCMS审计（9.2）；

j）对BCMS进行有效的管理评审（9.3）；以及

k）指导和支持BCMS的改进（第10条）。

管理层承诺也可通过以下方式体现：

一通过指导小组进行业务参与；

-将业务连续性作为管理会议的常设议题。

5.3政策

最高管理层应根据组织的目标和义务来定义业务连续性政策，并确保：

-符合组织的目标（根据其规模、性质和复杂性，并反映其文化、依赖性和运营环境）；

一提供目标设定框架；

-包括与适用要求相关的明确承诺，包括法律和监管义务以及BCMS的持续改进；

-在组织内部进行沟通和理解；

一与其他相关政策相辅相成；

经管理层批准，可向相关方提供一。

应制定适当的条款，以批准政策、保留有关文件信息并定期（例如每年）审查这些信息，以及在内部或外部因素发生重大变化时（例如高层管理变动或新法规的引入）。此类规定的适用性将取决于组织的规模、复杂性、性质和范围。

该政策还应：

一在组织业务连续性的范围和界限方面提供指导，包括限制和排除；

-确定任何必要的当局和代表团，包括负责组织BCMS的个人或人员；

一确定要处理的事故类型和规模的标准；以及

-包括BCMS应考虑或遵守的标准、指南、法规或政策的参考。

业务连续性政策可能包含以下内容：

一key术语；

一funding承诺；

一引用其他相关政策；

一实施业务连续性要求；

一承诺进行和保持业务连续性。

5.4组织机构的职责、权限

最高管理者应确保职责和权限的分配和沟通在BCMS内。

最高管理层成员应全面负责并对BCMS负责。

组织的最高管理层应任命一名或多名具体的管理代表，无论其承担其他职责，都应具有明确的职责、责任和权限：

-确保按照业务连续性政策建立、实施和维护BCM；

—向topmanagementforreviewandasthebasisforimprovement；报告BCM的性能

一在整个组织内提高对业务连续性的认识；以及

-确保为突发事件响应制定的程序的有效性，但不一定是在突发事件期间实施这些程序。

管理者代表可以：

——被称为“业务连续性经理”；

一在组织内承担其他职责；以及

-取决于组织的规模、规模和复杂性，存在于组织的许多领域。

组织的每个职能部门或地点的代表可能被指定来协助实施BCMS。他们的角色、责任、权限和权力应纳入工作描述中，并通过将其纳入组织的评估、奖励和认可政策来加以强化。

最高管理层可任命其他机构，例如指导委员会，监督BCM的实施和持续监测。

应明确并记录BCM的所有角色、职责和权限，并接受审核。

6规划

6.1针对风险和机会的行动

组织应确定如何解决4.1中确定的任何问题和4.2中的要求。 这应该包括评估是否需要制定行动计划，以：

一防止意外结果；

一利用任何机会来改进BCMS。

必要时还应包括：

一将这些行动整合并实施到BCMS流程中（8.1）；以及

-确保有文件记录的信息可用于评估这些措施是否有效（7.5）。

6.2业务连续性目标和实现这些目标的计划

应制定BCM的建立和管理计划（如第8条所述），并应包括确定职责和为完成任务设定适当和现实的目标。 该计划应基于已设定并传达给组织内相关职能和级别的连续性目标。应监测并记录该计划的进展。

随着BCMS的发展，应定期审查并可能需要更新该计划。

以下是在某些情况下可能满足ISO22301规定要求的业务连续性目标示例：

一“建立一个与ISO 22313一致的BCMS”；

一“在截止日期前获得ISO22301：2012认证”；

-“到日期为止，我们将有满足我们对关键客户义务的业务连续性”；and一“到日期为止，我们将有保护关键产品和服务的BCM”。

7支持

7.1资源

7.1.1概述

组织应确定并提供BCMS所需的资源，这些资源将：

a）实现业务连续性政策和目标；

b)满足组织不断变化的要求；

c)在内部和外部就业务连续性管理系统事项进行有效沟通；以及

d）提供业务连续性管理体系的持续运行和不断改进。

这些服务应以及时和有效的方式提供。

7.1.2 BCMS资源

在确定BCMS所需资源时，组织应为以下方面做出充分的安排：

a)人员和人事资源，包括：

1）履行BCMS职责和责任所需的时间；

2）培训、教育、意识和锻炼；

3）BCMS人员管理；

b)设施，包括适当的工作地点和基础设施；

c)信息和通信技术（信通技术），包括支持有效和高效方案管理的应用；

d)所有形式的文件化信息的管理和控制；

e）与相关方的沟通（见图4）；

f)财务和资金。

应定期审查资源及其分配，以确保其充分性。可能需要让高层管理人员参与此审查。

7.1.3事件响应人员

组织应指定具有必要责任、权限和能力来管理事件的事件响应人员。

事件响应人员应组成一个小组，负责管理任何对组织产生重大影响或可能产生重大影响的破坏性事件。

可根据人员在处理突发事件不同方面的能力，将其分配到不同的团队中，例如：

一事件管理/战略管理（8.4.4.3.1）；

一Communications (8.4.4.3.2);

一安全和福利(8.4.4.3. 3);

一救援和安全（8.4.4.3.4）；

一恢复活动（8.4.4.3.5）；

一信息和通信技术恢复（8.4.4.3.6）。

这些小组的所有人员都应有明确界定的责任和权限，适用于事件发生前、中、后。

7.2能力

该组织应建立一个适当的、有效的系统，管理在其控制下从事BCMS工作的人的能力。

管理层应确定所有BCMS角色和职责所需的能力以及履行这些职责所需的意识、知识、理解、技能和经验。 组织内分配角色的所有人员应展示所需的能力，并提供

需要培训、教育、发展和其他支持才能做到这一点。这可以称为能力发展计划，包括：

一对所担任职务的能力进行评估；

一制定个人发展计划，确定为获得能力所需的培训、教育、发展和其他支持；

提供培训和指导，包括选择适当的方法和材料；

一knowledge分享；

一工作分享；

一雇佣或聘用合格人员；

一目标群体培训；

一记录和监控所接受的培训；

-根据规定的培训需求和要求对所接受的培训进行评估，以验证是否符合BCMS培训要求；以及

一根据需要改进开发方案。

组织应有一个流程，用于确定和提供所有参与者的业务连续性培训要求，并评估其交付的有效性。

适合特定角色的培训类型如下：

a)建立和管理BCMS：

1）建立和管理BCM；

2）进行业务影响分析；

3）风险评估；

4)沟通技巧；

5）制定和实施业务连续性文档；以及

6）进行锻炼计划。

b）突发事件响应和业务恢复：

1）事故评估；

2)疏散和就地避难管理，包括登记流程以说明员工情况；

3）在备用工作地点的安排；以及

4)处理媒体询问。

应通过实践培训，包括积极参与演习，来培养整个组织的反应能力和能力。

响应和恢复团队应接受有关其职责和义务的教育和培训，包括与第一响应者和其他有关方面的互动。应定期（至少每年一次）对团队进行培训，并在新成员加入响应结构时对其进行培训。这些团队还应接受防止可能升级为危机的事件的培训。

业务环境和业务运作的变化影响着业务连续性活动的规划、设计和实施。组织可通过积极参与行业BCM活动来表明其对BCM趋势的认识，这些活动可能包括：

一产业利益集团成员；

一会议组织委员会成员；

一在会议和研讨会上做报告；

一出席当地或全球的BCM会议。

积极参加的证明方式可以是以下一种或多种方式：

一会议和研讨会组织委员会成员；

一在会议和研讨会上发表论文。

可以通过以下任何一种方式增强能力：

——将BCMS的成就融入到组织的奖励和认可流程中；

——将BCMS的成就融入组织的绩效和评估过程；

——将BCMS角色、责任、职责和权限整合到组织内部职位描述和滑雪装备；

-业务用户和高层管理人员积极参与排练、演习和测试。

组织应为所有可能受到破坏性事件影响的现有员工建立培训和意识方案，并要求代表其工作的承包商证明在其控制下工作的人员具备BCMS和响应角色所需的能力。

7.3意识

在本组织控制下工作的人员应适当了解BCMS。

这些人可能包括工作人员、承包商和供应商。他们应了解业务连续性政策并：

——他们在事故预防、检测、缓解和自我保护方面的作用和责任保护、疏散、响应、连续性和恢复；

一遵守业务连续性政策和程序的重要性；

一组织运作变化的影响；

-他们对BCMS有效性的贡献，包括BCM性能改进带来的好处；以及

一在实现符合其要求方面的作用和责任。

组织应建立、促进和嵌入一种文化，这种文化：

——成为组织核心价值观和管理的一部分；

一让利益相关者了解业务continuitypolicyandtheirroleinassociatedprocedures。具有积极业务连续性文化的组织将：

一更有效地开发业务连续性；

-在其利益相关方（尤其是员工和客户）中灌输信心，使其相信其有能力处理破坏性事件；

-通过确保在所有级别的决策中考虑业务连续性影响，从而提高其随时间的弹性；以及

一尽可能减少中断的可能性和影响。

BC培养物的开发由以下内容支持：

一组织内所有人员的参与；

一分散的组织领导结构；

一职责分配；

一基于绩效指标的测量；

一将业务连续性纳入日常管理实践；

一awareness提高；

一技能培训；以及

一练习业务连续性计划。

提高认识方案可包括：

一与组织内所有员工就BCM的建立和管理进行协商；

——在组织的通讯、简报和介绍中讨论业务连续性方案或期刊（包括新员工入职培训）；

一在相关网页上包含业务连续性；

一将BCM作为员工和管理团队会议的主题；

一事件发生后选择性发布报告；

一高层管理人员的简报；

一访问指定的替代地点(e.g.a恢复中心）；以及

-向主要供应商和经销商介绍本组织的业务连续性安排。

7.4通信

在建立和管理BCMS时，组织应具有与利益相关方交流信息的有效沟通和协商程序。

这些应包括以下所有内容：

a）各利益相关方之间的内部沟通，包括组织内的员工；

b）与客户、供应商、当地社区和其他利益相关方的外部沟通，包括媒体；

c)接收、记录和回复所有相关方的通信；

d)适当地将国家或区域威胁咨询系统或类似系统纳入规划和业务使用；

e）确保在发生破坏性事件时通讯手段的可用性；

f）确保组织与外部机构进行沟通的能力，以及在适当情况下，确保其他组织和人员能够相互沟通；以及

g）在正常通信中断期间使用通信能力的操作和测试。

组织可邀请可能参与响应的任何外部资源，如消防、警察、公共卫生和第三方供应商，与管理层一起审查其业务连续性程序的相关部分。

组织可在供应商和客户通讯及简报中提及其BCMS和业务连续性安排。

组织应提供有效的外部沟通，作为其意识计划（7.3）和事件发生后（8.4）的一部分。

7.5记录信息

7.5.1概述

文件化信息提供了符合要求和管理体系有效运行的证据。

术语“程序”是指执行某项活动或过程的特定方式。术语“文件化程序”是指应将程序建立并保存在任何媒介上。

一份文件可以涉及一个或多个成文程序的要求，而对成文程序的要求可能由多个文件来涵盖。

本国际标准要求的文件信息包括：

一组织的背景（4.1）；

一法律、法规和其他要求以及合规性证据（4.2.2）；

一BCMS的范围和任何排除（4.3.2）；

一业务连续性政策（5.3）；

一业务连续性目标（6.2）；

一Competence (7.2);

