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。

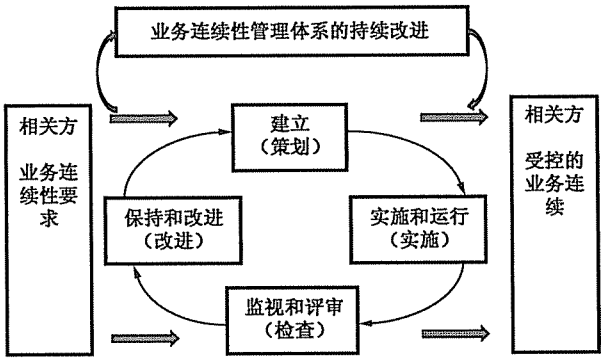

图 1　应用于 BCMS 过程的 PDCA 模型

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”。

3.3

业务连续性 business continuity

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。

[ISO 22300]

3.4

业务连续性管理 business continuity management

识别对组织的潜在威胁以及这些威胁一旦发生可能对业务运行带来的影响的一整套管理过程。该过程为组织建立有效应对威胁的自我恢复能力提供了框架，以保护关键相关方的利益、声誉、品牌和创造价值的活动。

3.5

业务连续性管理体系 business continuity management system；BCMS

用于建立、实施、运行、监视、评审、保持和改进业务连续性，是一个组织整个管理体系的一部分。

注：管理体系包括组织结构、方针、规划活动、职责、程序、过程和资源。

3.6

业务连续性计划 business continuity plan

用于指导组织在业务中断时进行响应、恢复、重新开始和还原到预先确定的业务运行水平的形成文件的程序。

注：业务连续性计划通常包括确保关键业务功能的连续性所需的资源、服务和活动。

3.7

业务连续性方案 business continuity programme

由最高管理者和适当的资源所支撑的，为实施和保持业务连续性管理所进行的持续不断的管理和治理过程。

3.8

业务影响分析 business impact analysis

分析活动和业务中断可能带来的影响的过程。

[ISO 22300]

3.9

能力 competence

经证实的应用知识和技能的本领。

3.10

合格(符合) conformity

满足要求。

[ISO 22300]

3.11

持续改进 continual improvement

为提高绩效进行的循环活动。

[ISO 22300]

3.12

纠正 correction

为消除已发现的不符合所采取的措施。

[ISO 22300]

3.13

纠正措施 corrective action

为消除造成已发现不符合要求的原因并预防其再次发生所采取的措施。

注：在其他不期望结果出现的情况下，采取措施以减少或消除原因并减小影响，或防止再次发生是必要的。此类措施在本定义所指的“纠正措施”概念之外。

[ISO 22300]

3.14

文件 document

信息及其承载媒介。

注1：媒介可以是纸张，计算机磁盘、光盘或其他电子媒体，照片或标准样品，或它们的组合。

注2：一组文件，如若干个规范和记录，也通常称为“文档”。

3.15

存档信息 documented information

需要被组织控制和保持的信息及其承载媒介。

注1：存档信息可以是多种格式的，也可是任何来源的任何承载媒体。

注2：存档信息指：

——管理体系，包括相关的过程；

——为组织运行所生成的信息(文档)；

——所取得结果的证据(记录)。

3.16

有效性 effectiveness

完成制定计划活动并获得计划预期结果的程度。

[ISO 22300]

3.17

事态 event

特定情况集合的发生或变化。

注1：事态可以是一次或多次发生的，可能有多个原因。

注2：事态可以包括不是正在发生的事情。

注3：事态有时可发展为“事件”或“事故”。

注4：没有造成后果的事态也可能被称为“未遂”“接近发生”或“紧急”。

[ISO/IEC 指南 73]

3.18

演练 exercise

在组织中训练、评估、实践和提高绩效的过程。

注1：演练可以用于：验证方针、计划、程序、培训、设备和组织间的协议；对人员的角色和职责进行明确和培训；改善组织间的协调和沟通；识别资源上的差距；提升个人绩能；识别改进机会；把握机会提升应变能力。

注2：测试是演练的一种特殊类型，它包含了对正在计划的演练目标或目的中成功或失败因素的预期。

[ISO 22300]

3.19

事件 incident

可能或将导致中断、损失、紧急状况或危机的情况。

[ISO 22300]

