ICS 03.100.01
CCS A 90

中华人民共和国国家标准

GB/T 31595—2025/ISO 22313:2020
代替 GB/T 31595—2015

安全与韧性　业务连续性管理体系　GB/T 30146 使用指南

Security and resilience—Business continuity management systems—Guidance on the use of GB/T 30146

（ISO 22313:2020,Security and resilience—Business continuity management systems—Guidance on the use of ISO 22301,IDT）

2025-10-05 发布　　2026-02-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

本文件按照 GB/T 1.1—2020《标准化工作导则　第 1 部分：标准化文件的结构和起草规则》的规定起草。

本文件代替 GB/T 31595—2015《公共安全　业务连续性管理体系　指南》，与 GB/T 31595—2015 相比，除结构调整和编辑性改动外，主要技术变化如下：

——更改了范围（见第 1 章，2015 年版的第 1 章）；

——删除了“管理承诺”（见 2015 年版的 5.2）；

——增加了“业务连续性管理体系变更的策划”（见 6.3）；

——更改了“沟通”的相关内容（见 7.4，2015 年版的 7.4）；

——将“存档信息”改为“成文信息”（见 7.5，2015 年版的 7.5）；

——将“实施”改为“运行”（见第 8 章，2015 年版的第 8 章）；

——更改了“业务影响分析”的相关内容（见 8.2.2，2015 年版的 8.2.2）；

——更改了“业务连续性策略”的相关内容（见 8.3，2015 年版的 8.3）；

——将“演练和测试”改为“演练方案”（见 8.5，2015 年版的 8.5）；

——增加了“业务连续性文件和能力评价”（见 8.6）；

——将“绩效评估”改为“绩效评价”（见第 9 章，2015 年版的第 9 章）；

——更改了“监控、测量、分析和评价”的相关内容（见 9.1，2015 年版的 9.1.1）；

——删除了“业务连续性程序的评价”（见 2015 年版的 9.1.2）；

——增加了“审核方案”（见 9.2.2）；

——更改了“管理评审”的相关内容（见 9.3，2015 年版的 9.3）；

——更改了“持续改进”的相关内容（见 10.2，2015 年版的 10.2）。

本文件使等同采用 ISO 22313:2020《安全与韧性　业务连续性管理体系　ISO 22301 使用指南》。

本文件做了下列最小限度的编辑性改动：

——为与现有标准协调，将标准名称改为《安全与韧性　业务连续性管理体系　GB/T 30146 使用指南》。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件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。

本文件起草单位：北京市科学技术研究院、中国标准化研究院、中国科学技术大学、国家市场监督管理总局认证认可技术研究中心、北京科技大学、厦门民航凯亚有限公司。

本文件主要起草人：王晶晶、孟祥程、王亚飞、王皖、朱伟、周倩、潘英、徐凤娇、秦挺鑫、王春凯、庞磊、王健、肖丽妮。

本文件及其所代替文件的历次版本发布情况为：

——2015 年首次发布为 GB/T 31595—2015；

——本次为第一次修订。

引　言

0.1　总则

本文件旨在为 GB/T 30146 中规定的要求提供指南，而非为业务连续性的所有方面提供通用指南。

本文件虽然和 GB/T 30146 包括相同的条款标题，但不会重述其要求以及相关术语和定义。

本文件旨在解释并阐明 GB/T 30146 中要求的含义和目的，并帮助理解 GB/T 30146。本文件中引用并提供补充指导的国际标准和国家标准包括 GB/T 35625、GB/T 38299、GB/T 40054、ISO 22330、ISO 22331 及 GB/T 38209。这些文件的范围可能超出 GB/T 30146 的要求。因此，组织宜始终参考 GB/T 30146 来验证所要满足的要求。

本文件使用的图示是为了进一步阐明和解释要点。这些图示仅用于说明性目的，相关内容优先参考本文件正文。

业务连续性管理体系强调以下方面的重要性：

a) 建立与组织目标一致的业务连续性方针和目标；

b) 运行并保持过程、能力与响应机制，确保组织能经受住冲扰；

c) 监控和评审业务连续性管理体系绩效和有效性；

d) 基于定性和定量测量的持续改进。

业务连续性管理体系与其他管理体系类似，包括以下组成部分。

a) 方针。

b) 具备相应能力且职责明确的人员。

c) 涉及以下内容的管理过程：

1) 方针；

2) 策划；

3) 实施和运行；

4) 绩效评估；

5) 管理评审；

6) 持续改进。

d) 支持运行控制和绩效评价的成文信息。

业务连续性通常是针对某一组织而言的，然而其实施可能会对更广泛的群体及第三方产生深远影响。组织很可能依赖于一些外部组织，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构建更具韧性的社会。

0.2　业务连续性管理体系的效益

业务连续性管理体系提高了组织在冲扰期间持续运行的准备水平，还可改进对组织内外部关系的理解，更好地与相关方沟通，创造持续改进的环境。按照本文件中的建议和 GB/T 30146 的要求，实施业务连续性管理体系可带来许多其他的效益。

a) 按照第 4 章(“组织环境”)，组织：

1) 评审其战略目标，以确保业务连续性管理体系支持这些目标；

2) 重新考虑相关方的需求、期望和要求；

3) 了解适用的法律法规和其他义务。

b) 按照第 5 章(“领导力”)，组织：

1) 重新考虑管理的角色和职责；
2) 推动建设持续改进文化；
3) 分配绩效监控和报告的职责。

c) 按照第6章(“策划”),组织：
1) 重新审视其风险和机会,并找到应对和利用措施；
2) 建立有效的变更管理。

d) 按照第7章(“支持”),组织：
1) 建立对业务连续性管理体系资源的有效管理,包括能力管理；
2) 提高员工对管理重要事项的认识；
3) 具有有效的内部和外部沟通机制；
4) 有效管理文件。

e) 按照第8章(“运行”),组织需考虑：
1) 变化的意外后果；
2) 业务连续性优先级和要求；
3) 依赖关系；
4) 从影响角度看待脆弱性；
5) 冲扰风险,并确定最佳应对方法；
6) 在资源有限的情况下业务运行的替代方案；
7) 处理冲扰的有效结构和程序；
8) 对社会和其他相关方的职责。

f) 按照第9章(“绩效评价”),组织：
1) 具有有效的监控、测量和绩效评价机制；
2) 管理者参与监控业务连续性管理体系的绩效并对其有效性作出贡献。

g) 按照第10章(“改进”),组织：
1) 具有监控绩效和提高有效性的程序；
2) 受益于管理体系的持续改进。

因此,实施业务连续性管理体系能：

a) 保护生命、资产和环境；
b) 保护和提高组织的声誉与信誉；
c) 使其在冲扰期间运行,有助于提高组织竞争优势；
d) 减少因冲扰产生的成本,并提高组织在冲扰期间保持有效的能力；
e) 有助于组织的整体韧性建设；
f) 有助于相关方对组织的成功更有信心；
g) 减少组织的法律和财务风险；
h) 证明组织管理风险和解决运行脆弱性的能力。

0.3 策划—实施—检查—改进(PDCA)循环

本文件应用策划—实施—检查—改进(PDCA)循环,从而策划、建立、实施、运行、监控、审查、保持和持续改进组织业务连续性管理体系的有效性。PDCA循环的说明见表1。

图1说明了业务连续性管理体系把相关方的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业务连续性成果(即受控的业务连续性)。

表 1　PDCA 循环说明

策划 （建立）	建立与改进业务连续性相关的业务连续性方针、目标、过程和程序，并与组织的总方针和目标一致
实施 （执行和运行）	实施和运行业务连续性的方针、过程和程序
检查 （监控和评审）	根据业务连续性方针和目标对绩效进行监控和评审，并将结果报告管理者以供评审，确定并授权采取补救和改进措施
改进 （保持和改进）	根据管理评审的结果和对业务连续性管理体系范围、业务连续性方针和目标的重新评估，采取纠正措施，保持和持续改进业务连续性管理体系

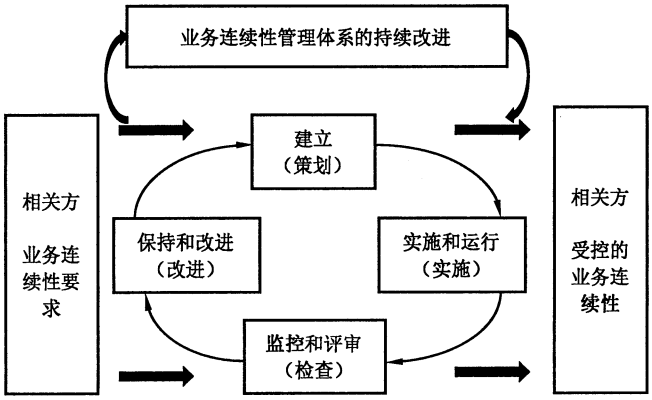

图 1　应用于业务连续性管理体系过程的 PDCA 循环

0.4　本文件中 PDCA 的组成

本文件中各章节和图 1 内容间对应关系如表 2 所示。

表 2　PDCA 循环与第 4 章～第 10 章的对应关系

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”），组织如何满足业务连续性管理体系要求，并考虑所有相关的内外部因素，包括： ——相关方的需求和期望； ——法律法规义务； ——业务连续性管理体系要求的范围
	第 5 章（“领导力”），管理者在证明承诺、确定方针、分配角色和职责方面的关键作用
	第 6 章（“策划”），为实施业务连续性管理体系建立战略目标和指导原则的措施
	第 7 章（“支持”），支持业务连续性管理体系所需的要素，即资源、能力、意识、沟通和成文信息
实施 （实施和运行）	第 8 章（“运行”），建立和保持业务连续性的过程
检查 （监控和评审）	第 9 章（“绩效评价”），通过绩效测量和评价，为改进业务连续性管理体系提供基础
改进 （保持和改进）	第 10 章（“改进”），解决通过绩效评价识别的不符合的纠正措施

0.5 本文件的内容

本文件的目的不是要建立统一的业务连续性管理体系结构，而是为组织设计适合其自身需求并满足相关方要求的业务连续性管理体系。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构成。

本文件不可用于评估组织的能力是否满足其业务连续性要求，也不能用于评估是否满足其客户、法律法规的要求。有此需求的组织可使用 GB/T 30146。

第 1 章～第 3 章阐述了范围、规范性引用文件以及适用于本文件使用的术语和定义。第 4 章～第 10 章包含对 GB/T 30146 中要求的使用指南。

本文件运用了下列助动词：

a) “宜”表示建议；

b) “可”表示许可；

c) “能”表示一种可能性或能力。

0.6 业务连续性

业务连续性是在冲扰发生后，组织在预先定义的可接受的水平上连续交付产品或提供服务的能力。业务连续性管理是实施和保持业务连续性的过程(见 8.1.2 和图 5)，以预防、减轻和管理损失，并为冲扰做好准备。

建立业务连续性管理体系使组织能控制、评价和持续改进其业务连续性。

本文件中，“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，适用于大型、中型、小型的工业、商业、公共和非营利组织。

冲扰有可能中断组织的整个运营及其交付产品和服务的能力。但是，在冲扰发生前实施业务连续性管理体系，而不是在突发事件发生后以非计划的方式进行响应，将使组织能够在所受影响尚未严重到不可接受之前恢复运营。

业务连续性管理包括：

a) 识别组织的产品和服务，以及交付这些产品和服务的活动；

b) 分析不恢复相关活动所造成的影响，以及活动所依赖的资源；

c) 了解冲扰的风险；

d) 确定恢复产品和服务交付的优先级、时间范围、能力和策略；

e) 制定解决方案和计划，在冲扰发生后所要求的时间范围内继续活动；

f) 确保这些计划得到例行评审和更新，从而使其在各种情况下都有效。

组织的业务连续性管理方法及其成文信息宜与其环境(如：运营环境、复杂性、需求、资源)相适应。

业务连续性对处理突发冲扰(如爆炸)和渐进冲扰(如大流行病)均有效。

造成活动冲扰的突发事件非常多，其中许多是难以预测和分析的。由于业务连续性关注冲扰带来的影响而不是其产生的原因，所以业务连续性使组织能够确定对其履行义务重要的活动。通过业务连续性，组织能认识到在冲扰发生前需要做哪些准备来保护其资源(如：人、场地、技术和信息)、供应链、相关方以及声誉。基于该认识，组织能将响应机制落实到位，从而有信心管理冲扰的影响。

图 2 和图 3 从概念上说明在某种情况下业务连续性如何有效地减轻影响，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长度。