一业务影响分析和风险评估过程（8.2）；

一业务连续性战略（8.3），包括考虑的战略选项;

一继续性、突发事件管理和恢复程序（8。 4);

一Post-运动报告（8.5）；

一BCMS监测（9.1）；

一Internal审计（9.2）；

一管理评审（9.3）；

一不符合项和纠正措施（10.1）。

此外，可能需要记录包含以下信息的文件，以确保BCMS的有效性：

-客户合同和服务水平；

——业务影响分析结果；

—风险评估结果；

一确定和选择业务连续性策略；

一事件响应概述；

一awareness方案；

一BCMS和与员工及利益相关方的事件沟通，如通讯、会议记录和警报；

一为组织和个人提供的培训方案；

一exercise时间表；

一与供应商签订合同和服务水平协议；

一承包商和供应商通知及响应程序；

一检查、维护和校准的证据；

一post事故和接近事故的事件报告；

一BCMS评审会议纪要。

7.5.2创建和更新

为符合创建和更新文件化信息的要求：

-所有记录的信息应包括其标识和description(e.g.atitle、名称、日期、作者、编号、修订版本参考等；

—应指定可接受的格式（例如。 语言、软件版本、图形)和媒体(例如。纸（电子）用于记录信息的采集和展示的电子设备应明确说明；

一应对所有记录的信息进行审核和批准，以确保其充分性。

捕获和展示应包括使用的格式（e.g.language、软件版本、图形）和使用的媒体（例如。纸张，电子文档）。

由于以下因素，不同组织的BCMS记录信息范围可能有所不同：

-组织的规模、产品和服务以及它所从事的活动类型；

一活动的复杂性和相互作用；以及人的能力。

7.5.3文档信息控制

所有要求的文件化信息都应受控。

控制文件的目的是确保组织以适当和充分的方式创建、维护和保护文件，以便实施和运行BCMS。重点应放在这一目的上，而不是建立一个复杂的文件控制系统。

保护的示例包括防止文档被破坏、未经适当授权而修改以及意外删除。

可以授予不同的访问级别和组合，例如只查看、查看和更改以及受限查看。

应建立文件化程序，以确定需要的控制措施，以便：

a)分发文件化信息；

b)提供访问权限（访问权限包括查看或更改记录信息的权限和授权）；

c)在发布前批准文件的充分性；

d）根据需要对文件进行审核和更新，并重新批准文件；

e）确保识别文件的变更和当前修订状态；

f）确保在使用点处有适用文件的相关版本；

g）确保文件清晰可辨，易于识别；

h)确保确定组织认为规划和运行BCMS所必需的外部来源文件得到识别，并对其分发进行控制；

i）防止过时文件的非预期使用，并在出于任何目的保留这些文件时，对它们进行适当的标识；

j）建立文件保留和存档参数；

k）保证保密信息的保护和不泄露。

组织应确保文件信息的完整性，包括：防篡改、安全备份、仅授权人员可访问、防止损坏、退化和丢失。

组织应充分遵守有关保留文件化信息的所有相关法律和法规，并建立、实施和维护实现合规性所需的流程。

8操作

8.1运营规划和控制

组织应确定、规划、实施和控制为实现业务连续性政策和目标以及满足相关需求和要求而需要采取的行动。

这些行动可以结合在一起，创建一个程序，以确保组织的业务连续性得到适当的管理，并保持其有效性。

组织应在项目中建立控制机制，包括：

a）决定如何确定、规划、实施和控制这些行动，例如通过制定实施计划并商定适合实施BCM的方法；

b）确保对这些行动的控制按照所作决定执行，例如设定项目里程碑和规定所需可交付成果；以及

c）保留文件化信息，以证明过程已按计划执行。

组织应确保计划变更得到控制，非预期变更得到审查，并采取适当的措施。

8.1.1 BCM要素

BCM包括以下元素，如图5所示：

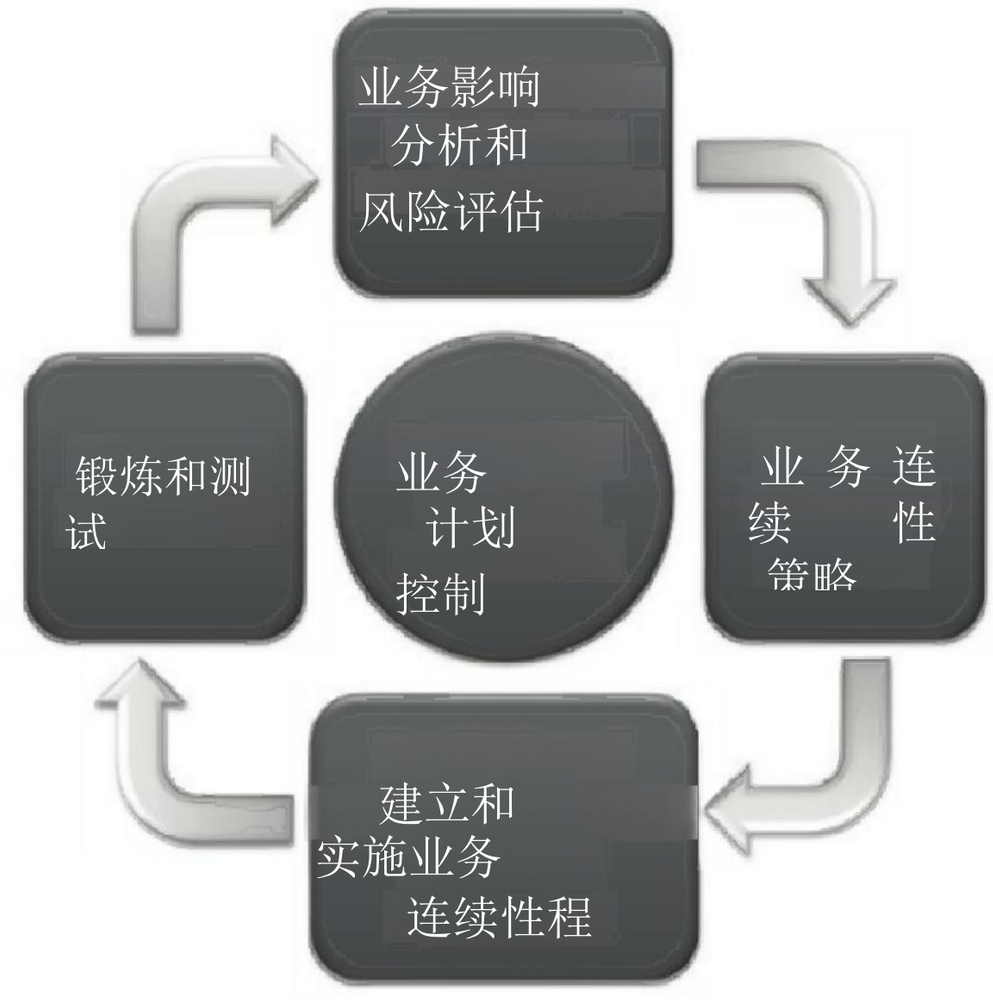

图5-业务连续性管理（BCM）要素

这些要素以及在本国际标准中对它们的处理如下：

a）运营计划和控制（8.1）

有效的运营计划和控制是业务连续性管理的核心，应由高层管理人员指定的负责人领导。

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），可以达成对业务连续性优先事项和要求的共识和理解。BIA使组织能够确定恢复支持其产品和服务的活动的优先级。风险评估有助于了解优先活动的风险及其依赖关系，以及破坏性事件的潜在后果。这种理解使组织能够选择适当的业务连续性策略。

c)业务连续性战略（8.3）

识别和评估一系列业务连续性策略选项，使组织能够选择适当的方法来防止其优先活动的中断，并处理发生的任何中断。选定的业务连续性策略将确保活动在可接受的操作水平下恢复，并在商定的时间框架内完成。

注：所选策略需要考虑已经实施的风险处理措施组织（8.3.3）。

d）建立并实施业务连续性程序（8.4）

实施业务连续性安排将导致创建事件响应结构（8.4.2）、检测和响应事件的方法（8.4.3）、业务连续性计划（8.4.4）以及恢复“业务正常”（8.4.5）的程序。

e)练习和测试(8. 5)