3.20

基础设施 infrastructure

组织运行所必需的设施、设备和服务的体系。

3.21

相关方 interested party

对决策或活动产生影响，受到影响，认为被影响的个人或组织。

注：可以是与组织的任何决策或活动有利益关系的个人或团体。

3.22

内部审核 internal audit

用于管理评审或其他内部目的由组织自身或以组织名义进行的审核，可作为组织符合性自我声明的基础。

注：在许多情况下，特别是一些小型组织，可以由与正在被审核活动无职责的人员进行，以显示独立性。

3.23

启动 invocation

为持续提供关键产品或服务，组织宣布开启其业务连续性安排的活动。

3.24

管理体系 management system

组织建立方针、目标和过程并实现这些目标的相互关联或相互作用的一组元素。

注1：一个管理体系可以关注一个或多个规范要求。

注2：体系元素包括组织结构、角色和职责、计划、运行等。

注3：管理体系的范围可以包括整个组织、组织内某些特定的职能、特定的部分，或是跨越多个组织的一个或多个职能。

3.25

最长可接受中断时间 maximum acceptable outage；MAO

不能提供产品/服务，或者活动无法进行可能带来的负面影响，变得不能接受之前的时间。

注：参见最长可容忍中断时间。

3.26

最长可容忍中断时间 maximum tolerable period of disruption ；MTPD

不能提供产品/服务，或者活动无法进行可能带来的负面影响，变得不能容忍之前的时间。

注：参见最长可接受中断时间。

3.27

测量 measurement

确定一个量值的过程。

3.28

最小业务连续性目标 minimum business continuity objective ；MBCO

在中断中组织为达到其业务连续性目标可以接受的最低标准的服务和(或)产品。

3.29

监视 monitoring

确定一个体系、过程或活动的状态。

注：可能需要通过检查、监督或密切观察来确定状态。

3.30

互助协议 mutual aid agreement

两个或多个实体为了互相帮助而预先达成的共识。

[ISO 22300]

3.31

不符合 nonconformity

未满足要求。

[ISO 22300]

3.32

目标 objective

想要取得的结果。

注 1：目标可以是战略的、策略的或运行层面的。

注 2：目标可以和不同的规范要求相关(例如财政的、健康和安全以及环境目标)，也可以应用于不同的层次(例如战略、组织范围、项目、产品和过程)。

注 3：目标可以用其他方式来表示，例如作为预期结果、意图、运行准则、社会安全目标或用其他意思相近的词来表达(例如目的或宗旨)。

注 4：在公共安全管理体系标准的背景下，公共安全目标是由组织设定的，与公共安全方针一致的，用于达成特定结果的目标。

3.33

组织 organization

为了实现目标形成的具有自身职能，按照一系列职责、权限和相互关系安排的个人或一组人员。

注 1：组织的概念包括但不限于个体商户、公司、集团、企事业单位、研究机构、合伙企业、慈善机构、或是上述单位的结合体，无论其是否为法人团体，公营还是私营。

注 2：对于拥有一个以上运营单位的组织，可以把每一个单独运营的单位视为一个组织。

3.34

外包(动词) outsource (verb)

把组织的部分职能或过程安排给外部组织。

注：虽然外包的职能和过程属于管理体系的范围，但外部组织则在此范围之外。

3.35

绩效 performance

可测量的结果。

注 1：绩效与定量或定性的结果有关。

注 2：绩效与活动、流程、产品(包括服务)、体系或组织的管理有关。

3.36

绩效评估 performance evaluation

确定可测量结果的过程。

3.37

人员 personnel

为组织工作并受其管理的人。

注：人员的概念包括但不限于员工、兼职人员和派遣人员。

3.38

方针 policy

由组织最高管理者正式发布的意图和方向。

3.39

程序 procedure

为进行某项活动或过程所规定的途径。

3.40

过程 process

将输入转化为输出的相互关联或相互作用的一组活动。

3.41

产品和服务 products and services

组织提供给顾客、服务对象和相关方的有益的成果，例如制成品、汽车保险和社区护理。

3.42

优先活动 prioritized activities

事件发生后为了减轻影响必须优先执行的活动。

注：描述此类活动的常用术语包括：紧要的、必要的、重要的、紧急的和关键的。

[ISO 22300]