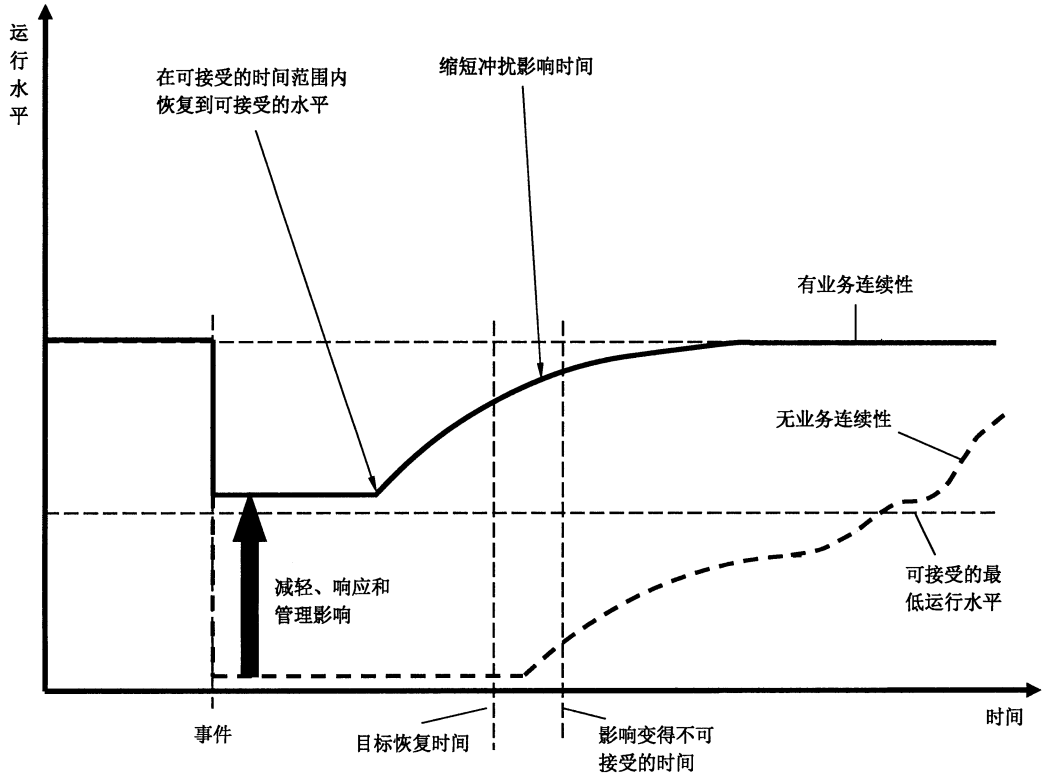

图 2　业务连续性对突发冲扰有效

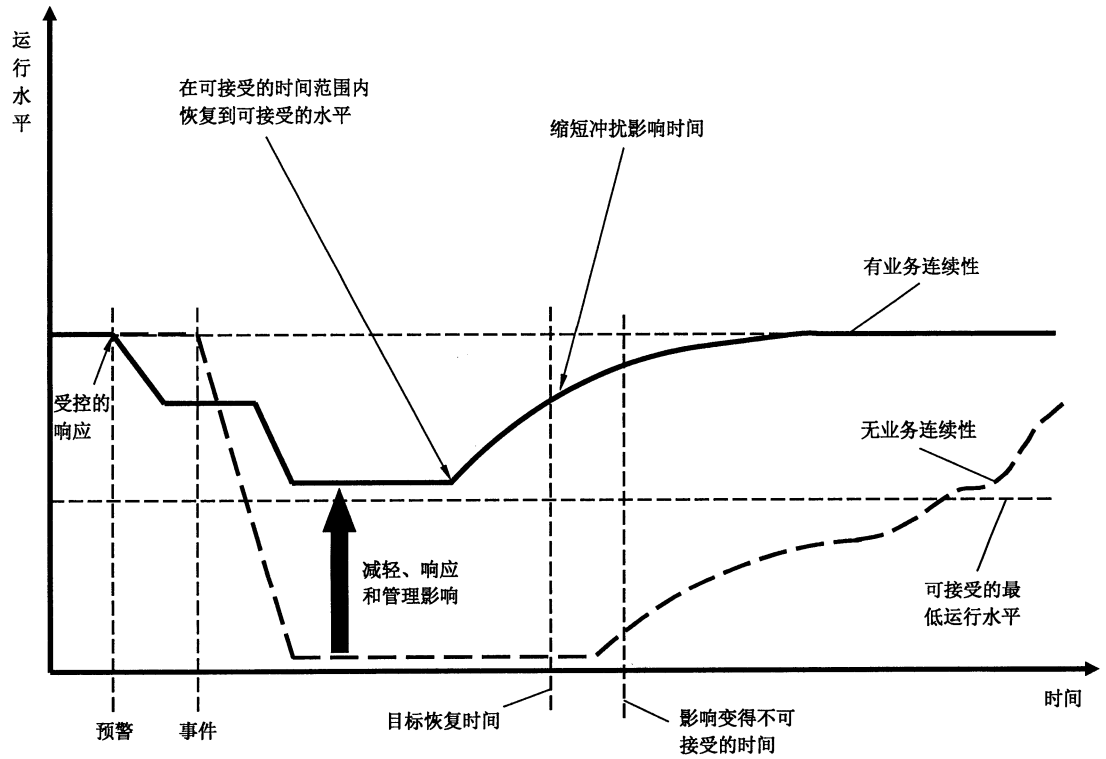

图 3　业务连续性对渐进冲扰有效(如:即将爆发的大流行病)

安全与韧性　业务连续性管理体系 GB/T 30146使用指南

1　范围

本文件为应用GB/T 30146业务连续性管理体系(业务连续性管理体系)的要求提供了指南和建议。这些指南和建议以良好的国际实践为基础。

本文件适用于组织：

a)　实施、保持和改进业务连续性管理体系；

b)　确保符合既定的业务连续性方针；

c)　需要能够在冲扰期间以可接受的预定能力连续交付产品和服务；

d)　试图通过有效运用业务连续性管理体系增强其韧性。

本文件适用于所有规模和类型的组织应用GB/T 30146建立业务连续性管理体系，采用的方法取决于组织的运行环境和复杂性。

2　规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 22300　安全与韧性　术语(Security and resilence—Vocabulary)

注：GB/T 44483—2024　安全与韧性　术语(ISO 22300:2021,MOD)

ISO 22301　安全与韧性　业务连续性管理体系　要求(Security and resilience—Business continuity management systems—Requirements)

注：GB/T 30146—2023　安全与韧性　业务连续性管理体系　要求(ISO 22301:2019,IDT)

3　术语和定义

ISO 22300、ISO 22301界定的术语和定义适用于本文件。

4　组织环境

4.1　理解组织和组织环境

本条为理解业务连续性管理体系相关的组织环境提供建议。建立和保持业务连续性的建议见8.1。

组织宜评估和理解其总体目标相关的内部和外部事项(包括需考虑的积极和消极因素或条件)、产品和服务，以及它可以承担或不可承担的风险的数量和类型。组织在实施和保持其业务连续性管理体系时宜考虑这些信息并排列优先级。

组织相关的外部环境包括：

a)　国际、国家、地区或本地的政治、法律和监管环境；

b)　社会和文化环境；

c) 国际、国家、地区或本地的金融、科技、经济、自然和竞争环境；
d) 供应链的承诺和关系(见 GB/T 38299)；
e) 影响组织目标和运行的驱动因素(如：风险、技术)和趋势；
f) 组织外部相关方的关系、理念和价值观；
g) 用于明确和形成这些关系的沟通渠道，包括社交媒体。

组织相关的内部环境包括：

a) 产品和服务、活动、资源、供应链以及和相关方的关系；
b) 资源和知识方面的能力(如：资本、时间、人员、过程、系统和技术)；
c) 现有的管理体系；
d) 信息和数据(以实物或电子形式存储)以及决策制定过程(正式和非正式的)；
e) 组织内部相关方，包括内部供应商[考虑服务等级协议(SLA)、已评估的韧性和恢复安排，GB/T 38299]；
f) 方针和目标，以及实现它们的策略；
g) 未来机会和业务优先级；
h) 理念、价值观和文化；
i) 组织采用的标准和参考模型；
j) 组织结构(如：管理，角色和责任)；
k) 用于在员工之间交换信息的内部沟通渠道(如：社交媒体)。

4.2 理解相关方的需求和期望

4.2.1 概述

4.2.1.1 组织对组织内外的人员负有关注义务(见 ISO/TS 22330)。在建立业务连续性管理体系时，组织宜确保考虑所有相关方的需求和要求。

4.2.1.2 组织宜识别与其业务连续性管理体系相关的所有相关方(见图 4)，并基于相关方的需要和期望确定其要求。识别强制的、阐明的和隐含的要求很重要。

4.2.1.3 在策划和实施业务连续性管理体系时，重要的是识别相关方适用的措施，并对其进行区分。如，在冲扰发生后适宜与所有相关方进行沟通，而实施和保持业务连续性管理(见 8.1.2)时不适宜与所有相关方进行沟通。

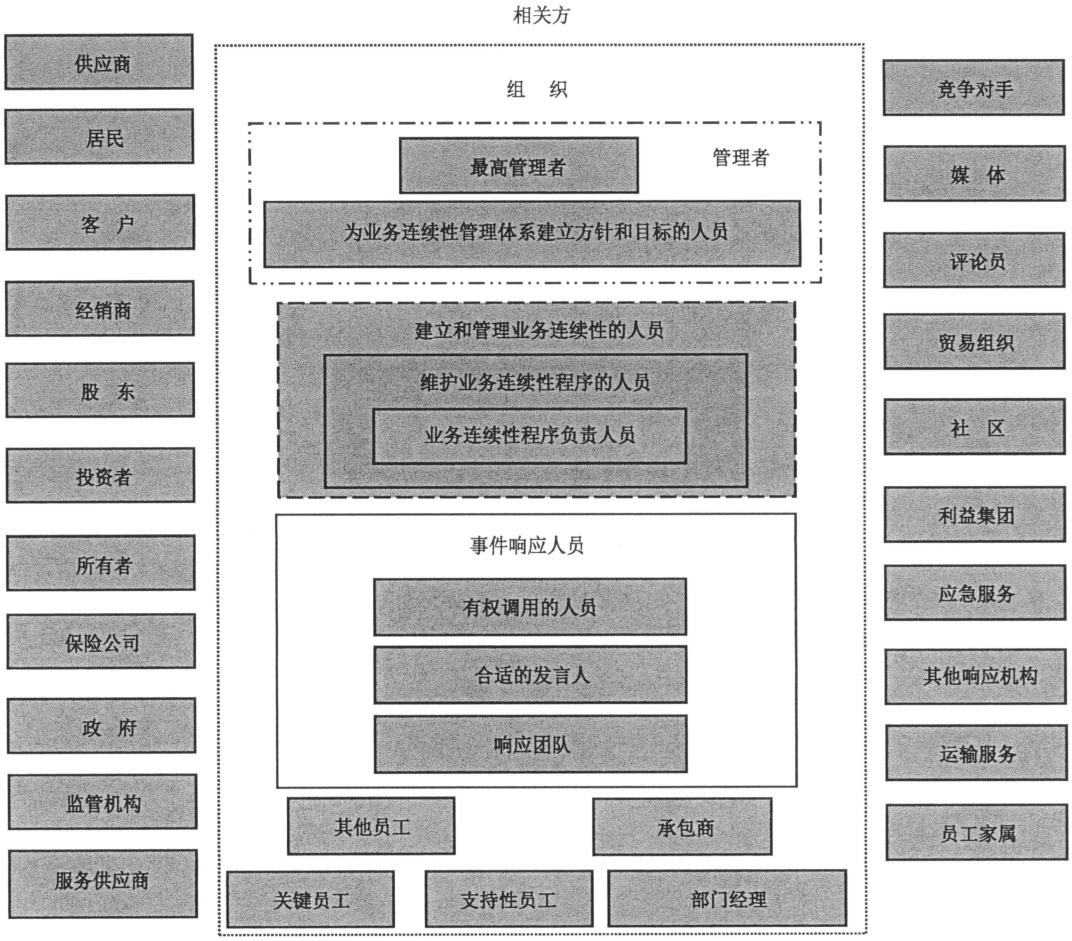

图 4 组织或企事业单位需考虑的相关方的示例

4.2.2 法律和法规要求

4.2.2.1 应用本文件的前提是了解适用的法律和法规要求。

4.2.2.2 这些要求可能是隐含的、阐明的或强制性的。有关这些要求的信息宜形成文件，并及时更新。新的要求或对现有要求的变更宜通知受影响的员工和相关方。

4.2.2.3 组织宜表明其可以获得与运营相关的现行和待定的法律法规要求，以及如何满足这些要求。要求可能包括：

a) 突发事件响应，包括应急管理和其他相关法律；

b) 业务连续性，可能规定方案的范围、恢复的程度或速度；

c) 风险，定义风险管理的范围或方法的要求；

d) 危险(如与危险品存放场所相关的运行要求)。

多场所经营的组织还要满足不同司法管辖区的要求。

4.3 确定业务连续性管理体系的范围

4.3.1 概述

4.3.1.1 确定业务连续性管理体系范围的目的是识别其边界和适用性，以确保覆盖所有相关产品和服务、活动、场所、资源、供应商和其他依赖关系。

4.3.1.2 范围宜包括 4.1 中确定的事项、4.2 中确定的相关方要求以及组织的使命、目标和义务。

4.3.1.3 组织宜准备一份声明，以适合组织规模、性质和复杂性的方式，描述业务连续性管理体系的范围。该声明宜提供给相关方。

4.3.2 业务连续性管理体系的范围

4.3.2.1 组织宜包括以下内容。

a) 参考产品和服务，确定业务连续性管理体系范围包括或排除组织的哪些部分，如：
   1) 仅包括向一个国家或地区交付特定产品；
   2) 排除一个不再可行或对组织价值不高的产品；
   3) 仅包括产品及服务的一部分。
b) 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。

4.3.2.2 范围可：

a) 包括业务连续性管理体系将应对的突发事件规模或严重程度的说明；
b) 识别业务连续性管理体系如何融入组织的业务战略和风险管理方法。

4.3.3 范围删减

4.3.3.1 范围确定了业务连续性管理体系适用的场所、产品和服务、活动和资源。即使没有在范围声明中明确确定，所有依赖关系也都在范围内。例如，如果一家制造公司将一款产品纳入其业务连续性管理体系范围，那么在任何场所直接或间接参与向客户交付该产品的原材料供应、加工、交付和所有支持功能(如数据处理，采购和人力资源)，都将包含在范围内。

4.3.3.2 删减的范围不宜影响组织满足由业务影响分析确定的业务连续性要求(见 8.2.2)的能力。不能删减交付范围内产品和服务必需的活动、资源和供应链。

4.3.3.3 业务连续性管理体系范围的删减宜形成文件并阐明原因。

4.3.3.4 如将业务连续性管理体系整合到现有的管理体系中，组织宜确保业务连续性管理体系的所有要素都包括在内。

4.4 业务连续性管理体系

本条的目的是强调组织实施和保持过程的必要性，使业务连续性管理体系能够满足 GB/T 30146 的要求，其中包括过程之间的相互作用。

在确定过程及其在整个组织中的应用时，组织宜：

a) 确定这些过程中所需的输入和预期的输出；
b) 确定这些过程的顺序和相互作用；
c) 确定和应用确保这些过程有效运行和控制所需的准则和方法(包括监控、测量和相关绩效指标)；
d) 确定这些过程所需的资源并确保其可获得性；
e) 分配这些过程的职责和权限；
f) 应对 6.1 中确定的风险和机会；
g) 评估这些过程，并实施所需的变更，以确保这些过程达到预期的结果；
h) 改进过程和业务连续性管理体系。

必要时，组织宜：

a) 维护成文信息以支持其过程的运行；
b) 保留成文信息以确保过程正在按计划进行。

5 领导力

5.1 领导力和承诺

5.1.1 概述

组织的各级管理者宜证明其在职责范围内的领导力和承诺。

5.1.2 最高管理者

最高管理者宜通过以下方式证明其领导力和承诺：

a) 分配管理角色并确保其履行职责(见 5.1.3)；
b) 建立业务连续性方针(见 5.2)；
c) 任命一名或多名具有适当权限和能力的人员负责业务连续性管理体系，并对其有效运行负责(见 5.3)；
d) 沟通业务连续性和符合业务连续性管理体系要求的重要性；
e) 使必要的资源可获得，包括适当水平的资金(见 7.1)；
f) 推动持续改进(见 10.2)；
g) 确保实现业务连续性管理体系的预期结果；
h) 为其他级别的管理者提供支持，使他们能够证明其在职责范围内的领导力和承诺。