锻炼和测试为组织提供了以下机会：

一提高员工意识和能力发展；

-确保业务连续性和业务连续性程序是完整的、最新的和适当的；以及

一找出改进业务连续性的机会。

8.1.2管理BCM环境

BCM环境的有效管理包括：

a）确保业务连续性的范围、作用和责任的持续相关性；

b)在适当情况下，促进并嵌入整个组织和其他利益相关方的连续性；

c)管理与业务连续性相关的成本；

d）在业务连续性管理系统内建立和监控变更管理和继任管理机制；

e）安排或提供适当的员工培训和意识；以及

f）保持与组织的规模和复杂性相适应的方案文件。

组织的BCM安排的每个组成部分，包括文件，应定期审查、执行和更新。　当组织的业务环境、结构、地点、人员、流程或技术发生重大变化，或者当演习或事件凸显出缺陷时，也应审查和更新这些安排。

本组织可采用公认的项目管理方法，以确保BCM方案得到有效管理。

8.1.3维持业务连续性

保持有效的业务连续性包括：

a）通过良好的实践保持BCM电流；

b)管理运动计划；

c）协调业务连续性定期评审和更新，包括评审或重新制定业务影响分析（BIA）和风险评估；以及

d）确保维持适合于响应团队需要的业务连续性程序。

8.1.4测量有效性

衡量有效性需要解决以下两个问题：

a）监测业务连续性的表现；以及

b)监测和审查外包活动的业务连续性安排以及供应商的BCM能力。

可用于衡量有效性的指标示例包括：

-活动和资源在其规定的恢复时间目标内可恢复，信息是所需的时间（恢复点目标）；

-在备用地点（或多个地点）提供必要的住宿和设备，以便恢复和继续开展活动；

-已经证明具备了在规定的恢复时间目标内恢复优先活动所需的能力；以及

一已经证明具备应对和管理事故所需的能力。

8.1.5结果

表明有效的BCM的结果可能包括以下内容：

a）启用事件管理功能，提供有效的响应；

b)组织对自身及其与其他组织、相关监管机构或政府部门、地方当局和应急服务机构的关系的了解得到适当的发展、记录和理解；

c)定期进行的演习确保员工接受培训，以便有效应对突发事件或中断；

d）了解并能够满足相关方的要求；

e)在发生中断时，员工得到充分的支持和沟通；

f)组织的声誉得到保护；

g）本组织继续遵守其法律和监管义务；以及

h）在整个事件过程中保持财务控制。

8.2业务影响分析和风险评估

8.2.1概述

组织应建立、实施并维护业务影响分析（BIA）和风险评估的表格和文档化流程。从BIA和风险评估中获得的组织内部理解为有效的业务连续性提供了基础。

一个组织通过向客户提供产品和服务来实现其目的。因此，重要的是要理解这些产品和服务（及其相关活动）的中断会对组织的目标和运营产生不利影响。同时，了解支持产品和服务的活动之间的相互关系及其资源需求，以及对这些活动的威胁，也是非常重要的。

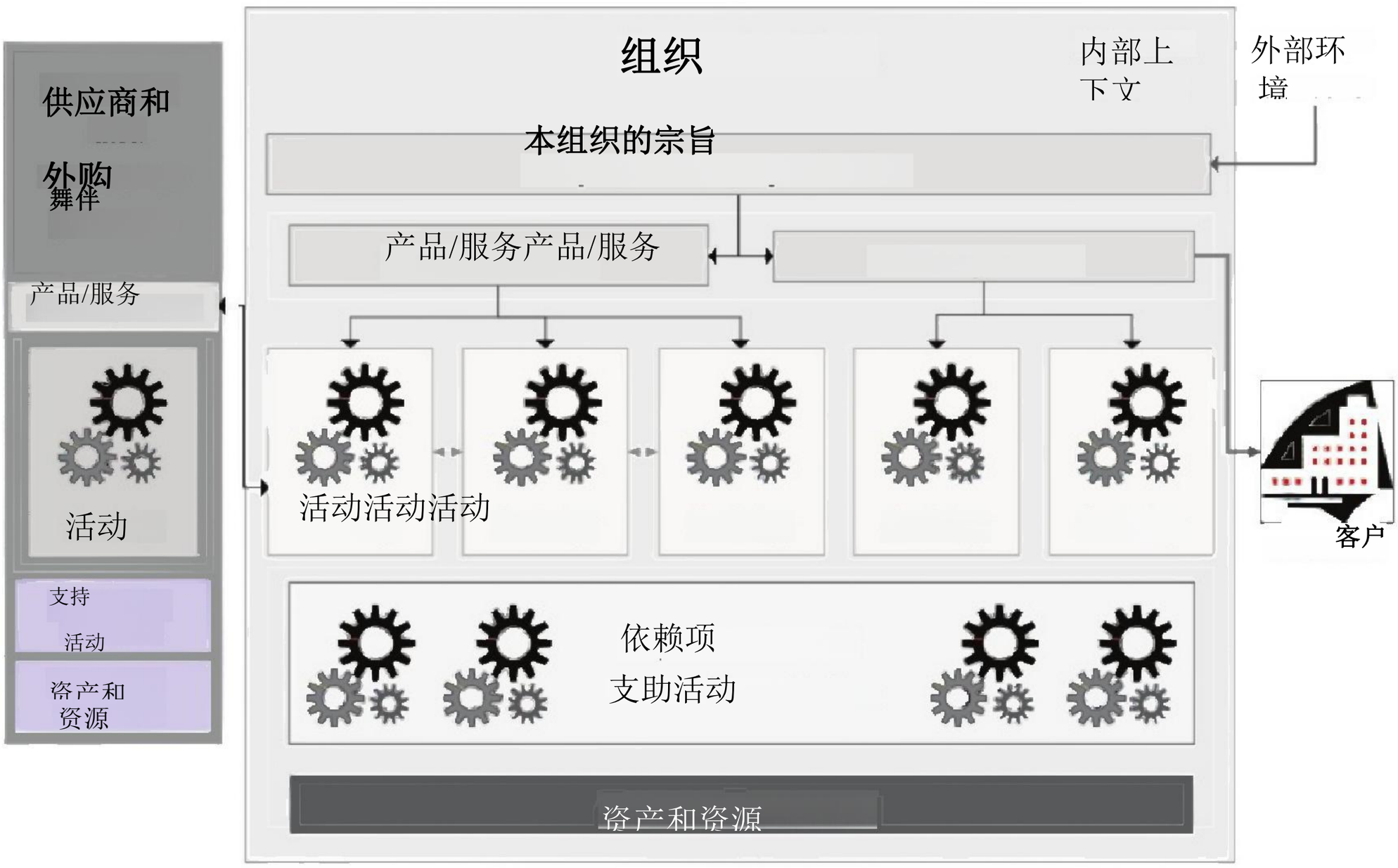

图6-理解组织

通过理解，本组织能够确保其业务连续性与其宗旨、法定职责和对利益相关方的义务相一致。通过业务影响分析和风险评估过程实现理解。这些过程提供了组织确定和选择业务连续性策略所需的信息（8.3.1）。

BIA和风险评估应使组织能够确定以下措施：

a)限制中断对组织的影响；

b)缩短中断时间；以及

c)减少中断的可能性。

应事先确定并商定BIA和风险评估结果的背景、评价标准和格式。应定期审查收集到的信息，特别是在变化期间。

8.2.2业务影响分析

本组织应建立正式的评估程序，以确定连续性和恢复的优先事项和目标。

BIA的目的是：

-了解组织的关键产品和服务以及提供这些产品的活动；

一确定恢复活动的优先次序和时间范围；

-确定可能需要的用于连续性和恢复的关键资源；以及

一确定依赖关系（内部和外部）。

业务影响分析应包括：

a）确定支持组织关键产品和服务交付的活动——“关键”是指BCMS范围内的活动；

b)评估不受控制的、非特定事件对这些活动造成的中断的潜在影响。在评估影响时，组织应解决与业务目标和目的以及利益相关方有关的影响。这些可能包括：

1)对员工或公众福祉的不利影响；

2）违反法定职责或监管要求的后果；

3)损害名誉；

4)财务生存能力下降；

5）产品或服务质量下降；

6）环境破坏。

注1：活动的中断可直接或间接地导致产品和服务的交付中断。例如，丧失向供应商付款的能力可能会损害组织的声誉，并导致供应商拒绝供货，从而阻止产品制造或服务交付。注2：活动通常有日常变化，可能具有周期性。经常存在季节性变化，与每周、每月或每年的截止日期或项目交付日期相关的活动水平较高。假设中断发生在这些周期中最糟糕的时间，可以确保评估出可能的最大影响。

c)估计组织活动中断所造成的影响变得不可接受需要多长时间；

注3：影响变得不可接受所需的时间可能在几秒到几个月之间，这取决于活动的性质。时间敏感的活动可能需要以高度精确的方式加以规定，例如。精确到分钟或小时。对于时间敏感的活动，较低的准确度是可以接受的。

注4：影响变得不可接受所需的时间可称为“最大可容忍中断时间”、“最大可容忍时间”或“最大可接受中断”。组织可接受的产品或服务的最低水平可表示为最低业务连续性目标（MBCO）。

d)根据对潜在影响的评估并考虑到其他相关因素，为恢复这些活动设定优先时间表，在最低可接受水平上；

e）确定活动之间的依赖关系；

f)确定每项活动对支持资源的依赖性，包括供应商和其他相关利益方。

恢复活动的优先时间范围可称为恢复时间目标（RTO）。RTO可以考虑相互关联活动的依赖关系以及不恢复活动的影响变得不可接受的时间[参见上文c]。

注5：从本标准的这一点开始，将使用术语“恢复时间目标”或其缩写“RTO”，而不是“优先时间范围”。

业务影响分析的输出应予以记录，并包括以下识别：

一产品、服务和活动；

一恢复优先级；

一重要的依赖性和支持资源。

业务影响分析的信息可能来自：

一interviews;

一问卷调查;