3.43

记录 record

所取得结果的说明或提供所完成活动的证据。

3.44

恢复点目标 recovery point objective ;RPO

为使活动能够恢复进行，而必须将该活动所用的信息恢复到某时间点。

3.45

恢复时间目标 recovery time objective ;RTO

事件发生后到下列活动完成之间的时间段。

——产品或服务必须恢复，或

——活动必须恢复，或

——资源必须复原。

注：对于产品、服务和活动，恢复时间目标必须小于组织不能接受的导致产品/服务停止供应、活动无法执行等负面影响所需的时间。

3.46

要求 requirement

明示的、通常隐含的或必须履行的需求或期望。

注 1："通常隐含"是指顾客或相关方的惯例或一般做法，所考虑的需求和期望是不言而喻的。

注 2：规定要求是经明示的要求，如：记录信息。

3.47

资源 resources

为了运行和实现目标，组织在需要时可供使用的所有资产、人员、技能、信息、技术（包括工厂和设备）、场地、物资和信息（无论是否为电子格式）。

3.48

风险 risk

对于目标的不确定性影响。

注 1：该影响是偏离预期目标的——正面的或负面的。

注 2：目标可以有不同的方面（例如财政、健康和安全以及环境目标），也可以应用于不同的层次（例如战略、组织范围、项目、产品和过程）。目标可以用其他方式来表示，例如作为预期结果、意图、运行准则、业务连续性目标或用其他意思相近的词来表达（例如目的或宗旨）。

注 3：风险常被描述为潜在事态（ISO/IEC 指南 73 中 3.5.1.3）和后果（ISO/IEC 指南 73 中 3.6.1.3），或它们的组合。

注 4：风险通常被表述为事态的后果（包括环境的变化）和发生的可能性（ISO/IEC 指南 73 中 3.6.1.1）。

注 5：不确定性是指完全或部分缺乏有关某项事态的了解或认识（包括其后果和发生可能性）信息的状态。

注 6：在业务连续性管理体系的背景下，为取得特定的结果，组织在与业务连续性方针保持一致的前提下制定了业务连续性目标。当应用风险和风险管理要素等术语的时候，往往都和组织目标有关。这些目标包括但不仅限于 6.2 中提到的业务连续性目标。

[ISO/IEC 指南 73]

3.49

风险偏好 risk appetite

组织愿意接受或承担风险的数量和类别。

3.50

风险评估　risk assessment

风险识别、风险分析和风险评价的整个过程。

[ISO/IEC 指南 73]

3.51

风险管理　risk management

指导和控制一个组织相关风险的协调活动。

[ISO/IEC 指南 73]

3.52

测试　testing

一个用以确定某事物的存在、质量或真实性的评价程序。

注 1：测试可能会涉及到“试验”。

注 2：测试经常被用于支持计划。

[ISO 22300]

3.53

最高管理者　top management

在最高层指挥和控制组织的一个人或一组人。

注 1：最高管理者有权力在组织内进行授权，并提供资源。

注 2：如果管理体系的范围只涵盖了组织的一部分，那么最高管理者指那些直接指导和操控该部分组织的人。

3.54

验证　verification

通过提供证据对规定要求已得到满足的认定。

3.55

工作环境　work environment

工作时所处的一组条件。

注：条件包括物理的、社会的、心理的和环境的因素（例如温度、承认方式、人因工效和大气成分）。

[ISO 22300]

