ICS 13.200
A 90

中华人民共和国国家标准

GB/T 30146—2013/ISO 22301:2012

公共安全　业务连续性管理体系　要求

Social security—Business continuity management systems—Requirements

（ISO 22301:2012,IDT）

2013-12-17 发布　　2014-05-01 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 22301:2012《公共安全　业务连续性管理体系　要求》(英文版),仅有编辑性修改。

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、中金数据系统有限公司。

本标准主要起草人:王金玉、秦挺鑫、董晓媛、刘俊华、张超、李忠强、魏军、尤其、王明、尹晖。

引　言

0.1　总则

本标准规定了建立和管理一个有效的业务连续性管理体系(BCMS)的要求。

BCMS 强调以下方面的重要性：

——理解组织的需求以及制定业务连续性管理方针和目标的必要性；

——实施和运行控制措施来管理组织应对中断事件的整体能力；

——监视和评审业务连续性管理体系的绩效和有效性；

——基于客观测量的持续改进。

和其他管理体系一样，BCMS 包括以下关键部分：

a)　方针；

b)　职责明确的人员；

c)　与以下几点相关的管理过程：

　　1)　方针；

　　2)　策划；

　　3)　实施和运行；

　　4)　绩效评估；

　　5)　管理评审；

　　6)　改进；

d)　提供含有审核证据的文件；

e)　任何和组织有关的业务连续性管理过程。

业务连续性有助于构建更具弹性的社会，更宽泛的群体以及组织环境对组织的影响会要求其他的组织参与到恢复过程中来。

0.2　策划—实施—检查—处置(PDCA)模型

本标准采用了“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、保持和改进组织 BCMS 的有效性。

PDCA 模型的采用在一定程度上保证了与其他管理体系标准(例如 GB/T 19001 质量管理体系、GB/T 24001 环境管理体系、GB/T 22080 信息安全管理体系、GB/T 24405.1 信息技术——服务管理和 ISO 28000 供应链的安全管理体系规范)的一致性，从而支持与相关管理体系整合后的实施与运行。

图 1 说明了 BCMS 如何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连续性结果(例如受控的业务连续性)。表 1 对 PDCA 模型进行了解释。

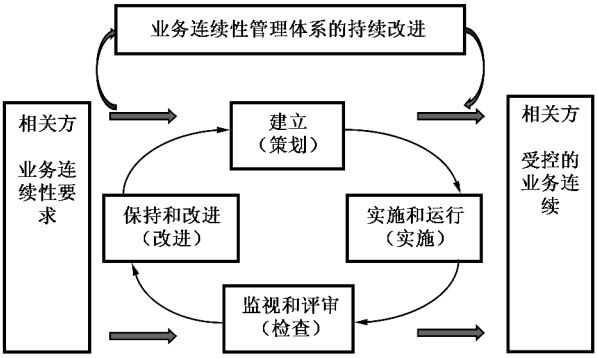

图 1　应用于 BCMS 过程的 PDCA 模型

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、指标、控制措施、过程和程序，以提供与组织的总方针和总目标相一致的结果
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，确定和授权纠正与预防措施
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

0.3　本标准中 PDCA 组成部分

如图 1 所示的策划(Plan)—实施(Do)—检查(Check)—改进(Act)模型，本标准中的第 4 章至第 10 章包括以下组成部分：

——第 4 章属于策划部分。它提出了将本标准应用于组织建立 BCMS 的环境、需求、要求和范围时的必要的要求。

——第 5 章属于策划部分。它总结了对业务连续性管理体系中最高管理者角色的要求，以及领导层如何通过方针声明向组织阐明它的期望。

——第 6 章属于策划部分。它描述了制定整个 BCMS 的战略目标和指导原则的相关要求。第 6 章的内容与风险评估中的风险处置机会，以及业务影响分析(BIA)中建立恢复目标的内容不同。

注：第 8 章对业务影响分析和风险评估过程的要求进行了规定。

——第 7 章属于策划部分。它为 BCMS 的运行提供了支撑，涉及能力的建立、在循环/必要的基础上与相关方的沟通，以及对记录、管理、保持和保留所需文件的要求。

——第 8 章属于实施部分。它定义了业务连续性的要求，确定了怎样达到要求以及如何通过制定程序来管理中断事件。

——第 9 章属于检查部分。它汇总了测量业务连续性管理绩效、BCMS 与本标准和管理层期望的符合性，以及从管理层的期望值方面寻求反馈信息的必要要求。

——第 10 章属于改进部分。它识别并通过采取纠正措施处置 BCMS 的不符合。

公共安全　业务连续性管理体系　要求

1　范围

本标准为策划、建立、实施、运行、监视、评审、保持和持续改进一个文件化的业务连续性管理体系规定了要求，用以实施保护，减少中断事件发生的可能性，以及当中断事件发生时准备、响应并恢复。

本标准规定的所有要求是通用的，适用于各种类型、规模和特性的组织或组织的一部分。这些要求的适用范围取决于组织的运行环境和复杂性。

本标准的目的不是要规定统一的业务连续性管理体系(BCMS)结构，而是为组织设计一个适合其自身需要且同时符合相关方要求的 BCMS。这些需求由法律、法规、标准、产品和服务、工作流程、组织的规模和结构以及相关方的要求等方面构成。

本标准适用于有如下期望的各种类型和规模的组织：

a)　建立、实施、保持和改进 BCMS；

b)　确保符合声明的业务连续性方针；

c)　向其他组织证明自身的符合性；

d)　欲使其 BCMS 获得被认可的第三方认证机构的认证/注册；

e)　做出符合本标准的自我声明。

本标准可用于评估一个组织满足自身连续性需求和要求的能力。

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。

无规范性引用文件。

3　术语和定义

下列术语和定义适用于本文件。

3.1

活动　activity

由组织(或其代表)为生产或支持一个或者多个产品和服务而执行的过程或者一组过程。

示例：此类过程包括账务、呼叫中心服务、信息技术、生产和配送。

3.2

审核　audit

为获得审核证据并对其进行客观的评价，以确定满足审核准则的程度所进行的系统的、独立的并形成文件的过程。

注 1：审核可以是内部审核(第一方审核)或是外部审核(第二或第三方审核)，也可以是结合审核(结合两个或两个以上管理体系)。

注 2：GB/T 19011 中定义了“审核证据”和“审核准则”。