一workshops；以及

-其他内部和外部来源。

8.2.3风险评估

组织应建立正式的风险评估过程，系统地识别、分析和评价破坏组织优先活动以及支持这些活动的流程、系统、信息、人员、资产、供应商和其他资源的风险。

风险评估提供了一个结构化的过程，用于分析风险的后果和可能性，然后决定是否需要进一步治疗。这个结构化的过程试图回答一些基本问题：

a）可能发生什么情况以及原因（风险识别）？

b)可能的后果是什么？

c)m发生的可能性是多少？

d)是否有办法减轻后果或降低可能性？

这一过程需要考虑财政、政府和社会义务。

组织应了解其活动所需资源所面临的威胁和脆弱性，特别是：

一高优先级活动所需；或

一需要较长的更换准备时间。

组织应选择适当的方法来识别、分析和评估可能导致中断的风险。ISO 31000规定了风险管理的原则和相关指南。　　本国际标准中应包括的典型要素如下：

-风险识别：确定组织优先级活动以及支持这些活动的流程、系统、信息、人员、资产、供应商和其他资源中断的风险。这些风险可能来自：

一特定威胁，可描述为可能在某个时间点中断活动和资源的事件或行动（例如。诸如火灾、洪水、停电、人员流失、员工缺勤、计算机病毒和硬件故障等威胁）；

-破坏性事件，可能由资源内部的漏洞引起(例如。　　单点故障、消防不足、缺乏电力弹性、人员配备不足和IT安全性和弹性差)；

-风险评估：评估哪些中断相关风险需要处理。　　这应该侧重于高优先级活动或具有较长更换时间的活动所需资源；以及-治疗措施的确定：确定能够提供业务连续性的治疗措施

目标与组织的风险偏好一致（4.1）。

注：如果组织或外部机构已经进行了任何其他风险分析，那么可以提供与风险评估相关的有用信息。

社会需求或监管义务可能要求组织与某些利益相关方分享风险评估的部分结果。

8.3业务连续性策略

8.3.1确定和选择

8.3.1.1概述

确定业务连续性战略是识别出为解决业务影响分析和风险评估结果而需要采取的行动，并以符合组织业务连续性目标的方式进行。在发生破坏性事件之前、期间和之后，可能需要采取此类行动，例如：

一将制造生产线分散到两个地点；

一安装发电机；或

-通过业务连续性安排缩短中断时间并将其强度降低到可接受水平，从而减少破坏性事件的总体影响。

业务连续性战略的确定和选择应基于业务影响分析和风险评估的结果（8 .2）。

组织应确定以下方面的适当战略选择：

一保护优先活动；

一稳定、持续、恢复和恢复优先活动；

一减缓、应对和管理影响。

组织应建立审查和批准建议解决方案的机制。

8.3.1.2保护优先活动

对优先活动的保护可针对：

-降低活动风险；

-将活动转移给第三方（尽管责任仍然由组织承担）；一如果有可行的替代方案，停止或改变活动。

应根据以下内容选择保护优先级活动的选项：

-活动的感知脆弱性；

一与估计效益相比，措施的成本；

一（可选）活动的紧迫性——因为解决这个问题的时间将更少；以及——选项的整体可行性和适用性。

如果组织估计威胁“极不可能”或保护优先活动的成本“过高”，则可选择接受风险，并将其作为其持续BCMS绩效评估的一部分进行重新评估（第10条）。

8.3.1.3稳定、持续、恢复和恢复优先活动

稳定、持续、恢复和恢复优先活动，也应解决其依赖性和支持资源问题；

业务连续性策略选项可能包括：

a）活动转移：将部分或全部活动转移至组织内部的另一部门，或外部的第三方，可以是独立转移，也可以是通过互惠或互助协议进行转移；

b)资源重新安置或重新分配：资源，包括员工被转移到组织内的另一个地点或活动，或者外部的第三方；

c）备用流程和备用容量：建立备用流程或在流程和/或库存中创建冗余/备用容量；

d)资源和技能的替换：增强人员能力，包括关键人员的多技能或通过外包获得额外的人力资源。替代资源由第三方提供或由组织远程持有的库存提供；或者与外部组织和关键利益相关方建立互助协议，以提供临时访问额外能力；以及

e）临时变通办法：某些活动可采用不同的工作方式，以在有限时间内提供可接受的结果。解决办法可能更耗时和/或劳动密集型(e.g.a手动操作，而不是自动化系统）。由于这些原因，解决办法通常只适用于较短的时间段或推迟恢复正常业务。

f）在考虑恢复活动的地点时，业务连续性方案应包括受损/受影响的现场（或多个现场）和未受损的备用现场（或多个备用现场）。

为确保活动能够在恢复时间目标内恢复，也可以为其依赖项和支持资源设置恢复时间目标。设定这些恢复时间目标时，可能需要考虑：

-在需要全面恢复之前，提供最低限度服务的可能性；

一可能推迟恢复对支持资源的依赖性的变通方法（如手动过程）；

-积压的工作量和恢复丢失数据所需的时间；以及

-恢复要求的复杂性和规模，或者需要具有较长准备时间的专用设备。

组织应评估所有战略选择，以确定这些措施是否引入了新的风险。

业务连续性策略选项用于稳定、继续、恢复或恢复优先级活动，通常会非常昂贵。如果组织估计这种情况会发生，它应该选择可接受且符合其业务连续性目标的替代策略，或者根据4.3.2将受影响的产品和服务排除在BCMS范围之外。

8.3.1.4减缓、应对和管理影响

缓解事件影响和持续时间的选项可能包括：

a)保险：购买保险可以为一些损失提供一些经济补偿，但不能满足所有的费用（例如。未投保事件、品牌、声誉、利益相关方价值、市场份额和人力后果）。仅靠财务结算无法充分保护组织和

满足利益相关者的期望。保险覆盖更有可能与其他一种或多种策略结合使用；

b)资产恢复：与专门从事资产损坏后的清洁或修复的公司签订备用服务合同；以及

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

组织应确保对供应商的业务连续性进行评估。本组织不妨集中精力对付那些不履行交货义务将最迅速地扰乱优先活动的供应商。技术可能包括：

一招标和合同要求的规范；—供应商计划的定期审核；

一联合业务连续性演练。

8.3.2确定资源需求

8.3.2.1概述

组织应确定补充选定战略选项所需的资源：

组织应建立：

a)适当的团队，或对于较小的组织，具有适当权限监督突发事件准备、响应和恢复的个人；

b)为支持BCMS而生产或捐赠的服务、人员、资源、材料和设施的定位、获取、存储、分发、维护、测试和核算的后勤能力和程序;

c）在事件发生前、中、后，为支持业务连续性安排而采取的财务、后勤和行政程序。程序应：

1）确保财政决策能够迅速进行；

2)符合既定的权限级别、治理和会计原则；

d)对响应时间、人员、设备、培训、设施、资金、保险、责任控制、专业知识、材料以及组织资源和任何供应商的资源在这些方面所需的时间框架的资源管理目标；以及

e)关联方协助、沟通、战略联盟和互助的程序。

8.3.2.2人员

本组织应确定适当的措施，以维持和扩大核心技能和知识的可用性，以防事件导致工作人员可用性的减少。这些措施应包括拥有广泛专业技能和知识的雇员、承包商和其他利益相关方。保护或提高这些技能的技术可能包括：

-备用技术专家名单和呼叫u plan；

-对员工和承包商进行多技能培训；

-分离核心技能，以减少事件的影响，包括在多个地点对具有核心技能的员工进行物理隔离；

一使用第三方；

一继承规划；以及

-记录流程和其他形式的知识保留和管理。

依赖于事件后人员调动的程序可能需要考虑以下因素：

一人员调往其他地点；

备用站点的一人员需求，例如：

一accommodation;

一 cateringfacilities;

一个人和家庭承诺；

一对不同设备进行培训；

一家庭工作带来的挑战。

专家角色可能包括：

一security;

一运输物流；

一福利和紧急情况。

8.3.2.3信息和数据

组织运营中至关重要的信息应根据BIA中确定的时间框架进行保护和恢复。数据的存储和恢复应符合相关法规。

注1：ISO/IEC27031中给出了关于确保电子数据的时效性的进一步指导。ISO/IEC27002提供了关于确保数据的持续保密性、完整性和可用性的指导。

为使组织能够做出响应并恢复，需要的信息应具有适当的：

-保密性：例如，如果活动被转移到另一个地点；

一完整性：信息可靠，可信赖；

-可用性：信息的可用性应与活动的需求相匹配。响应期间所需的信息可能需要立即提供，而其他数据可能在事件发生后一段时间才需要；以及

—货币：根据需要保持最新，使活动能够运行—但是，由于事件而丢失的数据可能需要重新创建。

在所有情况下，活动所需的信息都应适当更新。这种时效性可称为恢复点目标（RPO）。当数据被复制时，可以使用各种方法，包括电子或磁带备份、缩微胶片、照片复印件以及在生产时创建双重副本。

应记录信息检索策略，以便检索尚未加密或备份到安全位置的信息。

信息战略应扩展到包括：

一物理（硬拷贝）格式；以及

一虚拟（电子）格式等。

注2：如果复制的信息存储在离原件太近的地方，破坏事件可能会损害其完整性或阻止访问。然而，距离过远可能会导致在需要时无法访问。因此，最好有书面证据证明这些相互冲突的问题是如何解决的。

本节中提及的信息可能包括：

-联系方式；

一供应商、利益相关方和利益相关方详细信息；

一法律文件（e.g.contracts、保险单、产权证）；

一其他服务文件（例如合同和服务水平协议）。

8.3.2.4建筑物、工作环境和相关设施

工作场所策略可能有显著差异，而且可能有多种选择。不同类型的事故或威胁可能需要实施不同的或多个工作场所选项。适当的策略在一定程度上取决于组织的规模、行业和活动范围、利益相关方以及地理基础。例如，公共当局需要在其社区内维持第一线服务，而有些组织则可能在另一个国家或大陆开展业务。