4　组织环境

4.1　了解组织和组织环境

组织应确定与其意图相关且影响其达到 BCMS 预期结果能力的外部和内部情况。

在建立、实施和保持组织的 BCMS 时，这些情况应被考虑。

组织应识别以下内容并形成文件：

a）　组织的活动、职能、服务、产品、合作方、供应链、与相关方的关系以及与中断事件有关的潜在影响；

b）　业务连续性方针和组织目标以及其他方针，包括其总体风险管理策略间的联系；

c）　组织的风险偏好。

在构建环境时，组织应：

a）　阐明其目标，包括与业务连续性有关的目标；

b）　确定会造成增加风险不确定性的外部和内部因素；

c）　根据风险偏好设定风险准则；

d）　确定 BCMS 的目的。

4.2 理解相关方的需求和期望

4.2.1 总则

在建立 BCMS 时，组织应确定：

a) 与 BCMS 有关的相关方；

b) 这些相关方的要求(即阐明的、通常隐含的或强制性的需求和期望)。

4.2.2 法律和法规要求

组织应建立、实施和保持一个程序(或多个程序)用以识别、利用和评估与业务运行、产品和服务，以及相关方连续性要求相关的适用的法律和法规要求。

组织应确保在建立、实施和保持其 BCMS 时考虑这些适用的法律、法规和经组织认同的其他要求。

组织应将这些信息形成文件并保持更新。应与受影响的员工和其他相关方沟通新制定或变更的法律、法规和其他要求。

4.3 确定业务连续性管理体系的范围

4.3.1 总则

组织应通过确定 BCMS 的边界和适用性来建立其范围。

组织在确定范围时应考虑：

——在 4.1 中涉及的外部和内部因素；

——在 4.2 中涉及的要求。

该范围应为可获得的存档信息。

4.3.2 BCMS 的范围

组织应：

a) 确定组织中被包含在 BCMS 范围内的部分；

b) 在考虑组织的任务、目标、内部和外部职责(包括与相关方有关的)以及法律和法规方面的责任下，建立 BCMS 的要求；

c) 识别 BCMS 范围内的产品、服务和所有相关活动；

d) 考虑相关方的需求和利益，例如客户、投资者、股东、供应链、公共和/或社区的投入和需求、期望和利益(如适用时)；

e) 按照组织规模、性质和复杂性确定合适的 BCMS 范围。

在定义范围时，组织应将删减理由形成文件，任何删减应不影响组织提供达到 BCMS 要求的业务和运行连续性的能力和责任，删减是由业务影响分析或风险评估和适用的法律或法规要求确定的。

4.4 业务连续性管理体系

组织应根据本标准的要求，建立、实施、保持和持续改进 BCMS，包括所需的过程和过程间的相互作用。

5 领导力

5.1 领导力和承诺

整个组织的最高管理者和其他相关管理人员应证明他们在 BCMS 方面的领导力。

例如：领导力和承诺能够通过激励和授权员工为 BCMS 的有效性做出贡献来体现。

5.2 管理承诺

最高管理者应通过以下方式来证明其在 BCMS 方面的领导力和承诺：

——确保已经为业务连续性管理体系制定了方针和目标并确保方针和目标与组织的战略方向是一致的；

——确保业务连续性管理体系的要求纳入组织的业务过程中；

——确保业务连续性管理体系所需的资源可用；

——就业务连续性管理的有效性和符合 BCMS 要求的重要性进行传达；

——确保业务连续性管理体系达到预期结果；

——指导和支持员工为 BCMS 的有效性作贡献；

——推动持续改进；

——支持其他相关管理角色在其职责领域内展示其领导作用和承诺。

注 1：本标准中的“业务”从广义上解释为对于组织的存在而言具有核心价值的活动。

最高管理者应通过以下活动为建立、实施、运行、监视、评审、保持和改进 BCMS 的承诺提供证据：

——建立业务连续性方针；

——确保 BCMS 目标和计划已被制定；

——为业务连续性管理确定角色、职责和能力；

——任命一名或多名具有适当权限和能力的 BCMS 责任人员来负责实施和保持 BCMS。

注 2：这些人员在组织内部可以承担其他职责。

最高管理者应通过以下方式确保相关角色的职责和职权在组织内被授权和传达：

——确定风险接受准则和可接受的风险级别；

——积极参与演练和测试；

——确保 BCMS 的内部审核被执行；

——实施 BCMS 的管理评审；

——证明其对持续改进的承诺。

5.3 方针

最高管理者应建立业务连续性方针，该方针应：

a) 符合组织的宗旨；

b) 为业务连续性目标的制定提供框架；

c) 包含满足适应要求的承诺；

d) 包含对 BCMS 进行持续改进的承诺。

BCMS 方针应：

——为可获得的存档信息；

——在组织内部传达；

——适当时使相关方能够获得；

——在规定的时间间隔内或当重大变化发生时对持续适用性进行评审。

组织应保留业务连续性方针方面的存档信息。

5.4 组织的角色、职责和权力

最高管理者应该确保相关角色的职责和权限在组织内部被授权和传达。

最高管理者应分配职责和职权以：

a) 确保管理体系符合本标准的要求；
b) 向最高管理者报告 BCMS 的绩效。

6 策划

6.1 应对风险和机会的措施

当进行 BCMS 策划时，组织应考虑 4.1 提到的因素和 4.2 提到的要求，并确定需要应对的风险和机会以：

a) 确保管理体系能够达到预期结果；
b) 防止或减少不良影响；
c) 实现持续改进。

组织应策划：

a) 应对风险和机会的措施；
b) 如何：
   1) 将这些措施在 BCMS 的过程中进行整合和实施(见 8.1)；
   2) 评估这些措施的有效性(见 9.1)。

