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)。

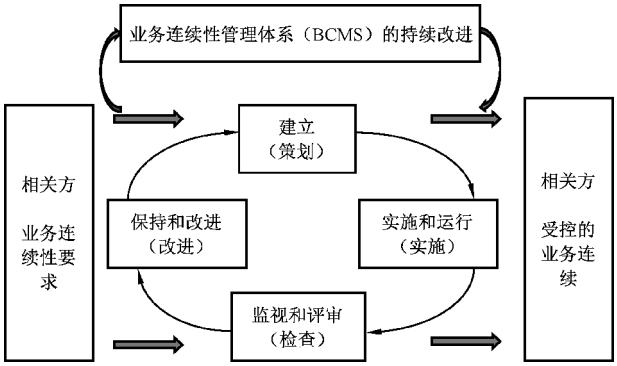

图 1　应用于 BCMS 过程的 PDCA

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

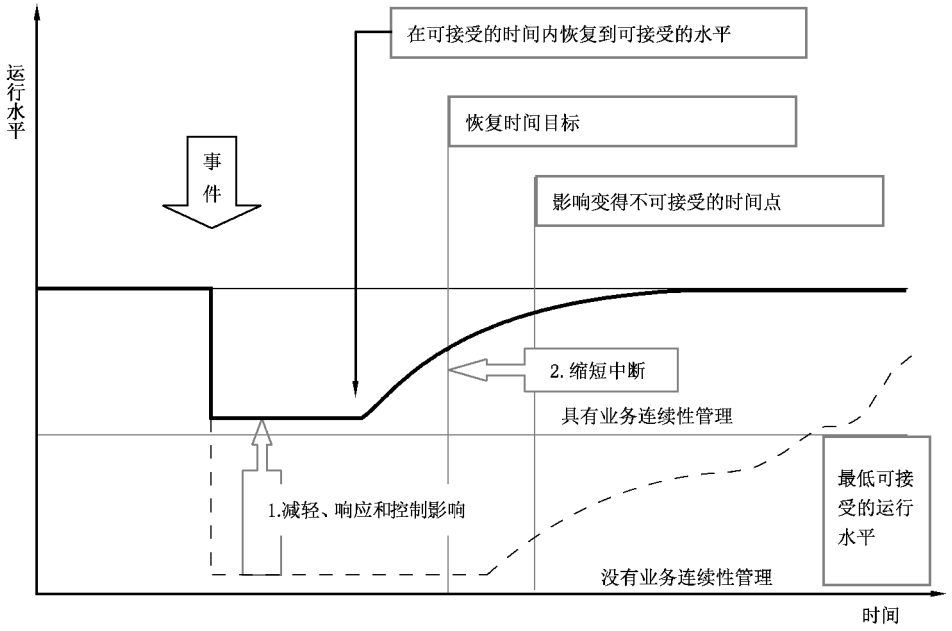

图 2 业务连续性对突发中断有效的图解

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

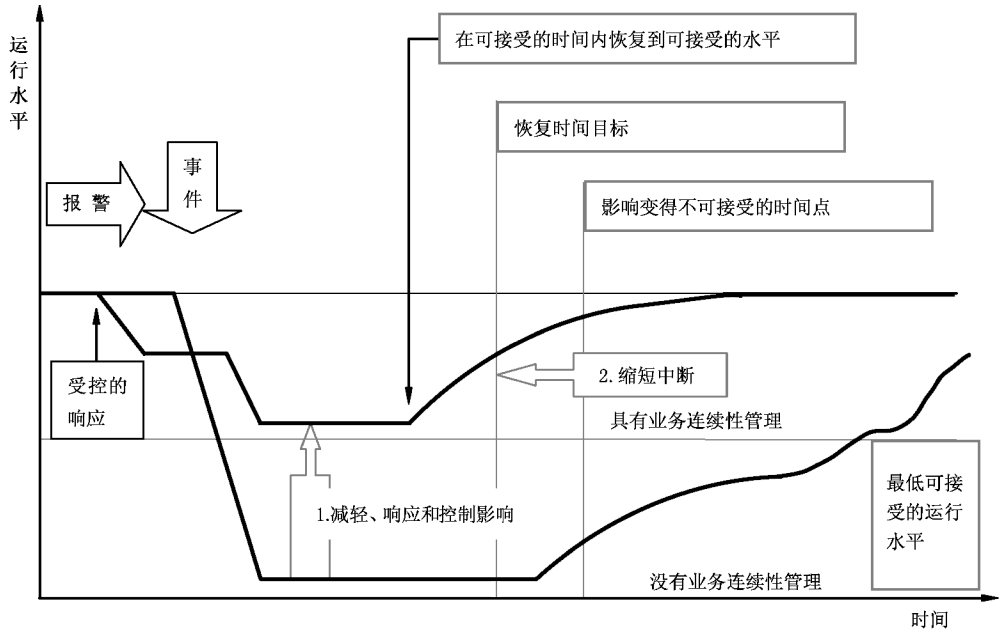

图 3　业务连续性对渐进中断有效的图解

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；