组织应制定一项战略，以减少其正常工作场所(s)不可用的影响。这可能包括以下一项或多项：

a）组织内部的替代场所（地点），包括其他活动的迁移；

b)其他组织提供的备选房地（不论是否为互惠安排）；

c)应急控制中心；

d)第三方专家提供的替代场所；

e)在家或远程工作；

f)其他双方同意的合适场所；以及

g）在已建立的现场使用替代劳动力。

备选场所应仔细选择，考虑可能受同一事件影响的地理区域。例如自然灾害可能会造成大面积损害，并影响电力、燃气、水和通信等基本服务。如果预计存在此类风险，备选场所应远离可能受影响的区域。

如果员工要搬到其他办公地点，这些办公地点应该足够近，员工愿意并且能够前往，同时考虑到事件可能带来的任何困难。然而，替代办公地点也不应太近，以免受到同一事件的影响。

为保持连续性而使用替代场所，应当明确说明替代场所所需的资源是否专供本组织使用。如果备用房地与其它组织共享，则应制定并记录缓解这些房地不可用的计划。

在某些situations(e.g.a生产线或呼叫中心，可能需要转移工作量而不是人员。这可能需要备用的容量、额外的人员（无论是加班还是招聘）以及其他资源。

8.3.2.5设施、设备和消耗品

本组织应查明并保持支持其优先活动的核心用品的库存。

有些设施和设备可能难以获得，价格昂贵（需要很长时间才能获得授权），或者交货期很长。提供这些资源的解决方案可能需要考虑这些问题。改变业务做法，如库存控制或建筑管理，可能提供解决方案。

提供这些服务的技术可能包括：

一在其他地点储存额外的用品；

一与第三方签订的在短时间内交付库存的协议；

一将即时交货转移至其他地点；

一在仓库或装运地点储存材料；

——将分组装作业转移到有供应的替代地点；

一识别替代/替代供应品；和

一设施和设备识别以及按阶段进行的多选项规划。

如果活动依赖于专业供应品，组织应确定关键供应商和单一的供应来源。管理供应连续性的策略可能包括：

一增加供应商数量；

一鼓励或要求供应商具备业务连续性；

一contractual和/或与主要供应商的服务水平协议；以及

一识别替代的、有能力的供应商。

如果活动需要搬迁，应核实供应商是否能够在替代地点有效提供其产品或服务。

8.3.2.6信息通信技术（ICT）系统

在许多组织中，没有信息和通信技术系统就无法开展活动，而且在恢复活动之前必须重新启用这些系统。如果可能和实际可行，组织可能需要在信息和通信技术服务恢复期间实施人工操作。

技术选择将取决于所采用的技术的性质及其与活动的关系，但通常将是以下内容的组合：

一组织内部提供的资源；

一由第三方向组织提供的服务；以及

一组织订阅的外部服务。

提供优先活动所需信通技术系统的方法可包括：

-在地理上扩散它们，例如，在不受同一破坏性事件影响的不同地点保持相同的技术；
-将旧设备作为紧急替换或备用设备；以及
一承包提供设备或恢复服务。

由于支持这些系统的技术复杂，因此信息和通信技术系统通常需要复杂的安排来确保能够及时恢复，因此应考虑：

—为信息和通信技术系统设定恢复时间目标（RTO），以便在这些目标范围内优先恢复活动；

-特别注意技术站点的位置和它们之间的距离；

一在多个站点之间分配技术；

-为增加的远程访问用户数量提供足够的设施；

一建立无人（暗）站点和有人站点；

-改善电信连接，增加冗余路由水平；

-提供自动“故障切换”，而不是要求人工干预来重新定向ICT供应；

一适应信息和通信技术的过时；以及

一提供额外的第三方连接和外部链接。

如果采用从一个站点到另一个站点的“故障转移”技术，可能需要考虑两个站点之间的网络路径距离。如果站点之间的距离非常长，这可能会减慢系统响应速度，并使信息和通信技术系统失效。

如果一个组织的信通技术系统在多个地点运行，那么可能有机会实施“相互信通技术战略”，即每个地点的规模都应能够容纳多个地点的综合信通技术能力。

如果一个组织使用非常专业或定制的、需要较长准备时间的技术，那么它可能需要考虑通过为替换或恢复做出特殊预测来加强其信息和通信技术的保护。

注：有关ICT连续性的进一步指南可参见ISO/IEC27031、ISO/IEC 27002和ISO/IEC 20000（两部分）。

8.3.2.7运输

发生事故后，可能需要提供运输服务，以：

一如果员工无法使用正常交通工具，可将其送回家；

一员工调往其他工作地点；以及—不同地点
所需资源。

本组织应预先确定在发生破坏性事件后可能需要的提供替代运输方式的备选方案。这些可能包括：

-确定可能由事故和异常情况直接引起的物流中断的可能情形；

-考虑交通状况、运输方式和其他物流网络，确保备选物流手段和路线的安全；

一与运输供应商的协议。

8.3.2.8财务

组织应确定在发生破坏性事件期间和之后确保有必要的资金可用的备选方案。这可能包括：

-为紧急采购提供资金，如食品、住宿、设施、消耗品和运输；

一工作人员费用报销；

-重大支出，例如，租赁或购买建筑物和设备；

为了防止滥用或便于提出保险索赔，可能有必要证明有效的财务控制，例如规定在发生破坏性事件期间和之后正式记录费用。

8.3.2.9供应商

如果产品、服务或活动已经外包，该产品、服务或活动的责任和问责制仍然由组织承担。因此，企业应确保其主要供应商有有效的连续性安排。一种方法是获取主要供应商连续性计划的可行性证据及其实施和维护计划。 见8.3.1.5。

8.3.3保护和缓解

对于需要处理且符合其整体风险态度的已识别风险，组织应考虑减少发生可能性、缩短持续时间和限制中断影响的方法。

8 .4建立并实施业务连续性程序

8.4.1概述

组织应制定并记录程序，以提供对破坏性事件的总体控制，并在恢复时间目标内恢复活动。业务连续性程序应建立适当的内部和外部通信协议，并且：

a)具体——关于在中断期间应该采取的直接步骤；

b）灵活——以便能够应对意外威胁情景和不断变化的内部和外部条件；

c）重点——应明确与可能破坏运营的事件的影响相关，并基于所述假设和相互依赖性分析进行开发；以及

d)有效—通过实施适当的缓解策略来尽量减少事故的后果。

8.4.2事件响应结构

组织应制定程序和管理结构，使其能够为破坏性事件做好准备，减轻影响，并有效应对。

响应结构应提供：

-确定影响阈值，以证明启动正式响应的合理性；

-评估破坏性事件的性质和范围或潜在影响；

一制定措施，保障受影响人员的福利；

一对破坏性事件做出适当的反应；

-有启动、运行、协调和通信响应的流程和程序；

—提供资源以支持管理破坏性事件和最小化影响所需的流程和程序；以及

一与有关各方的沟通，特别是作者和媒体。

响应结构应简单且能够快速形成。在确定结构时，应考虑：

-拥有一名或多名有能力的人员，以确定事件的影响并评估事件的影响或潜在影响及其时间范围；

-能够调动团队控制、遏制事件并启动适当的响应；以及

——包括适当的资源，可能包括工作人员、承包商、设备和资金。

较大或复杂的组织可以采用分层的事件响应方法，并且可以建立不同的团队来专注于事件响应、事件管理、通信、福利和业务恢复。在较小的组织中，事件响应的所有方面都可能由一个团队处理，但绝不能由单个个人负责。

每个团队应有管理其行动的程序，并包括具有必要责任、权力和能力的人员。个人和团队能力可通过以下方式体现
训练和锻炼。

8.4.3警告和沟通

8.4.3.1概述

组织应建立、实施和保持警告和沟通程序。这些应包括：

a）检测事故并提醒响应人员；

b)对事件的持续监测；

c)组织内部各级、各职能部门之间的沟通；

d）与利益相关方的外部沟通；

e）接收、记录和回复来自其他相关方的通信；

f）接收、记录和回复任何国家或区域风险咨询系统或其等效系统；

g)提醒可能受到实际或即将发生的破坏性事件影响的相关方；

h）确保在发生破坏性事件时，通信手段可用；

i）促进与应急响应人员的结构化沟通；

j)确保多个响应组织和人员的互操作性；

k）记录有关事件、采取的行动和作出的决定的重要信息；以及

1)通信设施的运行。

组织可能需要决定是否以及何时与外部利益相关方沟通其警告和沟通程序。在做出这一决定时，生命安全应是首要考虑因素。应记录下决定及其原因。

例如，从事可能威胁到邻近居民安全的危险活动的组织，可能需要确保向邻近居民通报潜在的危险。这可能意味着他们需要了解如何发出ala rms以及如何响应。

组织应有有效的程序和设施，以便快速发布警告、警报和外部沟通。对有特殊需要的人员，如老年人、残疾人等，应有特别安排，应定期进行预警和通信系统的演练。有关运动指导，请参见第8.5节。

8.4.3.2事件通报程序

需要制定程序，在潜在事故发生前，能够：

-接收、记录和响应任何国家或地区风险咨询系统或其等效系统；这些可能反映该地点常见的威胁，如海啸、地震或飓风预警；以及

——提醒可能受到实际或即将发生的破坏性事件影响的相关方——组织有法定或道义责任发出警告。

一旦事件开始，组织应制定程序以确保：

-通过当地观察或远程监测，持续监测事件，并将任何进展通报给适当的响应者；

一与急救人员进行结构化沟通；

-多个响应组织和人员之间的互操作性，这是该组织的责任；

-各响应小组与组织之间进行沟通；

-与工作人员和其他有护理义务的人，如访客和承包商保持定期沟通，这可能需要在疏散点进行，然后在家中或替代地点进行；以及

记录事件的重要信息、采取的行动和做出的决定，由事件的当事人或每个团队指定的日志管理员记录。

还需要制定程序，以促进相关方之间的有效双向沟通比如客户和媒体。

组织应与这些方保持联系，直到恢复正常业务运作为止，此时可能需要发出通信以表明事件结束。

8.4.3.3事故通讯设施

这些程序可以通过使用专用或临时通信设施来促进，该设施应位于离受影响地点足够远的地方，以确保其操作不会受到事故的影响，并且可以与其它事故响应设施位于同一位置。

可用的通信设备应认识到，该事件可能影响了正常通信的性能，因此可以提供多种替代方案，例如：

——扩音器或公共广播系统；

一备用移动电话；

-双向无线电。

8.4.4业务连续性计划

8.4.4.1概述

该组织应制定文件化的程序，使该组织能够对事件作出反应，并适当处理恢复和恢复其活动的问题。

这些程序应涵盖应对事故的所有方面，特别是与生命安全相关的问题，并满足所有使用者的要求。为确定要求，可能有益的做法是：

一参与程序的开发，以及将使用这些程序的人；

一利用锻炼中的反馈和从破坏性事件中学到的教训。

时间尺度和性能水平应基于业务影响分析（8.2.2）期间收集的信息以及所选的业务连续性策略（8.3.1）。

每个计划中应明确识别以下内容：

一目的和范围；

一优先活动的成功目标和衡量标准；

一激活标准和程序；

一 implementationprocedures;

-角色、职责和权限；

一通信要求和程序；

一内部和外部相互依赖和相互作用；—资源需求；以及

一信息流和文档编制流程。

处理破坏性事件时，需要考虑许多行动。 这些应包括在文件化程序(8.4.4.2和8.4.4.3)andinclude:

a）对事故作出反应并进行评估：

1)发生了什么，它是如何发生的？

2）组织的哪些部分和哪些利益相关方已经或可能受到影响？

3）预计事件持续时间及其影响?