6.2 业务连续性目标和实现计划

最高管理者应确保制定业务连续性目标并将其传达给组织内具有相关职责的人员。

业务连续性目标应：

a) 与业务连续性方针保持一致；
b) 考虑组织为实现目标所能接受的产品和服务的最低级别；
c) 是可测量的；
d) 考虑适用的要求；
e) 进行监视和适当的更新。

组织应保留与业务连续性目标有关的存档信息。

为了达到业务连续性目标，组织应确定：

——谁将负责；
——要做什么；
——需要什么资源；
——什么时候完成；
——怎样评估结果。

7 支持

7.1 资源

组织应确定并提供建立、实施、保持和持续改进 BCMS 所需的资源。

7.2 能力

组织应：

a) 根据绩效影响，确定其管理下的工作人员应具备的必要能力；
b) 确保人员在适当的教育、培训和实践经验的基础上能够胜任；

c) 在适用的情况下，采取措施以获得必要的能力，并评估所采取措施的有效性；

d) 保留适当的存档信息作为能力的证据。

注：适用的措施包括：提供培训、指导、重新分配当前工作人员或聘任有能力的人。

7.3 意识

在组织管理下的工作人员应了解：

a) 业务连续性方针；

b) 他们对 BCMS 有效性的贡献，包括改进业务连续性管理绩效带来的益处；

c) 不符合 BCMS 要求的后果；

d) 在发生中断事件时各自的角色。

7.4 沟通

组织应确定与 BCMS 有关的内部和外部沟通的需求，包括：

a) 沟通的内容；

b) 沟通的时机；

c) 沟通的对象。

组织应建立、实施和保持一个程序（或多个程序）以实现：

——与组织的相关方和雇员之间的内部沟通；

——与顾客、合作方、当地社区和包括媒体在内的其他相关方的外部沟通；

——收集、存档和回应来自相关方的信息；

——在适当的情况下，采用和纳入国家或地区的威胁预警体系（或类似的体系），供规划和运行使用；

——发生中断事件时，确保沟通手段的可用性；

——在合适的情况下，促进与相关政府机构进行有组织的沟通，确保多个响应机构和人员之间的协作；

——对于正常通信中断期间所需要的备用通信方式进行操作和测试。

注：关于应对事件的更多沟通要求，见 8.4.3。

7.5 存档信息

7.5.1 总则

组织的 BCMS 应包括：

——本标准所要求的存档信息；

——由组织确定的为实现 BCMS 绩效而必须的存档信息。

注：BCMS 的存档信息范围因组织而异：

——组织的规模以及它的活动、过程、产品和服务的类型；

——过程及其相互作用的复杂性；

——人员能力。

7.5.2 创建和更新

在创建和更新存档信息时，组织应确保合适的：

a) 标识和描述（如标题、日期、作者或编号）；

b) 格式（例如语言、软件版本、图形）、介质（例如纸质、电子的）以及对适宜性和充分性的评审和审批。

7.5.3 存档信息的管理

BCMS 和本标准所要求的存档信息应受控以确保：

a) 在需要使用的地点和时间是可用的和适宜的；

b) 得到切实的保护(例如丧失机密性、使用不当或失去完整性)。

适当时，组织应采取以下措施对存档信息进行控制：

——分发、访问、获取和使用；

——存储和保存，包括保护可读性；

——变更控制(例如版本控制)；

——保留和处置；

——获取和使用；

——可读性(即清晰可读)的保持；

——防止作废文件的非预期使用。

根据具体情况，组织确定的在 BCMS 的策划和运行中所必须的外来存档信息应被识别和控制。

建立存档信息的控制时，组织应确保对存档信息进行充分的保护(例如避免信息泄露、未授权修改或删除)。

注：信息获取权是指有关存档信息浏览许可的决定，或浏览和改变存档信息的许可和权力。

8 实施

8.1 实施的策划和控制

组织应通过以下方式策划、实施和控制为满足要求所需要的过程，并实施 6.1 中所确定的措施。

a) 建立过程准则；

b) 按照准则执行这些过程的控制；

c) 为了确定流程按计划进行，在必要的范围内保留存档信息。

组织应控制计划内的变更以及评审非预期的变更带来的结果，必要时采取行动减轻负面影响。

组织应确保外包过程的受控。

8.2 业务影响分析和风险评估

8.2.1 总则