5.1.3 其他管理角色

其他管理者宜通过下列方式证明其领导力和承诺：

a) 建立与组织战略目标相契合的业务连续性目标(见 6.2)；
b) 将业务连续性管理体系要求整合到组织的业务过程中(见 8.1)；
c) 熟知适用的法律、法规和其他要求(见 4.2.2)；
d) 建立业务连续性管理体系的角色、职责和能力(见 5.3 和 7.2)；
e) 实现业务连续性管理体系的预期结果；
f) 积极参与演练方案(见 8.5)；
g) 进行业务连续性管理体系内部审核(见 9.2)；
h) 对业务连续性管理体系进行有效的管理评审(见 9.3)；
i) 指导并支持业务连续性管理体系的改进(见第 10 章)。

也可以通过以下方式证明其管理承诺：

a) 通过指导委员会参与运营；
b) 将业务连续性作为管理者会议的常设议题。

5.2 方针

5.2.1 建立业务连续性方针

5.2.1.1 最高管理者宜根据组织的目标和义务确定业务连续性方针，并确保其：

a) 是最高管理者对业务连续性管理体系的意图和方向的简明的、高层级的声明；
b) 符合组织的宗旨(与组织的规模、性质和复杂度相适应并反映组织的文化、依赖关系和运行环境)；
c) 为目标的制定提供框架；
d) 包含满足相关适用要求的明确承诺，包括法律和法规所规定的义务；

e) 包含持续改进业务连续性管理体系的承诺。

5.2.1.2 方针宜：

a) 明确组织业务连续性的范围和边界，包括限制范围和删减范围(见 4.3)；

b) 识别权限和授权要求，包括负责组织业务连续性管理体系的人员或人群(见 5.3)；

c) 包括参考的标准、指南、法规或者业务连续性管理体系考虑或遵从的方针。

5.2.1.3 业务连续性方针可包括：

a) 资金承诺；

b) 所参考的其他相关方针；

c) 实施业务连续性的要求；

d) 演练和保持业务连续性的承诺。

5.2.1.4 对于已有管理体系的组织，可能适合将业务连续性管理体系方针与其他管理体系的方针整合。

5.2.1.5 组织宜制定适当的规定来审批方针、保存相关成文信息，并定期(如年度)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。

5.2.2 沟通业务连续性方针

业务连续性方针宜：

a) 可获得并作为成文信息保存；

b) 在组织内部得到沟通、理解和应用；

c) 经管理者批准后提供给相关方。

5.3 角色、职责和权限

5.3.1 最高管理者宜确保在业务连续性管理体系内对职责和权限进行分配和传达。

5.3.2 最高管理者中宜有一人负责业务连续性管理体系。组织的最高管理者可以任命其他机构(如指导委员会)监督业务连续性管理体系的实施和持续监控。就其他职责而言，宜任命代表，明确其角色、职责和权限，以：

a) 确保业务连续性管理体系符合业务连续性方针；

b) 向最高管理者汇报业务连续性管理体系的绩效以便于评审并作为改进的基础(见第 9 章和第 10 章)；

c) 在组织中提升业务连续性的意识(见 7.3)；

d) 确保制定的突发事件响应程序有效(见 8.4.4.2.2)。

5.3.3 管理代表可：

a) 被授予特定职务(如："业务连续性经理""业务连续性官"或"韧性经理")；

b) 在组织中负有其他职责；

c) 来自组织的任何领域。

5.3.4 可指派来自组织每个职能部门或区域的代表来协助实施业务连续性管理体系(如负责风险相关事务的人员)。他们的角色、义务、责任和权限宜写入其工作职责描述中，并通过将其纳入组织的评估、奖励和表彰方针而得到强调。表 3 列举了适用于业务连续性管理体系的角色和职责的示例。

注：适合于应对突发事件和重续活动的团队及其职责的示例见表 5(见 8.4.4)。

5.3.5 根据组织的规模，表 3 中列出的角色和职责可以用不同的方式设置。重要的是要确保所有的职责都有角色担任，并有一个负责人。

5.3.6 业务连续性管理体系的所有角色、职责和权限都宜被明确、存档和审核。

表 3　业务连续性管理体系角色和职责示例

角色	职责
最高管理者代表	——对业务连续性管理体系承担责任； ——在管理评审中代表业务连续性管理者
业务连续性经理	——负责业务连续性管理体系工作； ——建立并证明对业务连续性方针的承诺； ——领导所有的项目活动，并协调职能部门； ——提名具有适当资历、权限和能力的团队成员； ——协助审批解决方案、程序和演练方案； ——在管理评审会议上提出团队建议
业务连续性管理团队	——在整个组织中实施业务连续性管理； ——维护成文信息； ——确保及时评审方案； ——评估各职能部门的业务连续性的充分性； ——组织和协调业务连续性意识提升方案； ——制定演练方案并寻求相关部门的批准； ——演前简报和演后汇报； ——及时向相关方通报方案情况； ——确保演练按演练计划进行； ——确保内部审核和管理评审按时进行； ——维护与职能部门的关系，并在冲扰期间保持联系； ——确保及时实施纠正措施计划； ——推进职能代表/协调员的工作
职能代表	——维护业务连续性程序； ——向业务连续性经理通报准备状态； ——根据指示执行并报告方案活动； ——确认供应商的连续性计划已经测试和维护； ——协调人员参加演练； ——维护业务连续性演练记录； ——及时通知团队可能影响业务连续性的变更； ——及时跟进纠正措施的实施效果； ——向业务连续性经理汇报纠正措施的进展情况

6　策划

6.1　应对风险和机会的措施

6.1.1　确定风险和机会

6.1.1.1　确定和应对风险与机会使组织能够：

a）　确保业务连续性管理体系能够实现其预期结果；

b）　预防或减少不良影响；

c）　实现持续改进。

6.1.1.2 组织宜确定措施以处理4.1中确定的事项、4.2中确定的相关方的需求和期望以及4.2.2中确定的法律法规要求。

6.1.1.3 该决定宜包括对风险和机会的考虑及其对业务连续性管理体系有效性的潜在影响。风险和机会可能来自：

a) 缺乏最高管理者的领导和承诺；
b) 业务连续性管理体系资金不足导致响应不力；
c) 成文信息不足；
d) 缺乏具有经证实能力的人员；
e) 管理评审过程不到位；
f) 无法进入要求业务连续性的新业务领域。

6.1.2 应对风险和机会

组织宜以下列方式策划应对这些风险和机会所需的措施：

a) 预防意外结果；
b) 利用一切机会改进业务连续性管理体系；
c) 将这些措施在业务连续性管理体系的过程中进行整合(见8.1)；
d) 确保可获取成文信息以评估措施是否始终有效(见9.1)。

6.2 业务连续性目标及实现计划

6.2.1 建立业务连续性目标

组织宜建立实施和保持业务连续性管理的目标(见第8章)。这些目标宜与组织的总体目标相一致，并明确职责，设定适当的、现实的完成指标。宜在整个组织内传达目标的实现计划，监控并记录其实施过程。

随着业务连续性管理体系的发展，宜定期评审目标实现计划，并及时更新。

6.2.2 确定业务连续性目标

在确定业务连续性目标时，组织宜确保明确规定：

a) 要做什么；
b) 需要的资源；
c) 由谁负责；
d) 完成日期；
e) 如何评估结果。

以下业务连续性目标的示例在某些情况下符合GB/T 30146规定的要求：

a) “最高管理者将分配必要的资源，以确保按期为所有产品和服务建立符合GB/T 30146的业务连续性管理体系”；
b) “A总监将与×××咨询公司合作，按期为指定产品和服务获得GB/T 30146认证”；
c) “最高管理者将利用现有资源确保按期拥有符合GB/T 30146的业务连续性，以满足我们对指定客户的义务”；
d) “IT总监将与我们的供应商合作，将支持指定产品和服务的活动的恢复时间缩短10%，并如期实现”；
e) “在不动用额外资源的情况下，生产经理将按期准备好符合GB/T 30146并保护指名产品和服务的业务连续性管理”。

6.3 业务连续性管理体系变更的策划

变更管理是所有管理过程都要考虑的重要事项。

宜仔细策划业务连续性管理体系的变更，包括 10.1 中确定的变更，以确保预期目的得到充分研究和理解。其中宜考虑包括提议变更的后果、预期的和意外的后果、同时确保业务连续性管理体系的完整性。

组织还宜确保可获得适当和充分的资源，必要时分配或重新分配职责和权限。

7 支持

7.1 资源

7.1.1 概述

组织宜确定业务连续性管理体系所需的资源并确保资源有效、可用，这将：

a) 实现其业务连续性方针和目标；
b) 满足组织的变化要求；
c) 能就业务连续性管理体系相关事宜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持。

7.1.2 业务连续性管理体系资源

当识别业务连续性管理体系所需的资源时，组织宜提供适当的支持。

a) 人员及相关资源，包括：
   1) 履行业务连续性管理体系角色和职责所需的时间；
   2) 培训、教育、意识和演练；
   3) 业务连续性管理体系人员的管理。
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)系统，包括支持有效和高效方案管理的应用程序；
d) 管理和控制所有形式的成文信息；
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。该评审宜有最高管理者的参与。

7.2 能力

7.2.1 组织宜建立一个适当而有效的体系来管理在该体系控制下承担业务连续性管理体系工作的人员的能力。管理者宜确定所有业务连续性管理体系角色和职责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：

a) 对所承担的角色进行能力评价；
b) 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；
c) 提供培训和辅导，包括挑选适当的方法和资料；
d) 绩效评价；
e) 知识分享；
f) 工作分担；

g) 雇佣或与能胜任人员签订工作合同；
h) 目标团队的培训；
i) 记录并监督所接受的培训；
j) 根据培训需求和要求对所接受的培训进行评估以证明与业务连续性管理体系培训要求相一致；
k) 必要时，改进发展方案。

7.2.2 组织宜有识别和交付所有参与者的业务连续性培训需求，并对其交付的培训效果进行评估的过程。

7.2.3 建立、管理和保持业务连续性管理体系的适当的培训类型如下：
a) 建立并管理业务连续性管理体系；
b) 开展业务影响分析；
c) 开展风险评估；
d) 沟通技能；
e) 项目管理；
f) 开发和实施业务连续性文档；
g) 执行演练方案。

7.2.4 通过以下方式可加强能力：
a) 将业务连续性管理体系的业绩纳入组织的奖励和认可过程；
b) 将业务连续性管理体系的业绩纳入组织的绩效和评价过程；
c) 将业务连续性管理体系的角色、责任、职责和权限纳入组织的职位描述和技能要求；
d) 业务人员和最高管理者要积极参与演习、演练和测试。

7.2.5 组织宜要求承包商证明在其管理下工作的人员具备业务连续性管理体系所要求的能力并能胜任他们所履行的响应角色。

7.3 意识

7.3.1 组织宜确保在其管理下工作的人员(如：员工、承包商、供应商)了解业务连续性方针和业务连续性目标，以及：
a) 如何减少冲扰的可能性及其在识别突发事件、减轻、自我保护、疏散、响应、连续性和恢复中的角色；
b) 遵守业务连续性方针和程序的重要性；
c) 对供应商和外部合作方的依赖关系以及与业务目标相关的风险；
d) 组织运营的变化所带来的影响；
e) 他们对业务连续性管理体系有效性的贡献，包括改进业务连续性的效益；
f) 他们在实现其要求中的角色和职责。

7.3.2 组织宜在组织文化中建立、推动和融入业务连续性管理，以：
a) 使其成为组织核心价值观和管理的一部分；
b) 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。

7.3.3 将业务连续性管理融入组织文化中：
a) 更有效地开展业务连续性；
b) 使相关方(尤其是员工和客户)对组织处理冲扰的能力建立信心；
c) 通过确保在各级决策中都考虑了业务连续性理念以持续增强组织的韧性；
d) 降低冲扰的可能性和影响。

7.3.4 将业务连续性管理融入组织文化要依靠：
a) 组织全员参与；
b) 在整个组织中传播领导力；

c) 职责分配；
d) 绩效指标的测量及应用；
e) 将业务连续性融入组织日常管理实践；
f) 意识提升；
g) 技能培训；
h) 对业务连续性计划进行演练。

7.3.5 意识提升方案可包括：

a) 与组织中所有员工就建立和管理业务连续性管理进行协商的过程；
b) 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；
c) 将业务连续性纳入相关网页；
d) 将业务连续性管理纳入员工和管理团队会议的议题；
e) 对事后报告的选择性地公开发布；
f) 向最高管理者做简报；
g) 参观选定的备用场所(如恢复场所)；
h) 定期与供应商沟通，以确保他们了解组织的业务连续性要求，并能证明他们有能力满足约定的连续性能力。

7.3.6 业务环境和运营的变化会影响业务连续性活动的策划、设计和实施的方法。组织可通过积极参与行业业务连续性相关活动等方式来证明对业务连续性管理趋势的认知，可包括：

a) 成为行业利益团体成员；
b) 成为会议组织委员会成员；
c) 在会议和研讨会上发言；
d) 参加本地或国际业务连续性会议。

7.4 沟通

7.4.1 组织宜确定与业务连续性管理体系相关的沟通事宜。

7.4.2 与业务连续性管理体系相关的沟通使组织能够响应相关方的需求和期望(见 4.2)。为使沟通有效，组织宜确定并在适当时制定确定下列事项的准则。

a) 沟通内容：根据组织的性质和情况，可能需要就业务连续性管理体系进行沟通。如一些组织有法律法规义务进行沟通。
b) 沟通时间：可能存在一些阈值，超过这个阈值，组织就必须进行沟通，组织的环境可决定宜沟通的频次。
c) 沟通对象：所有相关方都需要适时进行沟通，因此重要的是对每个相关方，确定必须与其沟通的情况以及沟通的优先级。
d) 沟通方式：提前确定沟通的方法、工具和渠道，包括备选方案，使组织能够有效沟通。
e) 沟通执行人员：组织宜确定其发言人，指定特定人员作为沟通联络人。