4）是否可以通过常规管理安排来处理该事件？

b)根据每个程序的启动标准，对事件评估进行评价；

c）宣布事件并激活程序，当激活标准已满足时；

d）稳定、持续、恢复和复原活动；

e）建立和运行事件管理位置；

f）确定在处理事故及其影响时应优先考虑的问题和活动；

g)控制和协调所有激活的程序；

h)激活或建立备用站点，以恢复IT或其他基础设施能力，以及临时开展组织活动；

i)监测事件的进展；

j)根据变化的情况审查和调整计划；

k)停止计划，恢复常规管理，重新建立可持续能力；

l）进行总结并确定学习机会；

m）确保良好的治理和整理以及在事件管理和恢复期间生成的文档的安全。

为及时恢复组织的产品和服务交付，恢复各项活动的成文程序应：

一满足支持该产品或服务的活动的恢复时间目标；以及

一足够可靠。

这可以通过以下方式实现：

一拥有或控制实施程序的手段和资源；以及

一与第三方签订的合同、协议或服务级别。

为确保程序的运行不受同一干扰的影响，组织可以采取预防措施，例如，在多个地点分离人员和信息通信技术。然而，对于所有规模和类型的事件进行全面隔离是不可能的，这一限制应由高层管理确定并达成一致。这种限制可能以距离、最少人员或严重程度来表示，并可能由民事当局对严重和/或广泛事件的反应来决定。

8.4.4.2业务连续性计划的内容

业务连续性计划可以是单一的文件化程序，也可以是涵盖所有要求和BCM S范围的多个程序。

应定义每个文件化程序的目的、范围和目标，并且对于将要实施该程序的人员来说，这些目的、范围和目标应该是可理解的。应明确引用与其它要求的和相关的文件化程序或文件之间的关系，并且描述获取和访问这些程序或文件的方法。

在业务连续性计划中，应明确识别以下内容（参见also8.4.4.3)：

a）岗位职责：

1)确定将使用业务连续性计划的人员和团队的角色、职责和权限。如果业务连续性计划包含多个文件化程序，则应定义每个程序的角色、职责和权限；以及

2）关于谁有权启动程序以及在什么情况下启动程序的指南和标准，这可能遵循规定的升级阶段。

b）召唤和站立：

1）组织对破坏性事件作出反应的启动程序以及每个文件化程序中的启动标准和程序。可能需要考虑该程序是在正常工作时间还是在非正常工作时间启动；

2）事件发生后，停止团队工作的流程；以及

3)约会和见面地点，以及合适的替代方案。

c）事故管理：

1）管理破坏性事件的直接后果，充分考虑受影响人员（包括团队成员）的福利问题，应对破坏的备选方案（可描述为战略、战术和操作），以及预防或进一步损失或优先活动不可用；

2）在每个文件化程序中应有：

i)确定需要执行的行动和任务的实施程序，特别是组织如何在预定的时间框架内继续或恢复其优先活动；

ii)与文件化程序相关的资源需求（8.3.2）；以及

iiij）记录事件、采取的行动和做出的决定的关键信息的方法。

d）每个文件化程序中的联系信息：

1)团队成员和其他具有角色和职责的人员的联系方式——当地数据适用保护性立法，应根据该立法保存联系详情；以及

2)联系和动员可能需要的任何相关机构、组织和资源的细节。

e)通信（8.4.3）：

1）详细说明组织在何种情况下以及如何与员工及其亲属、主要利益相关方和紧急联系人进行沟通；

2)组织在发生事故后媒体反应的细节，包括其沟通策略、与媒体的首选接口、起草媒体声明的指导方针或模板以及确定合适的发言人。

8.4.4.3特定类型的程序

8.4.4.3.1事件管理/策略管理程序

事件管理的目的是确保组织对破坏性事件的响应在战略层面上是有效的。

程序应包括在突发事件期间管理组织面临的所有可能问题的基础，包括与利益相关方有关的问题。

组织应确定一个地点、房间或空间，以便对事件进行管理。 一旦确定，该地点应成为组织响应的焦点。还应指定一个备选会议地点，以防主要地点无法使用。每个地点都应具备适当的资源，以便事件管理团队能够立即启动有效的事件管理活动。

地点可能简单到酒店房间或工作人员的家中，也可能复杂到一个配有个人电脑、视频会议和多个电话的专用指挥中心。 最初，可能需要举行虚拟或异地meeting，e.g.via电话会议、电视会议或视频会议，以便及时作出关键决策。

所选位置应适合用途，可能包括：

一为所需人数提供空间；

-有效的初级和次级通信手段；以及

-获取和共享信息的设施，包括对新闻媒体的监控。 其他应急小组可能需要类似的设施。

8.4.4.3.2通信程序

通信程序可以包括在事件管理响应程序中，也可以根据需要由单独的团队使用。

需要积极管理和协调事件期间将发送和接收的许多通信。该程序应包括：

a)组织如何以及在什么情况下与员工及其亲属、紧急联系人和其他利益相关方进行沟通的详细信息；

b)事件发生后，组织媒体应对的详细信息，包括：

1）事故通讯策略；

2)与媒体的首选接口；

3）撰写媒体声明的指导方针或模板；

4）有适当数量的经过培训、称职的发言人，有权向媒体发布信息。

准备好的信息在事故的早期阶段可能特别有用。 它使组织能够在事件的细节仍处于建立阶段时提供有关组织及其业务的详细信息。

可能适合：

-建立一个合适的场所，以支持与媒体或其他利益相关方的联络；

-建立适当数量的合格、训练有素的人员来回答来自新闻界的电话询问；

一使用组织开放的所有通信渠道，包括社交媒体；以及

—准备有关组织及其运作的背景材料（这些信息应事先商定后发布）。

集体对组织有权力或影响力的压力或社区行动小组也需要考虑。

应包括一个确定与其他关键利益方的沟通内容并确定其优先次序的过程。 可能有必要制定一个单独的程序来管理利益相关方，提供确定优先次序的标准，并为向每个利益攸关方或利益攸关方群体分配人员作出规定。

8.4.4.3.3安全和福利程序

组织有直接责任保护员工、承包商、访客和客户的福利，当事件对生命、生计和福利构成直接威胁时。特别需要注意的是，任何有残疾或其他特定需求（如e.g.pregnancy/因伤导致的暂时性残疾）的群体。提前规划以满足这些需求可以降低风险并让受影响的人感到安心。事件的长期影响不容小觑。 制定适当的战略来支持人类福利，可直接促进组织内的身体和情感恢复，这些战略应考虑到相关的社会和文化因素。

应包括的福利应对措施要素：

一现场疏散（包括现场内部避难所活动）和集会地点；

一动员安全、急救和疏散-救援团队；

一定位和清点现场或附近人员。　　还可包括以下内容：

一翻译服务；

一提供交通协助，包括按要求提供路线；

-指定的联络人和紧急服务、适当机构和急救人员的联系方式；

一定位流离失所的劳动力或承包商；

一管理电话求助热线；以及

一康复和咨询（身体和情感）服务。

本组织可保留一种方式，以便在事件发生后向受影响的工作人员提供服务和咨询，并提供长期支持。　　服务可由外部提供，也可作为现有职业健康和雇员援助方案的延伸。

组织应部署具有适当权限的人员，在必要时与应急服务部门联络。应急服务部门在紧急情况下主要负责保护生命和减轻痛苦。因此，组织与其第一响应者及应急服务部门之间的早期联络、预先规划和实时事件协调可以提高事件响应效率。

应明确指出任何所需的资源，资源应能及时提供，并且应具有执行其预期功能的能力。应考虑到对资源使用的限制，而且应用资源不应比不使用资源承担更多的责任。资源的成本不应超过收益。

福利响应可能需要的资源包括但不限于以下内容：设备的位置、数量、可访问性、可操作性和维护（例如。　　重型、防护、运输、监测、去污、响应、个人防护设备）；

一supplies（e.g.medical，个人卫生，消耗品，行政，冰）；

一能源来源（例如：　　电气、燃料)；

-应急发电（发电机）；

一communications系统；—

食物和水；

—技术信息；

一服装和住所；

—专业人员（例如。　　医疗、宗教、志愿组织、灾难/紧急情况管理人员、公用事业工人、殡仪员和私人承包商)；

-专门的志愿者团体(例如。　　业余无线电、宗教救济组织、慈善机构)；

一志愿者、社区和应急响应支持；以及

一外部国际、国家、省、部落、地区和地方机构。

8.4.4.3.4救援和安全程序

组织可以编制书面程序，以处理打捞和安全问题，这可能包括以下方面的指导：

一设施、设备和记录信息的抢救优先级；以及

一一旦由应急服务部门移交，场所的安全。

-组织可在事故发生前任命专门的打捞承包商。对设施、设备和记录信息的有效打捞可限制影响并使恢复正常工作更快。

8.4.4.3.5恢复活动的程序

每个程序应规定：

一优先恢复的活动；

一重新开始的时间范围；

每个优先级活动所需的一恢复级别；以及

一可以使用该程序的情况。

每个部门应详细说明在适当的时间点上为实现目标而需要的资源，这可能包括：

— resourcenumbers;