组织应建立、实施和保持一个正式的、形成文件的业务影响分析和风险评估过程。

a) 建立评估的环境、确定标准和评估中断事件的潜在影响；

b) 考虑组织遵从的法律要求和其他要求；

c) 包括系统的分析、风险处置优先级以及相关的成本；

d) 明确业务影响分析和风险评估所要求的输出；

e) 提出输出信息更新和保密的要求。

注：不同的业务影响分析和风险评估方法会决定上述活动的执行顺序。

8.2.2 业务影响分析

组织应建立、实施、保持一个正式的、形成文件的确定连续性和恢复优先级、目标和指标的评价过程。这个过程应包括对支持该组织的产品和服务活动中断所造成的影响的评估。

业务影响分析应包括以下内容：

a) 识别支持产品和服务交付的活动；
b) 评估这些活动中断后随时间推移的影响；
c) 在最低可接受水平上制定业务恢复优先级时间表，要考虑在某时间内，没有恢复这些业务所造成的影响是不可接受的；
d) 识别这些活动间的依赖关系及支持资源，包括供应商、外包方和其他相关方。

8.2.3 风险评估

组织应建立、实施和保持一个正式的形成文件的风险评估过程。该过程能系统地识别、分析和评价中断事件给组织带来的风险。

注：这一过程可以参照 ISO 31000 来制定。

组织应：

a) 识别中断对于组织的优先活动以及过程、系统、信息、人员、资产、外包方和其他支持资源所带来的风险；
b) 系统地分析风险；
c) 评价哪种中断风险需要处理；
d) 识别与业务连续性目标相符以及与组织的风险偏好一致的处理措施。

注：组织必须意识到特定金融或政府部门会对这些风险披露的详细程度有要求。另外，特定的社会需求也要求在适当程度上共享此类信息。

8.3 业务连续性策略

8.3.1 确定和选择

策略的确定和选择应以业务影响分析和风险评估的输出结果为基础。

组织应确定一个适当的业务连续性策略以：

a) 保护优先活动；
b) 稳定、连续、重启和恢复优先活动以及该活动所依赖的活动和支持资源；
c) 减轻、响应和管理影响。

策略的确定应该包括批准活动恢复的优先级时间表。

组织应对供应商的业务连续能力进行评价。

8.3.2 建立资源要求

组织应为执行所选择的策略设置资源要求。所需考虑的资源类型应包括但不限于：

a) 人员；
b) 信息和数据；
c) 建筑物、工作环境和配套设施；
d) 设施、设备和耗材；
e) 信息通信技术系统；
f) 交通工具；
g) 资金；
h) 合作方和供应商。

8.3.3 保护和缓解

对于需要处理的已识别风险，组织应考虑采用主动措施以：

a) 减少中断的可能性；

b) 缩短中断的时间；

c) 限制中断对组织的关键产品和服务的影响。

组织应根据其风险偏好选择和实施适当的风险处置措施。

8.4 建立和实施业务连续性程序

8.4.1 总则

组织应以业务影响分析中已识别的恢复目标为基础，建立、实施和保持业务连续性程序，来管理中断事件和保证活动的连续性。

组织应将程序(包括必要的安排)形成文件，以确保活动的连续性和对中断事件的管理。

程序应：

a) 建立适当的内部和外部沟通协议；

b) 针对业务中断期间需要采取的紧急步骤进行详细规定；

c) 灵活地应对非预期的威胁和不断变化的内部和外部环境；

d) 关注可能导致潜在运行中断的事态影响；

e) 在已提出的假设和在相互依赖关系分析的基础上进行开发；

f) 通过实施适当的减缓策略有效地将后果最小化。

8.4.2 事件响应机制

组织应利用对事件管理有职责、权力和能力的人员来建立并实施中断事件响应程序和管理机制，并将其形成文件。

响应机制应：

a) 识别开始采取正式响应措施的影响阈值；

b) 评估中断事件的性质和范围以及潜在影响；

c) 启动适当的业务连续性响应；

d) 具备用于启动、运行、协调和沟通的响应过程和程序；

e) 具备可用于支持过程和程序的资源来处理中断事件以减轻影响；

f) 与相关方、权力机构以及媒体进行沟通。

组织应采取人身安全第一优先的原则，通过与相关方进行协商来决定是否就其重大风险和影响进行外部沟通，并将其决定形成文件。如果决定要进行外部沟通，组织应建立和实施针对此类与外部以及在适当情况下与媒体进行沟通和预警的程序。