7.4.3 在供应商和客户的通讯和简报里，组织也可对其业务连续性管理体系和业务连续性的安排进行介绍。

7.4.4 组织宜将有效的外部沟通作为其意识提升方案的一部分(见 7.3)，并在突发事件响应过程中提供有效的外部沟通(见 8.4.4)。

7.5 成文信息

7.5.1 概述

7.5.1.1 GB/T 30146 要求的成文信息为管理体系满足要求以及有效运行的证据。

7.5.1.2 “程序”指完成某项活动或过程的既定途径。“成文的程序”是指该程序宜在合适的介质上建立并维护。

7.5.1.3 单个文档可解决一个或多个成文的程序的要求，成文的程序的要求可能包含在多个文档中。

7.5.1.4 成文信息包括：

a) 对组织及其环境的理解(见 4.1)；
b) 法律、法规要求(见 4.2.2)；
c) 业务连续性管理体系的范围和删减范围(见 4.3)；
d) 方针(见 5.2)；
e) 业务连续性目标和实现计划(见 6.2)；
f) 能力(见 7.2)；
g) 业务影响分析和风险评估(见 8.2)；
h) 业务连续性策略和解决方案(见 8.3)；
i) 业务连续性计划和程序(见 8.4)；
j) 演练方案(见 8.5)；
k) 监控、测量、分析和评估(见 9.1)；
l) 内部审核(见 9.2)；
m) 管理评审(见 9.3)；
n) 不符合和纠正措施(见 10.1)。

7.5.1.5 为确保业务连续性管理体系的有效性，成文信息可包括：

a) 客户协议和服务等级；
b) 业务影响分析的结果；
c) 风险评估的结果；
d) 业务连续性解决方案的确定和选择；
e) 突发事件响应概述；
f) 意识提升方案；
g) 与员工和相关方就业务连续性管理体系及突发事件进行的沟通，如通信、会议纪要和警报；
h) 组织和个人的培训方案；
i) 演练进度表；
j) 与供应商的合同和服务级别协议；
k) 承包商和供应商的业务连续性方针和计划，包括对其供应商进行风险监控的证据，以及其供应商的连续性计划得到保持和实施的证据；
l) 承包商和供应商的通知和响应程序；
m) 检查、保持和校正的证据；
n) 已发生突发事件和未遂突发事件的报告；
o) 业务连续性管理体系评审会议记录。

7.5.2 创建和更新

为了符合创建和更新成文信息的要求：

a) 成文信息宜清楚标识(如姓名、参考编号、描述、日期、作者、版本)；
b) 组织宜指定可接受的格式(如语言、软件版本、图形)及用于储存成文信息的媒介(如纸质、电子)；
c) 使用的格式和媒介宜经过评审和批准，以确保其适宜性和充分性。

业务连续性管理体系成文信息的范围可能会根据组织的以下因素而有所不同：

a) 组织的规模、产品和服务以及所从事的活动类型；
b) 活动的复杂性及其相互关系；
c) 人员的能力。

7.5.3 成文信息的控制

7.5.3.1 访问成文信息

所有要求的成文信息宜受控。

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，以实施和运行业务连续性管理体系。宜主要关注该目的，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。

可设置不同的访问等级和组合(如只读、读写以及限制阅读)。组织也可根据其敏感性(如限制、机密、保护)对其成文信息进行分类。如在涉及内部劳动力中断的业务连续性解决方案中，或在业务连续性计划和程序包含竞争对手敏感信息时，可能需要分类。

7.5.3.2 控制类型

宜建立一个成文的程序来确定需要的控制措施，以：

a) 分发成文信息；
b) 提供成文信息访问(如：批准和授权查看或更改成文信息)；
c) 发布前审批文件的适当性；
d) 评审和更新以及必要时重新审批文件；
e) 确保文件的变更内容及其当前的修改状态得到确认；
f) 确保适用的文件版本在使用时的可用性；
g) 确保文件的清晰易读且易于识别；
h) 确保组织确定的为策划和运行业务连续性管理体系所需的外部文件得到识别，并控制文件的分发；
i) 避免意外使用过期文件，如这些文件因为某种原因需要加以保留，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。

组织宜确保成文信息的完整性，防止对其进行篡改，进行安全备份，仅限授权人员访问，并谨防损坏、变质和丢失。

组织宜证明其对保存成文信息相关的法律法规的意识，并宜保留合规证据。

8 运行

8.1 运行的策划和控制

8.1.1 概述

组织宜确定、策划、实施和控制建立和保持业务连续性方针和目标所需的过程，并满足适用的需求(见第4章)和实施6.1中确定的措施。

这些过程宜融入到组织的业务过程中，以确保它们得到适当的管理并有效地保持。

组织宜在过程中建立控制机制，包括：

a) 决定如何确定、策划、实施和控制这些过程(如通过建立实施计划并就实施业务连续性管理的方法达成一致)；

b) 确保过程按策划进行,如设置里程碑并明确交付物要求;

c) 保留成文信息证明过程按策划实施。

组织宜控制策划的变更,评审非预期变更,并采取适当的措施。

组织宜确保外包过程和供应链受控(见 8.3.4.9)。

8.1.2 业务连续性管理

业务连续性管理包括以下要素(如图 5 所示)。

a) 运行的策划和控制(见 8.1):运行的策划和控制是业务连续性管理的核心,宜由最高管理者任命的人员来负责。

b) 业务影响分析和风险评估(见 8.2):业务影响分析使组织能评估冲扰对产品和服务交付的影响,确定优先恢复的活动。了解冲扰风险使组织能够对其管理。业务影响分析和风险评估的结果使组织能够选取合适的业务连续性策略和解决方案。

c) 业务连续性策略和解决方案(见 8.3):识别和评估多种业务连续性策略,使组织能够识别降低风险和减轻优先活动冲扰影响的解决方案。选定的业务连续性解决方案将在可接受的能力(生产或服务水平)和在确定的时间范围内恢复产品和服务的交付。

d) 业务连续性计划和程序(见 8.4):业务连续性计划和程序使组织根据其业务连续性要求应对冲扰和持续活动。宜有明确的响应机制,确定负责响应冲扰的团队(见 8.4.2)。组织宜建立和实施预警和沟通(见 8.4.3)、突发事件响应(见 8.4.4.2.2)和恢复(见 8.4.5)的计划和程序。

e) 演练方案(见 8.5):演练方案使组织能够确认解决方案、计划和程序的有效性。演练方案为组织提供机会以:

   1) 提升个人意识并发展能力;

   2) 确保业务连续性和业务连续性程序是完整的、现行的和合适的;

   3) 改进其业务连续性。

f) 业务连续性文件和能力评价(见 8.6):组织宜对业务连续性管理进行评价,以确保其有效性,并使组织能够实现业务连续性目标。

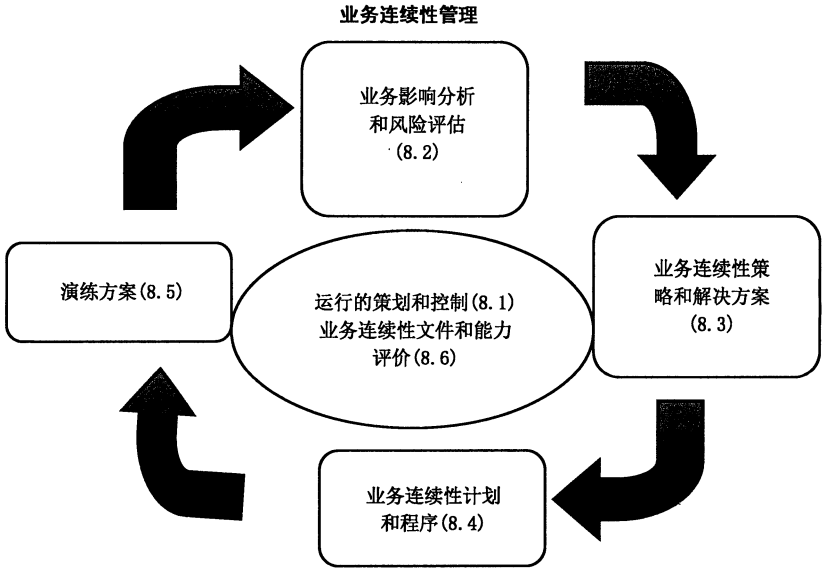

图 5 业务连续性管理要素

8.1.3 保持业务连续性

有效保持业务连续性包括:

a) 确保业务连续性的范围、角色和职责持续相关；
b) 适当时，在组织和相关方中融入业务连续性管理；
c) 管理与业务连续性相关的费用；
d) 在业务连续性管理体系内建立和监控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。

宜定期评审组织业务连续性管理的每个组成部分，包括成文信息。当组织的运行环境、架构、场所、人员、过程或技术发生显著变化，或者当某次演练或突发事件凸显不足时，宜进行评审和更新。

组织可采取公认的项目管理方法来确保业务连续性管理得到有效的管理。

确保业务连续性有效的方法包括：

a) 实施最佳实践；
b) 管理演练方案；
c) 统筹业务连续性的定期评审和更新，包括评估或重做业务影响分析和风险评估；
d) 确保业务连续性程序满足响应团队的需求。

8.2 业务影响分析和风险评估

8.2.1 概述

组织通过向客户交付产品和服务来实现其目标。因此，理解冲扰产品和服务（及相关活动）交付对组织和相关方的长期不利影响、支持产品和服务活动之间的关系和资源需求及它们所受的威胁是非常重要的。

组织宜实施和保持系统业务影响分析（见 8.2.2）和风险评估（见 8.2.3）的过程，以识别业务连续性策略和解决方案（见 8.3）。在策划的时间间隔及组织内部或运行环境发生重大变化时，宜对业务影响分析和风险评估进行评审。

对优先活动进行风险评估（见 8.2.3）后，组织可确定业务影响分析和风险评估的顺序。

8.2.2 业务影响分析

业务影响分析使组织能为恢复被冲扰活动设置优先级。其主要目的是使组织能够识别可能需要紧急行动的活动，并将其归类为优先活动，当这些活动被冲扰时，如不能迅速恢复可能导致不可接受的不利影响。除了需要迅速恢复的活动，可能需要优先考虑其他活动。例如，一项活动不需要在 6 个月内恢复，但至少需要 8 个月才能恢复也需要优先考虑。因此，优先活动也可被视为在其冲扰前需要实施业务连续性解决方案的活动（见 8.3.5）。

本文件使用术语“优先活动”，但组织可使用自己的术语、时间段或优先级。例如，可使用术语“关键的”“重要的”“必不可少的”和“主要的”。时间段可以是“0 h～2 h”“0 d～1 d”和“1 d～3 d”。优先级可以是“高”“中”和“低”，或“第一”“第二”和“第三”。

每个组织都以自己的方式描述其运行。例如，一个组织可将活动描述为组织为生产或交付产品和服务而执行的任务或任务集（见图 6）。其他组织可能希望将产品和服务描述为由活动组成的过程创建的。

业务影响分析宜涵盖业务连续性管理体系范围内的所有活动。可对一组活动进行分析，例如，与特定产品和服务相关的活动（见图 6）。

在进行业务影响分析时，使用的术语宜反映组织描述其自身运行的方式。

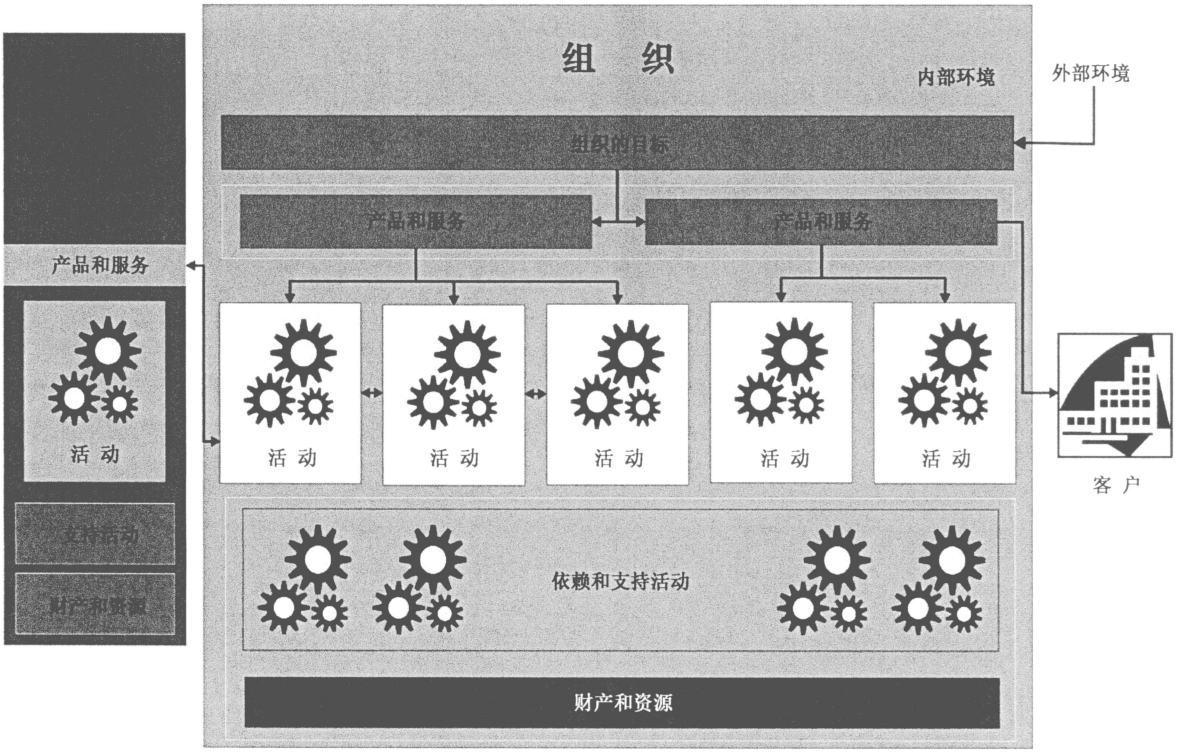

图 6 了解组织

GB/T 35625 包含开展业务影响分析的进一步指南。作为技术规范，提出了一种阶段性方法来满足 GB/T 30146 的要求。

业务影响分析使组织能够确定冲扰对其运行产生的不利影响，并形成业务连续性要求。

业务影响分析使组织能够：

a) 了解其产品和服务以及交付活动；

b) 为恢复产品和服务交付确定优先级和时间范围；

c) 识别业务连续性和恢复可能需要的资源；

d) 识别相互依赖关系(包括内部和外部)。

组织宜开展业务影响分析确定业务连续性优先级和需求。该过程宜基于组织环境、组织目标相关方的需求明确业务影响分析的评价标准，包括影响类型和时间范围。评价标准宜定期评审，并在变化时期加大频次。

表 4 列举了一些影响类型(可称为“影响类别”)。

表 4 影响类型示例

类型	描述
财务类	因罚款、罚金、利润损失或市场份额减少造成的损失
声誉类	负面新闻或品牌损害
运行类	冲扰业务运行的程度和持续时间
法律法规类	诉讼责任及吊销营业执照
合同类	违约或违反组织间的约定
业务目标类	未能实现目标或利用机会