一技能和资质；

一technical设备；

一电信设施；

-资源的可获得性，包括通过互助达成的合同、协议或可能获得的资源。

如果缺乏服务或资源威胁到恢复活动，应确定升级行动，这些行动可能包括：

一调动外部资源和第三方资源；

一恢复行动的沟通；以及

—执行手动变通方法、系统恢复、替代过程等的程序。 应记录所需资源，可能包括：

一重要记录（纸质和电子版）；

一操作和程序手册；

一IT技术恢复计划和程序；

一组织使用的场外储存设施的位置；

一 alternativelocations;

一有关当局/代表团支付紧急费用；

一拥有运营单位所需专业知识的员工名单；IT基础设施和应用程序文档；

—telecommunications支持来源；

—办公室和专业设备来源；

—公用设施（水、电等）联系人。

8.4.4.3.6信息和通信技术（ICT）系统的恢复

恢复活动的程序应确定其恢复所依赖的信息和通信技术系统，并提及任何现有的信息和通信技术连续性程序。

ICT连续性程序，如有，至少应包括：

—启动所需的信通技术响应，以及部署和调动信通技术人员；

—accessing备份数据并获取替代服务；以及

—数据、信息服务和通信及支持的恢复；

—业务连续性程序中规定了可用性和容量要求的时间表，使活动能够满足其恢复时间目标。

注：可在ISO 27031中找到进一步的指南。

8.4.5恢复

组织应有书面程序，以便在事件后，从为支持正常业务要求而采取的临时措施中恢复和返回业务运营。 这些应满足相关的审计和公司治理要求。

恢复的目的是在发生破坏性事件后重新建立业务活动，以支持正常的业务需求。 恢复正常可能通过以下方式实现：

—修复事故造成的损坏；

—将运营从临时场所迁回恢复的主业务地点；或

—搬到一个新的地点。

如何“恢复正常”的最佳决定将需要根据事故造成的损害的严重程度以及建立必要设施可能需要的时间来做出。

文件化的程序应提供对情况及其影响的详细评估，以及确定恢复所需的任务和步骤。
在恢复期间，组织可能需要：

a)建立恢复资源和基础设施;

b)在回收设施中操作；

c)恢复受损设施；

d)确保紧急采购和资金；

e)损坏设施中的抢救设备；

f)对现有保险单提出索赔；

g)获得额外的人力来支持恢复工作；

h)选择恢复和恢复正常选项；

i)将运营迁移到恢复设施；

j)恢复丢失的文档信息；

k)以适当频率与相关利益方进行沟通；

l)在恢复设施中规范操作；

m）进行恢复后审查；以及

n）对审计和公司治理要求进行尽职调查。

记录的恢复程序应包括规定恢复所有活动，而不仅仅是确定为优先活动的活动。这表明，需要在某个时间点恢复优先级较低的活动，并且需要资源（8.3.2）。

8.5练习和测试

8.5.1概述

一个组织的业务连续性程序和安排只有在实施后才能被认为是可靠的，除非其有效性得到维持。实施是确保已制定的战略、政策、计划和程序充分且符合业务连续性目标的关键。实施过程能够培养团队合作精神、能力、信心和知识，并应包括那些可能需要使用这些程序的人员。

8.5.2训练计划

无论一个程序设计得多么好，经过深思熟虑，一系列稳健和现实的练习将确定改进的领域。

一项锻炼计划应与业务连续性程序的范围一致，并适当考虑到任何相关的法律和法规。

应制定一个演练方案，以在一段时间内客观保证业务连续性程序和安排在需要时能按预期发挥作用。　　该方案应：

a）行使程序的技术、后勤、行政、程序和其他操作系统；

b）对在这些程序中负有责任的所有人员进行培训；

c）实施业务连续性安排和基础设施（包括例如事件管理地点和工作区）；以及

d)验证技术和电信恢复，包括人员的可用性和重新安置。

演习的规模和复杂性应与组织的业务连续性目标相适应。

应制定计划的演习时间表，其频率应取决于组织的需要、其运作环境和有关各方的要求。然而，演习方案应具有灵活性，考虑到组织内部的变化和以前演习的结果。组织发生重大变化时，可安排一次审查修订后的安排的演习。

演习方案应考虑所有各方的作用，包括关键第三方提供者、供应商和其他预期参与恢复活动的各方。一个组织可以将这些各方纳入其演习，并可以参加他们组织的演习。

演习的范围和细节应根据组织的经验、资源和能力，通过方案逐步成熟。　　早期成熟阶段，锻炼和测试可能有限

使用清单、演练和提高认识的练习。 随着方案的成熟，它可能扩展到包括桌面演习和全面的现场模拟。

8.5.3实施业务连续性计划

演习是旨在检验组织在面对特定破坏性情况时，是否能够有效应对、恢复并继续执行指定业务职能的活动。组织应利用演习及其记录的结果，确保其业务连续性计划的有效性和准备状态。

每项练习和测试都应有明确的目标和目的，并且基于适合实现这些目标的场景。

运动可能：

-预期到预先确定的outcome，e.g.are计划和范围；并允许组织开发创新解决方案

。

演习应是现实的、经过仔细计划和与相关方商定的，以使业务流程中断的风险最小化，并且不会因为演习而直接导致事故的发生。 只要不危及被测试目标的完整性，可以在受控和隔离的环境中进行该操作。

组织应设计满足演习目标的演习场景，并可使用风险评估中确定的威胁或其他适当事件。

业务连续性某些方面的有效性将要求特定的个人或占据特定职位的人具备特定的知识、技能和理解。这些知识、技能和理解应在演习之前到位，以便参与者能够将其应用于相关情景和模拟中。

设计和实施的运动应提供以下一项或多项：

a）验证恢复时间目标是否可实现（8.3.1）；

b）确信活动所需的信息是适当最新的（8.3.2.3）；

c)提高对供应商和其他利益相关方业务连续性依赖性的理解；

d)提高对组织环境和优先事项的认识；

e）提高对业务连续性程序内容和使用的理解；

f)提高对事件响应的信心；

g)提高能力的机会；

h）评估业务连续性战略的效用和适用性；

i)对开发的能力和资源分配的充分性进行评估；

j）识别以前未记录的要求和在管理事故或中断中采用的做法；

k)有机会查明书面业务连续性程序及其实施的其他不足之处；

1）确保业务连续性程序能够在需要时得到实施；m）提高利益相关方对组织准备情况的信心；以及

n）满足监管、合同或组织治理要求的手段。

练习可以有各种不同的形式。　　决定是否适合进行演习将取决于BCM的背景、演习的目标、预算和参与者的可用性，以及组织对演习造成的业务中断的容忍度。

ISO 22398（公司安全-演习和测试指南）中描述了主要的演习类型。

作为演习的一部分，应安排所有参与者进行一次审查，讨论问题和吸取的教训。应记录这些信息，并根据需要更新程序。

该组织应进行演习后的总结和分析，以考虑是否实现了演习的目标和目的。应编写一份运动后报告，其中包含建议和实施时间表。

在未来的演习中，应重新审视从演习和实际事故中得到的经验教训。如果演习显示程序存在严重缺陷或不准确之处，则应在采取纠正措施后重新进行演习。

锻炼和测试的好处包括：

一计划范围、假设和策略的确认；

一确保技术设施和资源的正常运行；

一保证备用设施的容量；

-提高效率，减少完成流程所需的时间（例如。　　使用重复练习来缩短反应时间)；

-利益相关方的意识得到提高；

一提高学员的能力和意识。

9业绩评价

9.1监测、测量、分析和评价

9.1.1概述

BCMS的性能和有效性程序应包括设定性能指标；评估优先活动的保护情况；确认符合要求；检查历史证据；以及使用记录信息来促进后续纠正措施。　　程序还应参考业务连续性政策和目标。

监测性能的程序应包括以下内容：

a）设定绩效指标，包括适合组织需求的定性和定量测量；

b)监测组织的业务连续性政策和目标的实现程度；

c)确定何时进行监测和测量；

d）评估保护优先活动的过程、程序和功能的绩效；

e)监测BCMS是否符合相关法规、法定和监管要求的绩效主动措施；

f）用于监控失效、事故、不合格（包括险些发生和误报）和其他BCMS性能缺陷历史证据的性能反应措施；以及

g）记录足够的监测和测量数据和结果，以便于后续的纠正措施分析。

程序应规定定期对组织的业务连续性进行系统性的测量、监测和评价。应制定一套绩效指标来衡量管理体系及其结果，这些指标可以是定量的也可以是定性的，绩效指标可以是管理、运营或经济指标，指标应提供有用的信息来识别成功和需要纠正或改进的领域。