8.4.3 预警和沟通

组织应建立、实施和保持程序以：

a) 发现事件；

b) 对事件进行日常监视；

c) 进行组织内部沟通并接收、存档和响应来自相关方的反馈；

d) 对国家或地区的威胁预警体系(或类似的体系)进行接收、记录和响应；

e) 确保在中断事件期间沟通手段的可用；

f) 为同应急响应人员进行有序的沟通提供便利；

g) 记录与事件、采取的措施和所做的决定相关的重要信息，适当时，下列事项应被考虑和实施：

——向将要受到正在发生或者即将发生的中断事件潜在影响的相关方进行预警；

——确保多个响应组织和人员之间的协同；

——通信设施的运行。

沟通和预警程序应定期进行演练。

8.4.4 业务连续性计划

组织应建立响应中断事件，以及如何在预定的时间内继续或恢复其活动的文件化程序。此程序应能针对使用者提出要求。

业务连续性计划应全部包含：

a) 确定在事件发生时和发生后相关人员和团队的角色和职责；

b) 一个启动响应的过程；

c) 处理中断事件所造成的直接后果的详细说明，要考虑到：

1) 个人福利；

2) 响应中断的策略、战术和执行方案的选择；

3) 防止进一步损失或优先活动无法执行；

d) 如何以及在何种情况下组织与员工及其亲属、关键相关方、以及紧急联络人进行沟通；

e) 组织将如何在预定的时间里继续或恢复其优先活动；

f) 事件发生后，组织的媒体响应的详细说明包括：

1) 沟通策略；

2) 首选的媒体接口；

3) 起草媒体声明的方针或模板；

4) 合适的发言人。

g) 事件一旦结束后的退出过程。

每个计划应确定：

——目的和范围；

——目标；

——启动的准则和程序；

——实施程序；

——角色、职责和职权；

——沟通的要求和程序；

——内部和外部的依赖关系和相互作用；

——资源的要求；

——信息流和存档过程。

8.4.5 恢复

组织应有用以在事件发生后从所采用的临时措施中恢复并重新开始业务正常活动的文件化程序。

8.5 演练和测试

组织应演练和测试其业务连续性程序，以确保它们和业务连续性目标相一致。

组织进行的演练和测试应：

a) 与 BCMS 的范围和目标保持一致；

b) 基于适当的，有周密计划以及明确目的和目标的场景；

c) 持续实施并召集相关方对其整套业务连续性安排进行验证；

d) 最大限度降低运行中断的风险；

e) 形成正式的演练总结报告，内容包括输出结果、建议和实施改进的措施；

f) 在促进持续改进的情况下被评审；

g) 按计划的时间间隔或者当组织或其运营环境出现重大变化时进行。

9 绩效评估

9.1 监视、测量、分析和评价

9.1.1 总则

组织应确定：

a) 需要被监视和测量的内容；

b) 监视、测量、分析和评价方法，确保得到有效的结果；

c) 何时进行监视和测量；

d) 何时进行监视和测量结果的分析和评价。

组织应保留适当的存档信息作为结果的证据。

组织应评价 BCMS 的绩效和 BCMS 的有效性。

另外，组织应：

——在不符合发生前采取必要措施以应对不利的趋势和结果；

——保留相关的存档信息作为结果的证据。

用于监视绩效的程序应提供：

——制定符合组织需求的绩效指标；

——对组织的业务连续性方针、目标和指标完成程度的监视；

——保护其优先级活动的过程、程序和职能的绩效；

——对本标准和业务连续性目标符合性的监视；

——对 BCMS 缺陷绩效的历史证据的监视；

——记录监视和测量的数据和结果，为采取后续纠正措施提供便利。

注：缺陷绩效包括不符合、未遂事件、错误警报和实际发生的事件。

9.1.2 业务连续性程序的评价

a) 组织应对其业务连续性程序和能力进行评价，以确保其持续的适宜性、充分性和有效性；

b) 这些评价应通过定期评审、演练、测试、事件总结报告和绩效评估来进行。重大变更应在一个(或多个)程序中得到及时的反映；

c) 组织应定期评价其对现行法律法规要求、行业最佳实践及其自身业务连续性方针和目标的符合性；

d) 组织应按计划的时间间隔或者当组织或运营环境出现重大变化时进行评估。

当中断事件发生并导致业务连续性程序的启动时，组织应进行事后评审并记录其结果。

9.2 内部审核

组织应按计划的时间间隔进行内部审核，提供信息以表明业务连续性管理体系是否：

a) 符合：

1) 组织自身对 BCMS 的要求；

2) 本标准的要求。

b) 得到有效的实施和保持。