影响变得不可接受的时间可能从几秒钟到几个月不等。时间范围取决于产品和服务的时间敏感性。例如，对时间非常敏感的产品，时间范围可能为几分钟或几小时。对时间敏感性较低的产品和服务，时间范围较长。

冲扰能间接影响产品和服务的交付。例如，无法向供应商付款能损害组织的声誉，导致供应商拒绝供应货物，从而阻碍产品生产或服务交付。产品和服务的需求每天都在变化，在本质上这些变化是周期性的。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通常有季节性变化和波峰波谷。考虑到间接后果，将冲扰设定在最不利时间点，能够确保对影响进行最大化的评估。

由组织的最高管理者确定组织不能接受的影响阈值。影响变得不可接受之前的时间可称为“最长可容忍中断时间(MTPD)”“最长可容忍时间”或“最大可接受中断时间”。组织可接受的最低标准的产品或服务称为“最小业务连续性目标(MBCO)”。

业务影响分析宜包括识别优先活动间的依赖关系，并将其包含在风险评估中(见 8.2.3)，用于确定业务连续性策略和解决方案(见 8.3)。

由于优先活动的依赖关系可能与所选择的业务连续性解决方案无关，在选择业务连续性解决方案(见 8.3.3)之前，组织宜确定优先活动的资源需求(见 8.3.4)。

业务影响分析的过程宜包括以下内容。

a) 定义与组织环境相关的评价标准，包括：
   1) 影响的类型；
   2) 时间范围。
b) 识别支持产品和服务交付的活动。
c) 使用评价标准评估冲扰随时间推移造成的影响。
d) 估算不重续活动时，影响变得不可接受的时间范围。
e) 在 d)识别的时间内，设定以最低可接受能力活动的时间范围(见图 2 和图 3)。
f) 识别优先活动。
g) 识别优先活动的依赖关系，包括人员(见 8.3.4.2)、信息和数据(见 8.3.4.3)、建筑、工作场所和相关公用设施(见 8.3.4.4)、设备和消耗品(见 8.3.4.5)、信息通信技术系统(见 8.3.4.6)、运输和物流(见 8.3.4.7)、财务(见 8.3.4.8)，以及合作方和供应链(见 8.3.4.9)。
h) 识别优先活动之间的相互依赖关系(如：采购依赖于财务发放资金)。

本文件中，重续活动的时间范围[见 e)]称为“恢复时间目标(RTO)”。设置恢复时间目标需考虑：

a) 对相关活动的依赖关系；
b) 恢复过程的复杂性。

对于恢复过程复杂的组织，可在接受的能力范围设置多个恢复时间目标。

在考虑活动对信息和数据的依赖关系时，组织宜确保重续活动所需的信息和数据是适当的、现行的。组织可使用术语“恢复点目标(RPO)”来表示。恢复点目标是恢复活动信息和数据使活动运行的时间点。恢复点目标还可用于确定备份频率，以避免不可接受的数据和信息丢失，以及其他可能阻止活动重续的正在进行的工作。

ISO/IEC 27031 为电子数据的流通提供了进一步的指南。ISO/IEC 27002 为确保数据的持续保密性、完整性和可用性提供了指南。

宜记录业务影响分析，包括：

a) 确定法律、法规和合同要求(义务)及其对业务连续性要求的影响(见 4.2.2)；
b) 确定或修改组织的业务连续性管理体系范围(见 4.3)；
c) 对组织的影响评价，作为业务连续性要求(时间和能力)的依据；
d) 识别产品与服务、活动与资源之间的关系；
e) 识别优先活动所依赖的支持资源；

f) 识别对其他活动、供应链、合作方和其他相关方的依赖关系。

信息可能来自：

a) 访谈；

b) 问卷；

c) 研讨会；

d) 其他内外部来源。

8.2.3 风险评估

风险评估的目的是使组织能够评估优先活动被冲扰的风险，以便采取适当的措施应对风险。

组织宜实施和保持正式的风险评估过程，系统地识别、分析和评估破坏组织优先活动的风险，以及支持这些活动的过程、体系、信息、人员、资金、供应商和其他资源。

风险评估是一个结构化过程，在决定可能需要的进一步处理之前，分析风险的可能性和后果。结构化过程试图回答一些基本的问题，如：

a) 会发生什么；

b) 发生的可能性有多大；

c) 会有什么后果；

d) 有什么方法可减轻后果或降低这种可能性。

该过程宜考虑组织环境以及相关方的需求和期望(见 4.1 和 4.2)。

组织宜了解与组织活动所需资源相关的威胁和脆弱性，特别是：

a) 识别为高优先级的活动所需的资源；

b) 当资源更换交付周期长于活动恢复时间目标时。

组织宜选择适当的方法识别、分析和评估可能导致冲扰的风险。GB/T 24353 给出了风险管理的原则和相关指南。本文件宜包含以下典型要素。

a) 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、资金、供应商和其他资源的潜在风险源，可能来自：

   1) 在某种情况下可能冲扰活动和资源的具体威胁(如：火灾、洪水、电力中断、员工流失、员工缺勤、电脑病毒和硬件故障等)；

   2) 由资源脆弱性(如单点故障、消防防护不充分、电力韧性不足、人员配备不足，IT 安全水平和韧性低下)引起的冲扰。

b) 风险分析：了解风险，以便对其进行评估和确定适当的处理方法。宜包括：

   1) 考虑风险的原因和来源，正面和负面后果的可能性，以及其他因素可能对这种可能性产生的影响；

   2) 确定风险主要根据风险的可能性和预期后果，但也要考虑现有控制措施的有效性和效率。分析的关键参数是可能性，因此宜考虑其有效性的可信度(根据专家之间的意见分歧、不确定性、可用性、信息的质量、数量和持续相关性，或建模的局限性)，并提请决策者和其他有关方面注意。

   分析可以是定性、半定量或定量的。

c) 风险评估：评估哪些与冲扰有关的风险需要处置。宜关注高优先级或重要替代物交付时间的活动需要的资源。

组织宜了解要求传达这些结果的财务、监管/立法或政府义务。此外，某些社会层面的要求也保证在适当的详细程度上共享这些信息。

注：本条与优先活动被冲扰的风险相关，与业务连续性管理体系有效性相关的风险见 6.1。

8.3 业务连续性策略和解决方案

8.3.1 概述

业务连续性策略是组织满足其业务连续性要求的可能方法。

a) 业务连续性策略宜包含至少一个业务连续性解决方案，但也可能需要多个解决方案来满足业务连续性要求。

b) 业务连续性解决方案包括实施业务策略的方法、安排、方式、程序、处置方法和措施。解决方案可用于多种策略。

业务连续性策略和解决方案：

a) 使组织能够在规定的时间范围内以可接受的能力恢复业务运行；

b) 确定组织可以实施并随时间改进、用来减缓冲扰相关风险的能力。

确定业务连续性策略和选择业务连续性解决方案时，宜基于业务影响分析(见 8.2.2)和风险评估(见 8.2.3)，并考虑相关成本。

组织宜制定程序来识别和选择业务连续性策略和解决方案，包括评审和批准建议的解决方案。组织宜考虑在冲扰之前、期间和之后可实施的选项。

8.3.2 识别策略和解决方案

8.3.2.1 总则

大多数策略需要一个或多个解决方案，但对于组织的某些活动，不采取措施或推迟恢复是可接受的策略。

例如，重续活动的重新部署策略可由若干解决方案组成，包括“紧急运输”“网络再定向”和“备用人员”。这些解决方案也可成为“延长工作时间”策略的一部分。

类似地，保护优先活动的生产策略可由若干解决方案组成，例如“将产品 A 30%的生产从 A 地转移到 B 地”或“将产品 A 的生产拆分到 C 地和 D 地”。

为确保业务连续性计划(见 8.4.4)的运行不受冲扰的不利影响，组织可能需要采取预防措施，例如，将团队和要恢复的信息通信技术系统分散到多个地点。但是并非总能实现各种规模和类型冲扰的分离，有必要认识到这种方式的局限性并与最高管理者达成一致。局限性可以用距离、最少人员或严重程度来表示，并会受到公共机构对严重或大范围冲扰响应的影响。

组织宜确定适当的策略和解决方案，以：

a) 保护优先活动；

b) 稳定、连续、恢复优先活动；

c) 减轻、响应和控制影响。

组织宜具备确定和选择业务连续性策略和解决方案的机制，包括批准和实施推荐的解决方案(见 8.3)。

ISO/TS 22331 为确定和选择业务连续性策略和解决方案提供了进一步的指南。

8.3.2.2 保护优先活动

保护优先活动可通过以下方式实现：

a) 降低活动受到冲扰影响的风险；

b) 将该活动转给第三方(但职责仍由组织承担)。

或者，如有切实可行的替代方案，可更改活动的执行方式。

在确定保护优先活动的策略和解决方案时，组织宜考虑：

a) 已发现活动的脆弱性以及活动冲扰可能带来的影响；

b) 措施的成本与预期收益的比较；
c) 由于只有较少时间来解决问题带来的紧迫性；
d) 整体可行性和适用性。

8.3.2.3 稳定、连续、恢复优先活动

为以预定的能力恢复优先活动而设置的恢复时间目标，使组织能够确定策略以缩短冲扰时间、减少影响，并及时恢复优先活动。

为确保优先活动可在恢复时间目标内恢复，宜为依赖关系和支持资源设定相匹配的恢复时间目标。组织宜确定恢复依赖关系和支持资源所需的能力。设置这些恢复时间目标时，组织需考虑：

a) 在全面恢复服务之前，提供不同服务的可能性；
b) 确保有效的人员动员；
c) 在必要时，鼓励和支持人员重返工作岗位；
d) 延缓恢复依赖资源的临时方案(如人工操作)；
e) 积压工作和恢复丢失信息所需时间；
f) 恢复要求的复杂性和规模，或交付时间较长的专业设备的需求。

业务连续性策略可包括以下内容。

a) 活动迁移：一些或所有活动转移到组织内部的其他部分，或者转移给外部第三方，可独立进行也可通过互惠互助协议来进行。在决定重续活动的场所时，宜考虑受损/受影响的场所和未受损的备用场所。
b) 资源迁移或再分配：包括员工在内的资源转移到组织内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) 临时应对方案：为在有限时间提供可接受的结果，某些活动可能会采取不同的工作方式。临时应对方案可能更加费时和/或费力(如：人工操作不同于自动化系统)。因此，临时应对方案通常仅适用于短期或延缓恢复正常业务的情况。

策略的例子包括：

a) 在备用场所提供备用生产能力；
b) 为关键员工提供远程工作能力。

8.3.2.4 减缓、响应及控制影响

减缓、响应和控制冲扰影响的策略可包括以下内容。

a) 保险：购买保险可为部分损失提供一定的经济补偿，但不能弥补全部损失(如：未投保突发事件、品牌、声誉、相关方价值、市场份额和对人员的影响)。仅靠财务结算并不能完全保护组织并满足相关方的期望。保险可与其他解决方案结合使用。
b) 资产恢复：与专业公司签订后续服务合同，在资产损坏后清理或修复。
c) 声誉管理：培养有效预警和沟通的能力(见 8.4.3)，建立有效的突发事件沟通程序(见 8.4.4.5)。

对于需要处理的风险，结合其整体风险态度，组织宜考虑降低风险发生的可能性、缩短冲扰时间和限制影响的方法。

如存在组织无法控制且可能会严重破坏组织的特定危害(如地震或洪水)，组织宜：

a) 确定策略并实施解决方案，以限制其潜在影响；
b) 确定负责监测此类危害的外部机构；
c) 与外部机构建立联系，了解它们的通知协议；
d) 分析通知协议，以确定它们是否符合组织的需求。

8.3.3 选择策略和解决方案

业务连续性策略的选择宜基于：

a) 使优先活动能够在业务影响分析中预定的时间范围内以预定的能力恢复(见 8.2.2)；

b) 与组织可承担或不可承担风险的数量和类型相一致；

c) 以可管理和合理的成本提供利益。

当组织的运行发生变化时，组织宜重新检查所有的解决方案。

用于稳定、连续、恢复优先活动的业务连续性解决方案的成本通常非常高。如组织估计到这样的情况，宜选择可接受的和满足其业务连续性目标的替代解决方案，或者按照 4.3.3 的要求将受影响的产品和服务从业务连续性管理体系范围中排除。

当组织估计威胁极不可能发生，或者保护优先活动的成本过高时，作为其持续进行的业务连续性管理体系绩效评价的一部分(见第 9 章)，组织可选择接受风险并对其重新评价。接受风险还可要求将受影响的产品或服务从业务连续性管理体系范围中排除。

8.3.4 资源要求

8.3.4.1 总则

组织宜确定资源要求以实施所选的解决方案。

组织宜建立以下措施。

a) 具有适当权限的团队或个人(对小规模组织而言)来监管突发事件的准备、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。

c) 财务、后勤和行政程序来支持在突发事件发生前、中、后的业务连续性安排，程序宜：

1) 确保可迅速做出财务决策；

2) 与已建立的权限等级、治理和会计原则相一致。

3) 响应时间、人员、设备、培训、设施、资金、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供应商那里获取每种资源的时间表；

4) 与相关方的协助、沟通、战略联盟和互助程序。

8.3.4.2 人员

8.3.4.2.1 总则

组织宜配备有能力响应和管理突发事件的人员，并参与恢复优先活动。

8.3.4.2.2 突发事件响应

组织宜指定具有管理突发事件所需职责、权限和能力的突发事件响应人员。

突发事件响应人员宜组成一个小组，负责管理对组织产生重大影响或可能产生重大影响的冲扰。

可根据人员的能力进行分组：

a) 突发事件/策略管理(见 8.4.4.4)；

b) 沟通(见 8.4.4.5)；

c) 安全和权益(见 8.4.4.6)；

d) 救援和安保(见 8.4.4.7)；

e) 重续优先活动(见 8.4.4.8)；

f) 恢复信息通信技术系统(见 8.4.4.9)。

小组中的所有人员宜有明确的、适用于冲扰之前、期间和之后的职责和权限。

适用于突发事件响应和业务恢复人员的培训包括：

a) 突发事件评估；

b) 疏散和避难场所的管理(如适用于上述范围)；

c) 替代生产场所的安排；

d) 有效进行内外部沟通的技巧；

e) 处理人员方面的事宜(见 ISO/TS 22330)。

整个组织的响应技能和能力宜通过实践培训来发展，包括积极参与演练等。

响应和恢复小组宜接受有关其职责的教育和培训，包括与第一响应者和其他相关方的互动。各小组宜定期接受培训，新成员加入应急机构时也宜接受培训。这些小组还宜接受防止突发事件升级为危机的培训。