BCMS应提供来自监测和测量的数据，以确定模式并获得有关其性能的信息。应利用这些数据确保组织的政策和目标得以实现，同时确定纠正措施和改进领域。

该组织应能够证明其已确定、评价并遵守了法律要求和它所接受的任何其他要求。

应保存所有定期评价的记录及其结果。

组织应分析并按计划的间隔，评价监测和测量的结果。

9.1.2业务连续性程序评估

组织应对其业务连续性程序进行评价，以确保其持续的适宜性、充分性和有效性。

评估应根据演习结果、事件后审查、变化的情况和持续改进的承诺等事项，解决对政策、目标、战略和BCMS其他要素进行变更的可能需要。

评价可以是内部或外部的审计，也可以是自我评估。评价的频率和时间取决于法律和法规，这取决于组织的规模、性质和法律地位。 它们也可能受到有关当事方要求的影响。

对组织的业务连续性程序进行评估，应确认：

a）已确定所有关键产品和服务及其支持活动和资源，并将其纳入组织的业务连续性战略；

b）组织的业务连续性政策、战略、框架和业务连续性程序准确地反映了其优先事项和要求（组织的目标）；

c）人员能力和组织的业务连续性有效且适合目的，将允许管理层、指挥、控制和协调组织对破坏性事件的响应；

d)本组织的业务连续性解决方案有效、最新且适合用途，且与本组织面临的风险水平相适应；

e）组织的业务连续性维护和演练计划已有效实施；

f)业务连续性战略和程序包括在事件和演习中发现的改进以及在维护计划中发现的改进；

g)本组织有一个持续的业务连续性培训和意识方案；

h）已将业务连续性程序有效地传达给相关员工，且这些员工了解其角色和职责；以及

i）变更控制过程到位并有效运行。

应建立一个明确的、有文件记录的维护计划。该计划应：

-确保对影响组织的任何变更（内部或外部）进行与BCM相关的审查；

-确定需要纳入BCMS的任何新产品和服务及其相关活动；

—确保组织的业务连续性仍然有效、适合目的和最新；以及

—当业务连续性策略或相关业务流程发生重大变更时，可修改现有的计划。

注：评估重大业务变更影响的有效方法是组织尽早审查业务影响分析（8.2.2），并根据结果对BCM的其他要素进行更改。

维护过程的结果应包括：

-有关组织主动管理和治理BCM的书面证据；

-确认负责实施业务连续性战略和程序的关键人员已经接受培训并且有能力胜任；

一验证BCM的运行规划和控制；

-证明组织已评估其业务连续性程序的符合性；以及

——证明组织结构、产品和服务以及活动的重大变化已及时反映在组织的业务连续性程序中。

如果发生事件，导致组织优先级活动中断或需要事件响应，则应进行事件后审查。这可能包括：

一识别事故的性质和原因；

一评估管理层的应对是否充分；

——评估组织在实现其恢复时间目标方面的有效性；

-评估业务连续性安排是否充分，以使员工做好应对事故的准备；

一确定业务连续性安排的改进措施；

-将实际影响与业务影响分析（8.2.2）中考虑的影响进行比较；以及-从利益相关者和参与响应的人员处获得反馈。

在持续改进的背景下，组织可以获取有关新的BCM技术和实践的知识，包括新的工具和技术。这些知识应进行评估，以确定其对组织的潜在益处。

应保存与所有定期评价及其结果有关的书面资料，作为评价的证据。

9.2内部审计

组织应按计划的时间间隔进行内部审核，以确保BCMS符合其自身要求和本国际标准的要求。

对BCMS进行内部审计是十分必要的，以确保BCMS实现其目标，符合其计划安排，并得到适当的实施和维护，同时确定改进的机会。BCMS的内部审计应在计划的时间间隔内进行。

确定并为最高管理层提供BCMS的适当性和有效性信息，为设定BCMS绩效持续改进目标提供依据。

组织应建立一个审计计划（见ISO 19011），以指导计划和开展审计，并确定为满足计划目标所需的审计。方案应根据组织活动的性质、风险评估和影响分析、以往审计结果和其他相关因素制定。

内部审计计划应基于BCMS的全部范围，然而，每次审计不必涵盖整个系统。审计可以分为较小的部分，只要审计计划确保在组织指定的审计期内，所有组织单位、职能、活动和系统要素以及BCMS的全部范围都得到审计。

内部BCMS审核的结果可以以报告的形式提供，用于纠正或防止特定的不符合项，并为管理评审的实施提供输入。

BCMS的内部审计可以由组织内部的人员或由组织选定的外部人员代表组织进行。无论哪种情况，执行审计的人员都应具备相应的资格，并能够公正、客观地进行工作。在较小的组织中，审计师的独立性可以通过其不受被审计活动责任的影响来体现。

9.3管理评审

最高管理者应按计划的时间间隔审查组织的BCMS，以确保其持续的适宜性、充分性和有效性，包括连续性程序和能力的有效运行。

管理评审应包括对以下方面的评价：

一以往评审中行动的现状；

-管理体系的绩效，包括从不符合项和纠正措施中明显看出的趋势、监视和测量的结果以及审核结果；

一组织及其环境（4.1）的变更，可能影响管理体系；以及

一持续改进的机会。

管理评审为最高管理者提供了评价管理体系持续的适宜性、充分性和有效性的机会。管理评审应涵盖BCMS的范围，尽管没有必要一次评审所有要素，评审过程可以分阶段进行。

最高管理层应定期安排并评价对BCMS的实施和结果。虽然建议进行持续的系统审查，但正式审查应有结构，并适当记录和安排在合适的时机。参与实施BCMS并分配其资源的人员应参与管理审查。

除了定期的管理系统审查之外，以下因素可能触发审查，或者在安排审查时应检查：

a）行业趋势：主要行业/部门的倡议应启动BCMS审查。可以使用行业/部门的一般趋势和最佳实践以及业务/运营连续性规划技术进行基准测试；

b）监管要求：新的监管要求可能需要对BCMS进行审查；以及

c）突发事件经验：应对破坏性突发事件做出响应后，无论是否启动响应程序，都应进行审查。如果激活，审查应考虑以下因素

说明响应程序的历史，它是如何工作的，为什么被激活等。 如果未激活响应程序，则评审应检查原因，以及是否为适当决定；

管理评审应提高BCMS的效率和性能，并可能导致以下变更：

一照明范围的变体；

一提高其有效性；

一更新业务连续性程序；

一控制措施的变更及其有效性衡量方法。

组织应保留文件化信息，作为管理评审结果的证据，并且应：

-向相关利益方传达管理评审的结果；

一对这些结果采取适当的行动。

10改进

10.1不符合项和纠正措施

组织应识别不符合项，采取措施控制、遏制和纠正不符合项，处理其后果，并评价消除其原因所需采取的行动。

组织应建立有效的程序，确保及时识别和沟通与BCMS相关的未满足要求、计划方法和弱点，以防止这种情况的进一步发生，并确定和解决根本原因。 程序应能对实际和潜在的不合格原因进行持续检测、分析和消除。

应及时识别和处理不符合项，以及解决不符合项的纠正措施。 纠正措施可能源自明确的不符合项声明，该声明清楚地说明了问题并被理解。

当发现任何不符合项时，应调查其根本原因，并制定纠正措施计划，立即解决问题。该行动计划应旨在减轻任何后果，并确定需要做出的更改以纠正情况、恢复正常运营并消除（或消除）原因，防止问题再次发生。 行动的性质和时机应与不符合项的规模和性质及其潜在后果相适应。

可能发现潜在问题，但不存在实际的不合格。 潜在问题可从内部BCMS审核过程或行业趋势和事件分析中识别的实际不合格项的纠正措施推断出来。 识别潜在的不合格项也可以成为意识到注意和传达潜在或实际问题重要性的人的日常职责的一部分。

建立处理实际和潜在不合格项的程序以及持续采取纠正措施有助于确保BCMS的可靠性和有效性。 程序应规定在计划和执行纠正措施时所承担的责任、权力和步骤。

最高管理者应确保纠正措施得到实施，并且有系统地跟进以评估其有效性。

10.2持续改进

组织应不断改进BCMS的有效性。

持续改进贯穿于PDCA周期的所有层面，并且应该由业务连续性政策和目标、审核结果、监控事件分析、纠正措施和管理评审来驱动。

纠正措施引起的变更应反映在BCMS文件中。

持续改进需要一个过程，该过程能够正确识别问题和不符合项，然后加以解决。该过程应针对问题的性质和问题存在的环境，包括改变环境以确保问题不会再次发生。每一步都应建立和改进前一步，以便改进涵盖更多的方面，而不仅仅是最初确定的问题，并对组织产生更广泛、更有说服力的影响。

纠正措施的实施应被确认为有效，每个措施都应有一个预计完成日期，在该日期之后，组织应确保已执行了规定的措施并且是有效的。如果审查发现行动没有按计划成功，应设定新的行动日期。

持续改进过程应遵循与纠正措施相同的基本流程，包括以下内容：

一确定需要解决的问题和当前状况（不合格）；

一确定当前过程和控制（根本原因）；

一确定要实施的变更（纠正措施）。

纠正措施解决BCMS中的缺陷，确保其按预期运行，而持续改进则将BCMS提升到更高的效率和有效性水平。

参考书目

[1] ISO 19011：2011，管理体系审核指南

[2] ISO 20000 (所有部分），信息技术—服务管理

[3] ISO 223981)，社会安全—演习指南

[4] ISO/ PAS22399：2007，社会安全-事件准备和业务连续性管理指南

[5] ISO 27002：2005，信息技术-安全技术-信息安全管理规范

[6] ISO 27031：2011，信息技术-安全技术-业务连续性信息和通信技术准备指南

[7]ISO 31000：2009，风险管理原则和指南

[8] BSI 25999-1：2006，业务连续性管理—实践准则

[9] BSI 25999-2：2007，业务连续性管理规范

*[10] HB 221：2004，业务连续性管理，澳大利亚标准/新西兰标准，*ISBN0-7337-6250-6

[11] SI 24001：2007，安全和连续性管理系统-使用要求和指南，以色列标准机构

[12] NFPA.1600：2007，灾害/应急管理和业务连续性计划标准，美国国家消防协会（USA）

[13]业务连续性计划起草指南。 日本经济产业省，2005年

*[14]业务连续性准则，中央灾害管理委员会，内阁办公室，政府*日本，2005

[15] ANSI/ ASIS SPC。 1：2009，组织弹性：安全、准备和连续性管理系统-要求及使用指南

[16] ANSI/ ASIS/ BSI BCM.01：2010，业务连续性管理系统：要求和使用指南

[17] SS 540：2008，新加坡业务连续性管理标准

---

1)待出版。

ICS 03.100.01

基于46页的价格