8.3.4.2.3 重续活动

组织宜确定适宜的措施，以保持和扩大可用的核心技能和知识，使活动能够在工作人员减少的情况下恢复。在突发事件发生时，人们可能不会按预期作出响应，可能需要鼓励、保证和支持。拥有广泛专业技能和知识的员工、承包商和其他相关方均宜包括在内。保护或提升这些技能的方法可包括：

a) 后备技术专家的名单及召集计划；

b) 员工和承包方的多技能培训；

c) 分散核心能力以减少突发事件的影响，包括把掌握核心技能的员工分配在多个场所；

d) 第三方的使用；

e) 继任计划；

f) 记录过程，其他形式的知识保留和管理。

突发事件发生后对员工进行重新安置的程序需考虑以下内容。

a) 员工到另一场所的交通。

b) 员工在备用场所的需求，如：

1) 住宿；

2) 餐饮设施；

3) 个人和家庭承诺；

4) 不同设备的培训。

c) 居家办公带来的挑战。

专家角色可包括：

a) 安全；

b) 交通物流；

c) 权益和应急。

为了鼓励和安抚那些需要对冲扰做出响应的人，组织宜提供实用的建议、风险意识培训、交通解决方案和家庭相关的支持。

业务连续性的人员方面的指南见 ISO/TS 22330。

8.3.4.3 信息和数据

“信息”和“数据”二词在日常生活中可互换使用。本文件中“信息”表示经过处理、组织和关联后产生意义的数据。因此，信息是由数据创建的，这些数据包括，例如，以电子形式保存、可在计算机上存储和使用的原始数据、统计数据和个人数据。

在冲扰期间，可从数据中重新创建信息，但处理时间可能会很长，方法也不一定可行。因此，组织宜

考虑各项活动对信息和数据的要求。如一项活动(不仅仅是优先活动)所需的信息或数据不可挽回地丢失了,那么该活动就不可能恢复。

宜根据业务影响分析中确定的时间范围保护对组织运营至关重要的信息和数据。当确定存储和恢复数据的安排时,组织宜了解适用的法律要求。

组织响应和恢复所需的信息或数据宜有适当的:

a) 保密性(如:活动迁移至另一场所);
b) 完整性:信息和数据可靠、可信、完整;
c) 可用性:信息和数据在活动需要时可尽快获取(在该活动的恢复时间目标以内);响应期间所需的信息和数据可能要求立即获得,但其他信息和数据可能在突发事件发生后一段时间内不需要;
d) 时效性:按要求及时更新,以使活动运行(8.2.2)—因突发事件丢失的信息可能需要重新创建,并且可能需要复原数据。

在复制信息和数据时,可使用各种方法,包括虚拟(电子)格式(如磁盘、云、磁带)和实物(硬拷贝)格式(如缩微胶片、影印、生产时就创建双份)。

对于尚未复制或备份到安全位置的信息和数据的恢复解决方案,宜记录在案。

如果信息或数据副本与其原始信息距离太近,冲扰可能会损坏其完整性或阻止对其存取。然而,距离过远可能会使信息/数据在需要时无法获得。宜有书面证据证明这些相互冲突的关注点是如何解决的。

与本子条款有关的信息和数据可包括:

a) 联系信息;
b) 供应商、相关方和相关方的详细信息;
c) 法律文件(如:合同、保单、所有权证书);
d) 其他服务文件(如:合同、服务水平协议);
e) 元数据(即以规定格式描述音视频内容及数据实质的资料);
f) 作为突发事件响应措施的通知和警报信息;
g) 关于谁有权调用程序的指引和标准。

8.3.4.4 建筑、工作场所和相关公用设施

工作场所解决方案的差别可能很大,选择范围也很广。不同类型的突发事件或威胁可能要求实施不同的或多个工作场所选项。恰当的选择取决于组织的规模、行业和活动范围,以及相关方和地理位置。例如,公共机构需要保持在其社区的一线服务交付,而有些组织却可在不同的国家或地区进行运营。

组织宜设计解决方案来降低正常场所不能使用带来的影响。该方案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) 指挥中心;
d) 第三方专业机构提供的备用场所;
e) 居家办公或远程办公;
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突发事件的影响。突发事件,如自然灾害,可能会导致大范围的损毁,影响基础服务,如电力、燃气、供水和通信。如存在这种风险,备用场所宜远离这种可能受影响的区域。

如员工需要转移到备用场所，宜充分考虑：

a) 确保有关场所距离不太近，以免受到同一突发事件的影响；

b) 确保办公场所足够近，员工愿意并能够前往那里工作；

c) 可能由突发事件引起的困难。

为连续性使用备用场所，宜对备用场所内要求的资源是否属于该组织进行明确的说明。如备用场所是与其他组织共享，宜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（如：生产线、呼叫中心或如恢复时间目标很短），转移工作任务可能比转移员工合适。这可能会要求备用场所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。

8.3.4.5 设备和消耗品

组织宜确定和维护支持其优先活动的核心供给品的库存。

有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，可能提供解决方案。

提供解决方案可能包括：

a) 在另一场所存储额外供给品；

b) 与第三方签订协议，确保可在短期内供货；

c) 将零库存交付产品分散到其他场所；

d) 在仓库或货运站存储物资；

e) 把部件装配业务转移到有物资供给的备用场所；

f) 确定备用或替代供给品；

g) 确认各阶段所需的设施和设备，并制定多种备选供货方案。

如有些活动需依赖专门的供给品，组织宜确定优先活动依赖的供应商，特别是单一货源的供应商。管理供应连续性的解决方案可包括：

a) 增加供应商的数量；

b) 鼓励或要求供应商具备业务连续性能力；

c) 与关键供应商签订合同或服务水平协议；

d) 确定有能力的备选供应商。

如业务活动改换到备用场所，宜确认供应商可高效地把他们的产品和服务送到备用场所。

8.3.4.6 信息通信技术（ICT）系统

在许多组织内，无信息通信技术系统就无法完成业务活动，在活动恢复之前，信息通信技术系统需要先得到恢复。在可能的实际情况下，信息通信技术系统恢复期间，可能需要手动的临时方案。

技术策略取决于所用技术的性质及其与活动之间的关系，但基本上是下列组合：

a) 组织内部自建；

b) 第三方向组织交付的服务；

c) 组织购买的外部服务。

提供优先活动所需的信息通信技术系统的方法可包括：

a) 在地理上将其分散布局（如在不会受到同一冲扰影响的不同场所维持同样的技术）；

b) 保留较老的设备，作为紧急情况下的替代品或备用品；

c) 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，因此宜注意：

a) 各技术站点的位置以及它们之间的距离；
b) 跨越分散站点的分布式技术；
c) 为远程访问用户的增加提供足够的设施；
d) 设置无人(暗)站点及有人站点；
e) 改进通讯的连通性并提高冗余路由的等级；
f) 采用自动“故障切换”替代要求人工干预来恢复信息通信技术系统；
g) 考虑信息通信技术系统的时效。

如组织在不止一个场所拥有信息通信技术系统，那就可能有机会实施一项解决方案，每个场所的规模宜达到多个信息通信技术系统合并后的容量要求。

如果组织使用了非常专业化或定制的技术，而且交付周期很长，就可能需要考虑通过为替换或复原作出特定规定来加强对其信息通信技术系统的保护。

业务连续性的信息通信技术准备指南见 ISO/IEC 27031。

8.3.4.7 运输和物流

突发事件发生后，可能需为员工提供交通运输服务：
a) 当员工平时所乘交通工具不可用时，送员工回家；
b) 将员工转移到备用工作场所；
c) 运送各地所需资源。

组织宜预先确定提供冲扰后可能需要的替代交通运输工具的选择，可能包括：
a) 确定物流冲扰的可能情形，包括由突发事件或异常情况直接导致的；
b) 保护替代交通运输工具和路线，以应对异常交通状况；
c) 与交通运输提供方签署协议。

8.3.4.8 财务

组织宜确定在冲扰发生期间及发生后确保提供必要财务服务的策略，可包括：
a) 提供紧急采购资金，例如食物、住所、设施、消耗品及交通工具；
b) 员工费用补贴；
c) 重大支出，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，组织可能有必要证明有效的财务控制，例如，提供在冲扰期间以及之后所有费用的正式记录。

8.3.4.9 合作方和供应链

业务网络和供应链通常是广泛、复杂和相互依赖的，并有多个层次。理解供应链及其给组织带来的风险是至关重要的。在分析业务影响时(见 8.2.2)，组织宜与相关供应商共同对优先活动所依赖的供应链进行分析。反之，宜要求供应商将分析传递到他们的供应商。

供应链分析宜基于组织制定的标准，给出通用的组织方法来评估对供应链和供应链内特定供应商的依赖程度，并了解寻找替代安排的时间表。

用于保证和评估供应商和合作方业务连续性的方法包括：
a) 在标书及合约中详细说明业务连续性的要求；
b) 定期审核供应商计划；
c) 评审演练和维护方案；
d) 参加业务连续性联合演练。

如将产品、服务或活动外包，对该产品、服务或活动的责任仍由组织承担。

当优先活动或业务连续性解决方案依赖于供应商的产品和服务时，组织宜评估供应商的业务连续性，以确保供应商对这些产品和服务部署了有效的业务连续性安排，例如：通过检查演练结果。

组织可将其工作侧重于未能交付产品和服务的供应商，因为这些供应商会最快地破坏优先活动。

8.3.5 实施解决方案

宜持续实施和维护选定的解决方案。

在选定业务连续性解决方案之后，管理人员宜参与业务连续性资源的选择（如工作环境、人员、设备、供给品）。宜注意确保这些资源在突发事件发生时可用。

为确保恢复和减缓策略是可行的，组织宜定义和实施在冲扰前需要到位的所有解决方案。如启用解决方案的准备时间超过了业务连续性需求，组织宜在冲扰之前实施所选的解决方案。

8.4 业务连续性计划和程序

8.4.1 概述

组织宜建立一个由业务连续性计划和程序支持的响应机制，以：

a) 控制对冲扰的响应；

b) 与相关方进行有效沟通；

c) 利用业务连续性解决方案在恢复时间目标内持续活动。

计划包括一个或多个程序。计划和程序，宜：

a) 确定立即采取的步骤并协助及时决策；

b) 具备足够的灵活性，以适应意外的威胁和多变的情况；

c) 关注冲扰的预期影响；

d) 与组织选择的业务连续性解决方案保持一致，以减少影响；

e) 为所有要执行的任务清晰地确定角色并分配职责。

8.4.2 响应机制

8.4.2.1 目的

有效的响应机制使组织能够检测事态、识别突发事件并确定是否可能导致冲扰。组织宜建立一个突发事件响应机制，无论冲扰的原因是什么都可对冲扰提供有效的响应。如没有达成一致的文件化结构，组织可能将无法有效地应对冲扰，也无法在必要的时间范围内重续被冲扰的活动。

8.4.2.2 设计

突发事件响应机制宜清晰确定：

a) 负责应对突发事件和重续活动的团队；

b) 团队的层级结构；

c) 团队的角色和职责。

响应机制宜简单，且能够快速形成。宜提供确保及时通报信息和决策的机制。

不存在适合所有组织的突发事件响应机制。每个组织宜设计自己的结构，并考虑：

a) 现有的管理结构；

b) 组织的性质、文化、规模、复杂性和过程基础设施；

c) 选定的业务连续性解决方案；

d) 组织的业务连续性要求；

e) 所有已发觉的对组织的威胁。

大型的或复杂的组织可能需要为突发事件的不同方面建立单独的团队。在较小的组织中，由一个团队来处理一个突发事件是可行的，但不宜是单个个人的职责。

8.4.2.3 团队能力

整体而言，团队宜具备以下能力：

a) 评估冲扰的性质、程度及其潜在影响；
b) 根据预先确定的影响阈值测量突发事件的潜在影响，以确定正式响应是否合理；
c) 对冲扰采取适当的应对措施，启动计划，动员响应团队，确保所需资源的可用性；
d) 策划所有要采取的行动；
e) 确定所有行动的优先级，把生命安全放在第一位；
f) 监测突发事件的发展情况，以及组织应对影响和后果的有效性；
g) 启用适当的业务连续性解决方案；
h) 有效指挥和控制组织对突发事件的响应，并随着情况的发展对变化做出响应；
i) 与相关方沟通，特别是员工、受影响的家庭成员、访客、政府和媒体。

8.4.2.4 团队组成和指导

每个团队宜有：

a) 确定的团队成员和候补成员，并具有必要的职责、权限和能力，使团队能够履行角色和职责；
b) 成文的程序，指导团队行动(见 8.4.4)。

8.4.3 预警和沟通

8.4.3.1 概述

从冲扰初始就有效地进行沟通会对组织的响应效率产生巨大的影响。只有在组织清楚知晓发生了什么、何时发生、与谁沟通以及如何沟通的情况下，才能实现有效沟通。因此，组织宜就下列与预警和沟通有关的行动建立成文程序，并确定负责执行行动的人员：

a) 在组织内部不同层级和部门之间进行的内部沟通；
b) 向相关方发出警报，并接收、记录和回复他们的沟通(可能包括员工的紧急联系人)；
c) 确保通信设备和设施可用；
d) 加强与应急响应人员的结构化沟通；
e) 管理组织对媒体的响应，并确保与组织的沟通策略一致；
f) 记录突发事件的重要信息、采取的行动和决策。

组织宜确保建立有效的程序和设施，以接收、记录和响应来自国家或地区风险咨询系统或类似系统的预警、警报和外部通信。一些组织可能需要在离受影响场所足够远的地方建立专用或临时设施，使其运营不受突发事件影响。对有特殊需要的人(如老年人和残疾人)需要特殊安排。警报传播方面的指南，包括信息内容和传播渠道，见 ISO 22322。

通信设备可能会受到冲扰的影响，因此可能需要提供替代方案，如：

a) 扩音器；
b) 公共广播系统；
c) 备用手机；
d) 卫星电话；
e) 双向无线电。

8.4.3.2 提醒相关方

在某些情况下,相关方可能会受到已经开始或即将发生的冲扰的影响。如从事危险操作或储存有毒产品的组织发生冲扰,可能会导致该组织的近邻处于危险之中。这些组织宜考虑:

a) 建立危险监测程序;
b) 预先确定在冲扰期间的公共预警信息;
c) 确定公共预警信息发送区域;
d) 科学评估危害严重性等级;
e) 明确发布预警的科学依据标准,并制定向具有公共预警职责的组织传递预警信息的程序;
f) 与负责潜在影响区域的外部机构建立关系。

这些组织也有必要:

a) 与具有公共预警职责的外部组织建立关系;
b) 确保近邻了解警报是如何发出的,以及如何应对。

预警和沟通程序宜作为组织演练方案的一部分进行演练(见 8.5)。

8.4.4 业务连续性计划

8.4.4.1 概述

业务连续性计划规定了团队如何应对业务连续性管理体系范围内的冲扰并持续活动。

组织之间采用的术语不同,在许多情况下,特定术语可互换使用,因此清楚地陈述团队的角色和职责至关重要,成文的程序有助于团队清楚地说明其目的、范围和目标(见表 5)。

表 5 团队及其可能的角色和职责示例

团队	角色	职责
现场应急响应 设施管理 安保	应急响应	生命安全 损失限制
损失评估	损失评估	损失评估
突发事件管理	突发事件管理和控制	突发事件管理
危机管理 高级管理人员	战略决策 突发事件发生期间的沟通	战略管理 危机管理 沟通 公共关系
沟通	突发事件发生期间的沟通	沟通 公共关系
信息通信技术恢复	恢复信息通信技术系统和基础设施	信息通信技术灾难恢复
财务管理	一般及财务管理	财务和行政
人力资源 职业健康	福利和特殊需求 相关方权益	人力资源 安全和福利

表 5　团队及其可能的角色和职责示例（续）

团队	角色	职责
救援 安保 设施 信息通信技术	设施、信息通信技术系统和数据抢救 安保	救援和安保
业务连续性	恢复被冲扰活动	协调恢复 管理资源

8.4.4.2　范围

8.4.4.2.1　总则

整体而言，业务连续性计划宜应对突发事件响应的所有方面，且宜针对使用计划的团队。以下做法可能有利于：

a）　各类人员包括专家团队，参与业务连续性计划的制定；

b）　利用演练反馈，从冲扰中吸取教训。

时间表和绩效水平宜基于业务影响分析（见 8.2.2）期间收集的信息以及选择的业务连续性策略和解决方案（见 8.3.3）。

8.4.4.2.2　突发事件响应

当处理突发事件时，需要考虑很多措施。以下措施宜包括在成文的程序中。

a）　响应和评估突发事件，包括：

1）　确定发生了什么，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）　突发事件预计要持续多长时间及其影响；

4）　常规管理措施能否应对该突发事件；

5）　参照预先设定的阈值判断突发事件是否会引起冲扰。

b）　管理突发事件的直接后果，适当考虑受影响人员（包括团队成员）的权益问题和对环境的影响，考虑突发事件响应方案，防止进一步的损失或损害。

c）　根据每个程序的启用标准评估突发事件。

d）　当满足启用标准时，宣布突发事件发生并启动程序。

e）　调动突发事件响应人员组成团队，开展维稳、连续性和重续活动。

f）　设立中心场所（指挥中心），供突发事件管理和控制团队使用。

g）　管理突发事件及其影响时，应对所要完成的事项和活动按重要性进行排序。

h）　控制和协调所有已启动的程序。

i）　启用或建立备用场所，以便恢复 IT 系统或其他基础设施，以及组织活动的临时运行。

j）　监控突发事件的进展。

k）　根据情况的变化评审和调整计划。

l）　运行能力恢复之后，宜逐步缩小规模、停止计划和恢复日常运营。

m）　进行事后总结并吸取经验教训。

n) 严格管理、整理和保护突发事件管理和恢复过程中生成的文件及记录。

为及时恢复组织产品和服务的交付，恢复每项活动的成文的程序宜：

a) 满足支持产品或服务活动的恢复时间目标；

b) 足够可靠。

可通过以下措施来实现：

a) 拥有或控制执行程序的方法和资源；

b) 与第三方签订合同、协议或服务等级。

8.4.4.3 内容和可用性

8.4.4.3.1 总则

业务连续性计划宜使用团队清楚的形式确定其目的、范围和目标。宜明确说明其他所需的或相关的成文的程序或文件的链接，并说明获取和访问这些程序或文件的方法。业务连续性计划宜包括：

a) 启用标准和程序；

b) 实施程序；

c) 沟通要求和程序；

d) 内部和外部的相互依赖和相互作用；

e) 资源要求；

f) 报告要求；

g) 信息流和存档过程。

8.4.4.3.2 指南和支持信息

计划宜包括以下内容。

a) 角色、职责和权限：

1) 为使用业务连续性计划的人员或团队确定角色、职责和权限；

2) 对于谁有权启动以及什么情况下启动程序(可能包含已定义的突发事件升级阶段)，宜有相关指引和标准予以明确。

b) 启动标准：

1) 启动组织对冲扰的响应过程，以及在成文的程序中启动标准和程序(可以考虑是在正常工作时间之内还是正常工作时间之外)；

2) 有合适替代方案的会议场所。

c) 运行参数：

1) 确定要执行的行动和任务，特别是与组织将如何在预定的时间范围内继续或恢复其优先活动有关的；

2) 相关的资源需求(见 8.3.4)；

3) 记录突发事件信息、采取的行动和决策的方法。

d) 用于协调和沟通的支持信息：

1) 团队成员和其他具有角色和职责的人员的联系信息，组织宜了解与信息保护有关的适用法律要求，并宜保留合规证据；

2) 可能需要的相关机构、组织和资源的联络信息以及调动细节。

e) 结束标准：

1) 突发事件过后的结束机制；

2） 要遵循的指令。

8.4.4.4 可用性

与任何形式的成文信息(见 7.5.3)一样,组织宜确保业务连续性计划在需要时随时随地可用。为确保业务连续性计划的运行不受冲扰的不利影响,组织可能需要采取预防措施(如,将团队和要恢复的信息通信技术系统分散到多个场所)。但是并非总能实现各种规模和类型冲扰的分离,有必要认识到这种方式的局限性并与最高管理者达成一致。局限性可以用距离、最少人员或严重程度来表示,并会受到公共机构对严重或大范围冲扰响应的影响。

8.4.4.5 突发事件/战略管理

突发事件管理的目的是确保组织在战略层面有效地应对冲扰。

突发事件管理程序宜包括在突发事件期间,组织管理可能面临的问题的方式,包括与相关方有关的问题,并宜解决管理突发事件的团队和其他响应团队可能需要的所有设施。

8.4.4.6 沟通

沟通程序可包括在突发事件管理或其他团队响应程序中。如有多个团队,宜密切合作。

突发事件发生期间,宜管理和协调需要传递和接收的沟通信息。该程序宜包括以下内容。

a） 如何以及在何种情况下组织需要与员工及其亲属、其他相关方和紧急联络人进行沟通的详细说明。

b） 组织在突发事件发生后媒体响应的详细说明,包括:

1） 突发事件沟通策略;

2） 首选媒体;

3） 起草媒体声明的指引或模板;

4） 有权向媒体发布信息的适当数量的、训练有素、称职的发言人。

重要的是,内部和外部沟通的时间和内容保持一致。要建立信心、信任和动力,首先要进行内部沟通。

在突发事件发生早期,预先准备的信息尤其有用,它使团队在突发事件细节仍在确定的情况下,能够提供有关组织及其业务活动的详细信息。

以下行为可能是适当的:

a） 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;

b） 任命一定数量能胜任、经过训练的人员接受媒体的电话采访;

c） 使用所有对组织开放的沟通渠道,包括社交媒体;

d） 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对组织有较大影响力的社会团体。

宜包括确定与其他关键相关方沟通并确定其优先级的过程,可能有必要制定一个单独的程序来管理相关方,提供设定优先级的标准,并预先为每个相关方或相关方团体分配人员。

8.4.4.7 安全和权益

当突发事件对生命、生活和权益造成直接危害时,组织有责任保护员工、承包方、访客和客户。对伤残人士或特殊群体(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降低风险,并可使受影响的人安心。突发事件所带来的长期影响不容低估。组织宜制定适当的

解决方案，包括考虑相关社会和文化问题，以促进组织内部的生理和心理康复。

权益响应的要素宜包括：

a) 现场疏散(包括内部就地避难活动)及集合点；

b) 调动安全、急救或疏散协助小组；

c) 对现场或附近的人员进行定位和清点。

还可能包括：

a) 翻译服务；

b) 交通帮助，包括所需的指引；

c) 紧急服务、相关机构和急救人员的指定联络人和联系信息；

d) 寻找替岗人员或承包方；

e) 管理电话救助热线；

f) 身体康复及心理支持。

宜具体确定所需的资源。资源宜及时提供并满足其预期功能。

8.4.4.8 救援和安保

组织可编制成文程序以解决救援和安保问题，并包括以下指导：

a) 设施、设备(包括信息通信技术系统)和成文信息(考虑信息安全性和隐私要求)的抢救优先级；

b) 应急部门移交场所的安保。

组织可在事发前指定专业救援承包商。有效地抢救设施、设备和成文信息可限制突发事件造成的影响，并使业务更快地恢复正常。

8.4.4.9 重续优先活动

宜制定程序规定：

a) 需要恢复的优先活动；

b) 恢复的时间表；

c) 恢复优先活动的能力；

d) 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，可包括：

a) 资源数量；

b) 技能与资格；

c) 技术设备；

d) 通信设施；

e) 通过签订互助协议可利用的资源，或其他可能获得的资源。

8.4.4.10 信息通信技术系统

重续活动的程序宜确定恢复所依赖的信息通信技术系统，宜涉及现有的信息通信技术连续性程序。

如有信息通信技术连续性程序，至少宜解决：

a) 调用所需信息通信技术响应，并部署信息通信技术人员；

b) 访问备份数据并获取备用服务资源；

c) 数据、信息服务、通信和支持资源的重建；

d) 可允许活动满足其恢复时间目标的可用性和容量要求的时间表。

更多指南见 ISO/IEC 27031。

8.4.5 恢复

组织宜预先确定如何在冲扰后恢复正常业务，并宜具有成文的程序，以恢复业务运行，并宜满足相关的审核和企业治理要求。

恢复的目的是在冲扰发生后重建业务活动，以支持正常的业务。可通过以下措施来实现正常运行：

a) 修复突发事件造成的损害；

b) 将业务运行从临时场所迁回至修复后的主业务场所；

c) 转移至新建场所。

如何最佳地恢复正常取决于突发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。

成文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) 修复受损设施；

d) 保障紧急采购和资金；

e) 抢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) 选择修复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) 恢复已丢失的文件信息；

k) 以适当的频次与相关方进行沟通；

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。

成文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恢复并且也有满足需要的资源要求(见 8.3.4)。

8.5 演练方案

8.5.1 概述

组织的业务连续性程序和安排只有经过演练并保持最新才被认为是可靠的。演练可以培养团队精神、能力、信心和知识，并宜包括那些可能需要使用程序的人员。

8.5.2 演练方案设计

即使在设计良好的过程中，稳健且现实的演练也能找出需要改进之处。组织宜设计一个演练方案，随着时间的推移验证其业务连续性策略和解决方案、计划和程序的有效性。

制定演练方案可以采取协调一致的办法建设、发展和完善组织的能力。方案宜涵盖有助于实现组织战略目标的独立计划、人员(包括来自外部组织的)、能力和资源。

最高管理者宜确保制定演练方案目标，并指派一名称职人员管理演练方案。演练方案的范围宜基

于实施演练的组织的规模和性质，以及所演练计划和能力的范围、功能、复杂性和成熟程度。在方案的早期阶段，演练和测试可能仅限于使用清单、演示和意识提升练习。随着方案不断成熟，可能扩展到包括桌面演练和实战模拟。

演练方案宜灵活，考虑到组织的变化和以前演练的结果。组织发生重大变化时可能会启动演练方案，以评估修订后的安排。

演练方案宜考虑所有参与者的角色，包括第三方服务商、供货商以及其他预计要参与重续活动的人员。组织安排的演练可包含上述各方，同时也可参加由他们所组织的演练。

为确保演练方案能在指定时间内有效进行，演练方案宜包括：

a) 需求分析；

b) 得到最高管理者的认可；

c) 明确的目标；

d) 演练的范围、数量、类型、持续时间、场所和时间表；

e) 该方案的适当支持人员；

f) 必要的资源和预算；

g) 处理保密、信息安全、健康安全及其他类似事项的过程。

演练方案宜保证，随着时间的推移，组织的总体响应将是有效的。方案在实施时宜：

a) 演练程序的技术、后勤、行政、程序和其他业务；

b) 演练程序中承担职责的所有人员，包括外部组织的人员；

c) 演练业务连续性安排和基础设施(如：包括指挥中心和工作区域)；

d) 验证技术和通信恢复，包括工作人员的可用性和重新安置；

e) 演练响应团队以管理供应链冲扰造成的影响。

组织宜监测和评估演练方案的实施，以确保其目标的实现。演练方案宜评审以确定改进。

8.5.3 演练业务连续性计划

演练，包括测试，是经过设计的一系列活动，用来检验组织面临特定冲扰情景时进行响应、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：

a) 预设预期的输出(如：事先进行演练设计并确定其范围)；

b) 允许组织开发创新的解决方案。

演练宜切合实际、认真设计并获得相关参与方的认可，以将由该演练直接导致突发事件发生并造成活动冲扰的风险降到最低。为实现该要求，在不破坏测试目标的完整性的前提下，可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，可利用风险评估中所确定的威胁或从之前冲扰获取的信息。

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，宜在演练前准备就绪，从而使参与者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) 验证活动恢复时间目标(见 8.2.2)以及优先活动的依赖关系和支持资源的恢复时间目标(见 8.3.2.3)是可实现的；

b) 确信业务活动所需的信息是适当的最新信息(见 8.3.4.3)；

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) 提高对组织环境及优先事项的认识；
e) 提高对于业务连续性程序内容及其使用的理解；
f) 提高应对突发事件的信心；
g) 作为改进组织能力的机会；
h) 评估业务连续性解决方案的实用性及其适用性；
i) 评估已有的能力和配备的资源是否充分；
j) 识别在应对冲扰过程中，所用到的以前没有记录的要求和实践；
k) 识别所编写的业务连续性程序及其执行中存在的不足；
l) 确保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。

演练可有不同的形式。演练类型的适用性取决于很多因素，包括：

a) 组织环境；
b) 演练目的；
c) 演练方案的成熟度；
d) 参与者的经验；
e) 预算；
f) 参与者参与程度；
g) 组织对举行演练造成运营冲扰的容忍度。

组织宜根据其演练结果采取行动，实施经批准的变更和改进。

不同类型的演练有不同的名称，通常归为以下几类。

a) 讨论：以讨论为基础的演练旨在使参与者在低压力环境下熟悉业务连续性计划和程序。
b) 模拟：基于行动的演练更加真实和具有挑战性。可在正常的运行环境、备用场所或指挥中心进行这种演练。

表 6 列举了演练方法示例。

表 6 演练方法示例

类别	方法	描述
讨论	方案评审	方案评审是对计划和程序的非正式评审，使参与者熟悉新的或更新的内容。在第一次制定或重大修订计划和程序时，方案评审是第一步，非常有效。计划评审通常需要 1 h～2 h
	桌面演练(现场)	现场桌面演练使用简单的场景，使参与者在低压力环境中熟悉计划和程序。它们还可以用于评审业务连续性策略和解决方案，以进行验证和改进。现场桌面演练通常是组织进行的第一种类型的正式演练，通常可在 2 h～3 h 内完成
	桌面演练(场外)	场外桌面演练通常在备用场所或指挥中心进行，目的是评审业务连续性计划和程序。这种演练通常使用简单的场景。与现场桌面演练的关键区别在于，在正常的运行环境之外进行演练。不包括交通运输时间，场外桌面演练通常可在 2 h～3 h 内完成
模拟	工作坊(单一或多个计划)	基于计划的研讨会通常在场外的备用场地进行，使用合理的复杂场景。根据演练的范围，参演者展示一个计划或多个计划。这样做的目的是让团队在压力更大的时间范围内练习合作和决策。涵盖多个计划的研讨会演练通常用时 3 h～5 h，具体取决于计划和场景的复杂性

表 6　演练方法示例（续）

类别	方法	描述
讨论	研讨会（一个或多个场所）	基于场所的研讨会通常在场外的备用场所进行，使用影响一个或多个场所的场景。演练的目的是让来自不同场所的团队练习合作和共同决策。一项涵盖多个场所的研讨会演通常可在 3 h～5 h 内完成，具体取决于场所数量及场景的复杂程度
模拟	全组织的研讨会（全面）	全面演练旨在让参与者做好准备，应对影响整个组织并需要启用业务连续性计划的冲扰。这是复杂的、高压力的演练，要精心策划和控制，以确保实现目标和不造成冲扰。全面演练可能用时半天到一周，取决于其复杂性和参演人员数量

作为演练的一部分，宜安排时间与所有的参与人员对业务连续性程序进行审查，讨论存在的问题和经验教训。宜记录这些信息，并按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。

从演练和经历的突发事件中得到的经验教训宜在以后的演练中再次得到检验。发现了严重缺陷和程序错误的演练，宜在纠正措施完成后再次进行演练。

演练和测试的益处包括：

a) 验证假设、业务连续性解决方案和业务连续性计划的范围；
b) 确保技术设施和资源正确有效；
c) 确保备用设施的能力；
d) 提高效率，减少完成过程所需的时间（如通过重复训练来缩短响应时间）；
e) 提高相关方的意识；
f) 提高演练参与者的能力和意识；
g) 演练类型、演练方案策划、实施和改进的指南见 GB/T 38209。

8.6　业务连续性文件和能力评价

8.6.1　概述

组织宜对其业务影响分析、风险评估、策略和解决方案、业务连续性计划和程序进行评价，以确保其持续的适用性、充分性和有效性。

宜通过演练结果、事后复盘以及组织环境的变化，考虑是否需要对业务连续性管理体系的方针、目标及其他业务连续性管理体系要素进行变更。

评价工作可采用内部审核、外部审核或自评价的形式。评价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。

评价宜验证：

a) 所有的产品和服务，以及支持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解决方案中；
b) 组织的业务连续性方针、解决方案和业务连续性程序能够准确地反映组织的优先事项和业务要求；
c) 人员的能力和组织的业务连续性是有效的，并与其目的相适应，能使组织管理、指挥、控制和协调对冲扰的响应；
d) 组织的业务连续性解决方案是有效的、及时更新的、与其目的相适应的；
e) 组织的演练和维护方案得到有效执行；

f) 业务连续性解决方案和程序包含了在突发事件和演练中以及在维护方案中确认的改进措施；
g) 组织具有持续开展业务连续性培训和意识提升方案；
h) 已与相关员工就业务连续性程序进行了有效的沟通，员工已理解他们的角色和职责；
i) 供应商和合作方对优先活动的依赖关系作出了适当和充分的业务连续性安排；
j) 组织充分遵守适用的法律法规要求和行业最佳实践，并符合业务连续性方针和目标；
k) 建立了变更控制过程并有效执行。

8.6.2 测量有效性

测量业务连续性计划、程序和能力的有效性宜包括外包活动的业务连续性安排，以及优先活动所依赖的供应商和合作方的业务连续性。

可用于测量有效性的指标：

a) 备份数据足以在规定的恢复时间目标内重续活动和资源；
b) 备用场所有所需的居住设施和设备，以便重续活动；
c) 具备在规定恢复时间目标内恢复优先活动所需的能力；
d) 具备应对和管理突发事件所需的能力。

当组织发生冲扰时，宜进行评审。可包括：

a) 确定冲扰的性质和原因；
b) 评价管理者响应的充分性；
c) 评价组织在满足恢复时间目标要求方面的有效性；
d) 评价业务连续性安排在员工应对突发事件方面的充分性；
e) 确定业务连续性安排有待改进之处；
f) 将实际影响与业务影响分析(见 8.2.2)中考虑的影响进行比较；
g) 收集相关方及参与响应人员的反馈。

8.6.3 结果

表明有效的业务连续性计划、程序和能力的结果，可包括：

a) 具备突发事件管理能力并提供有效的响应；
b) 组织对自身及其与其他组织、相关监管机构或政府部门、地方政府和应急服务部门关系的理解得到适当发展、记录和充分理解；
c) 定期演练以确保人员已接受培训，以有效应对冲扰；
d) 相关方的要求得到理解并能得到满足；
e) 冲扰期间员工能得到足够的支持和沟通；
f) 组织声誉得到保护；
g) 遵守法律法规的证明；
h) 在突发事件整个过程中保持财务控制；
i) 组织能向其客户和其他相关方证明其增强的韧性水平。

与所有评价及其结果相关的成文信息宜作为证据予以保存。

9 绩效评价

9.1 监控、测量、分析和评价

9.1.1 概述

监控、测量、分析和评价业务连续性管理体系的绩效与有效性宜包括以下程序。

a) 确定监控、测量、分析与评价的方式，包括：
   1) 明确要监控和测量的内容；
   2) 确定如何、何时以及由谁实施监控和测量；
   3) 设定绩效指标，包括适于组织并确保有效结果的定性和定量测量；
   4) 记录数据和结果，以促进后续的纠正措施分析。
b) 审查历史证据。
c) 监控组织业务连续性方针和目标的实现程度。
d) 测量业务连续性管理体系是否符合适用的法律法规要求。
e) 监控不符合和其他业务连续性管理体系绩效不足的证据。

9.1.2 保留证据

组织宜保存所有阶段性评价及其结果的成文信息。

9.1.3 绩效评价

组织宜使用绩效指标来评价业务连续性管理体系及其结果的绩效和有效性，以确定成功之处和需要改进的地方。获得的数据可用于识别模式，并使组织能够获得业务连续性管理体系绩效的信息。

9.2 内部审核

9.2.1 概述

组织宜定期开展内部审核工作，以评估业务连续性管理体系绩效。

业务连续性管理体系的内部审核提供了一种机制，用于衡量业务连续性管理体系实现其目标的程度、是否符合其计划的安排、是否得到适当的实施和维护，以及确定改进的机会。业务连续性管理体系的内部审核宜定期进行，为最高管理者确定业务连续性管理体系适宜性和有效性提供信息，也为制定持续改进业务连续性管理体系绩效的目标提供依据。

9.2.2 审核方案

组织宜建立审核方案(参照 GB/T 19011)来指导审核工作的计划和实施，并确定完成审核目标需要的审核工作。审核方案宜根据组织业务活动的性质、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业务连续性管理体系的全部范围，但是，每次审核不必覆盖整个体系。只要审核方案能够确保所有组织单位、职能、活动、体系要素和业务连续性管理体系的全部范围在组织规定的审核周期内完成，审核可分为若干较小部分。

业务连续性管理体系内部审核的结果可以报告的形式提供，并用于纠正或预防具体的不符合，并为开展管理评审提供输入。

业务连续性管理体系的内部审核可由组织内部的人员来开展，也可由组织选定的外部人员来执行。不论哪种情况，审核员宜能胜任审核工作，并能保证公正客观。在较小的组织里，审核员的独立性可以通过审核员不负责所审核的活动来证明。

9.3 管理评审

9.3.1 概述

最高管理者宜定期评审组织的业务连续性管理体系，从而保持其持续的适用性、充分性和有效性，包括其业务连续性程序和能力的有效运行。

9.3.2 管理评审输入

管理评审输入宜包括评价：

a) 以往管理评审所采取措施的情况；

b) 管理体系的绩效，包括不符合及其纠正措施的趋势、监控和测量结果，以及审核结果；

c) 供应链的变化以及供应链持续性安排的有效性；

d) 组织及其环境(见 4.1)的变化，以及可能影响管理体系的相关方反馈(见 4.2)；

e) 持续改进的机会。

管理评审为最高管理者提供了评估管理体系持续适应性、充分性和有效性的机会。管理评审的方法宜涵盖业务连续性管理体系的所有方面，包括删减范围(见 4.3)，但不必在一次评审中包括所有要素，评审过程可能会持续一段时间。

最高管理者宜定期开展并评估业务连续性管理体系的实施情况和结果。虽然评审是有益的，但正式的评审宜具备结构化特征，并保持适当的记录。参与业务连续性管理体系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，在安排好评审计划时间表后，宜对这些因素进行检查。

a) 部门/行业发展趋势：有重大部门/行业变化时，宜启动业务连续性管理体系评审。部门/行业内和业务/运营连续性规划技术的一般趋势和最佳实践可用来制定评价标准。

b) 监管要求：新的监管要求可能需要对业务连续性管理体系进行评审。

c) 突发事件经验：在一次冲扰响应后，不论是否启动了响应程序，都宜进行评审。如启动了响应程序，评审宜考虑响应程序的历史情况、其、工作原理以及启用原因等。如没有启动响应程序，评审就需要检查为什么不启动响应程序以及这一决定是否正确。评审影响同一部门和类似行业其他组织的冲扰也可能是有益的。

9.3.3 管理评审输出

9.3.3.1 业务连续性管理体系的改进

管理评审宜促进业务连续性管理体系效率、绩效和有效性的提升，并可能导致以下变化：

a) 业务连续性管理体系范围的改变；

b) 业务连续性策略和解决方案的更新；

c) 控制措施及其有效性测量方法的改变。

9.3.3.2 保存成文信息

组织宜保存文件记录信息作为管理评审结果的证据，并宜：

a) 就管理评审结果与相关方进行沟通；

b) 针对评审结果，采取适当的措施。

10 改进

10.1 不符合和纠正措施

10.1.1 概述

组织宜确定改进业务连续性管理体系的机会，并实施必要的措施以实现预期的结果。

10.1.2 不符合的发生

组织宜确定不符合，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识别：

a) 未满足的要求；

b) 无效的策划方法；

c) 与业务连续性管理体系相关的薄弱环节。

识别后，宜及时采取措施，防止事态进一步发展，并查明和解决根本原因。该程序宜能持续检查、分析和消除不符合的实际及潜在原因。

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，宜调查根本原因，并制定纠正措施计划以解决该问题。该措施计划宜减缓不符合所导致的后果，确定为纠正这种情况、重建正常运营和消除原因所需的变更，以防止问题再次出现。措施的性质和时间安排宜与不符合的规模、性质及潜在后果相适应。

即使没有不符合的证据，组织也宜改进业务连续性管理体系的绩效。改进措施包括纠正、纠正措施、创新和重组。

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，有助于确保业务连续性管理体系的可靠性和有效性。这些程序宜规定在策划和实施纠正措施时的职责、权限和步骤。最高管理者宜确保纠正措施得以实施，并对其有效性进行系统地跟进。

10.1.3 保留成文信息

组织宜保存成文信息，作为以下方面的证据：

a) 不符合的性质及其后续措施(如有)；

b) 纠正措施的结果(如有)。

10.2 持续改进

就业务连续性管理体系的适宜性、充分性和有效性而言，持续改进在 PDCA 循环的所有层面运行，并宜由业务连续性方针和目标、审核结果、冲扰分析、管理评审、志向和期望的成熟度水平来驱动。

持续改进需要识别机会的过程和管理机会的过程。持续改进过程宜遵循与纠正措施相同的基本过程，宜包括：

a) 识别需要解决的问题及其现状(改进空间)；

b) 识别当前的过程和控制措施；

c) 决定做出什么变化(改进)。

纠正措施解决业务连续性管理体系的缺陷，以使业务连续性管理体系能发挥其预定的作用，并确保其按预期工作，而持续改进使业务连续性管理体系达到更高的效率和效果。

组织可通过有效应用业务连续性管理体系过程来实现改进，如领导力(见第 5 章)、策划(见第 6 章)和绩效评价(见第 9 章)。最高管理者还宜考虑业务连续性管理体系改进的机会，包括以下方面的变化：

a) 组织环境(如竞争对手的失败)；

b) 组织内部结构(如增加额外的场所或员工)；

c) 生产或交付手段(如技术变革、基础设施改进)；

d) 不断发展的方法或可用的新恢复方法(如新的备用设施或网络技术)；

e) 技术和实践，包括新的工具和技术。

宜对这些进行评估，以确定它们对组织的潜在益处。

参 考 文 献

[1] GB/T 19011 管理体系审核指南

[2] GB/T 24353 风险管理 指南

[3] GB/T 38209 公共安全 演练指南

[4] GB/T 38299 公共安全 业务连续性管理体系 供应链连续性指南

[5] GB/T 35625 公共安全 业务连续性管理体系 业务影响分析指南

[6] ISO 22322 Security and resilience—Emergency management—Guidelines for public warning

[7] ISO/IEC 20000 Information technology—Service management

[8] ISO/IEC 27002 Information technology—Security techniques—Code of practice for information security controls

[9] ISO/IEC 27031 Information technology—Security techniques—Guidelines for information and communication technology readiness for business continuity

[10] ISO/TS 22317 Societal security—Business continuity management systems—Guidelines for business impact analysis (BIA)

[11] ISO/TS 22318 Societal security—Business continuity management systems—Guidelines for supply chain continuity

[12] ISO/TS 22330 Security and resilience—Business continuity management systems—Guidelines for people aspects of business continuity

[13] ISO/TS 22331 Security and resilience—Business continuity management systems—Guidelines for business continuity strategy