组织应：

——策划、建立、实施和保持一个或多个审核方案，包括频次、方法、职责、策划要求和报告。审核方案应该考虑到所关注过程的重要性和以往审核的结果。

——确定每次审核的审核准则和范围。

——审核员的选择和审核的执行应确保审核过程的客观性和公正性。

——确保审核结果被报告给相关管理层。

——保留执行审核方案和审核结果的存档信息作为证据。

审核方案，包括任何日程安排，应以组织活动的风险评估和以往的审核结果为基础。审核程序应涵盖范围、频次、方法和能力，以及执行审核和报告结果的职责和要求。

负责被审核领域的管理层人员应确保及时采取必要的纠正和纠正措施，以消除发现的不符合及其根源，不得无故拖延。后续活动应该包括对所采取措施进行验证以及验证结果的报告。

9.3 管理评审

最高管理者应按计划的时间间隔评审组织的 BCMS，以确保其持续适宜、充分和有效。

管理评审应考虑以下内容：

a) 以往管理评审措施的状态；

b) 与业务连续性管理体系有关的外部和内部因素的变化；

c) 业务连续性绩效的信息，包括在以下方面的趋势：

1) 不符合项及纠正措施；

2) 监视和测量评价结果；

3) 审核结果。

d) 持续改进的机会。

管理评审应该考虑到组织的绩效，包括：

——以往管理审核的后续跟进；

——改变 BCMS 的变更需求，包括方针和目标；

——改进机会；

——BCMS 的审核和评审的结果，包括对关键供应商和合作方(适用时)；

——可能用于改进组织的 BCMS 绩效和有效性的技术、产品或程序；

——纠正措施的状态；

——演练和测试的结果；

——在以往的风险评估中没有引起足够重视的风险和问题；

——无论是 BCMS 范围内部还是外部的任何能对 BCMS 产生影响的变化；

——方针的充分性；

——改进建议；

——在中断事件中采取的措施以及从中吸取的经验；

——新出现的良好实践和指导。

管理评审的输出应当包括与持续改进机会相关的决定以及可能存在的对 BCMS 变更的需求，并且还包括：

a) 对 BCMS 范围的变化；

b) 对 BCMS 有效性的改进；

c) 对风险评估、业务影响分析、业务连续性计划和相关程序的更新；

d) 对用以响应可能对 BCMS 产生影响的内部或外部事件的程序和控制措施的修改，包括对下列事项的变更：

1) 业务和运行要求；

2） 风险降低和安全要求；
3） 运行条件和过程；
4） 法律和法规要求；
5） 合同义务；
6） 风险级别和/或风险接受准则；
7） 资源需求；
8） 资金和预算要求；

e） 对控制措施的有效性进行测量的方式。

组织应保留存档信息作为管理评审结果的证据。

组织应：

——向相关方传达管理评审的结果；

——针对这些结果采取适当的措施。

10 改进

10.1 不符合和纠正措施

当不符合发生时，组织应：

a） 识别不符合；

b） 对不符合做出反馈，并且，适当时：
1） 采取措施进行控制和纠正；
2） 对结果进行处理。

c） 评估为消除不符合的原因所采取措施的需求，为了防止不符合在别处出现或者再现，可采取下列方法：
1） 评审不符合；
2） 确定引起不符合的原因；
3） 确定是否存在或有可能出现类似不符合；
4） 评估纠正措施的必要性以确保不符合不会重复或在别处发生；
5） 确定和实施需要的纠正措施；
6） 评审所采取的任何纠正措施的有效性；
7） 必要时，对 BCMS 进行变更。

d） 实施需要的任何措施；

e） 评审所采取的任何纠正措施的有效性；

f） 必要时，对 BCMS 进行变更。

纠正措施应与所遇到不符合的影响程度相适应。

组织应保留下列存档信息作为证据：

——不符合的性质和任何所采取的后续措施；

——各项纠正措施的结果。

10.2 持续改进

组织应持续改进 BCMS 的适宜性、充分性或有效性。

注：组织可以运用 BCMS 的过程来实现改进，例如领导力、策划和绩效评估。

参 考 文 献

[1] ISO 9001, Quality management systems—Requirements.

[2] ISO 14001, Environmental management systems—Requirements with guidance for use.

[3] ISO 19011, Guidelines for auditing management systems.

[4] ISO/IEC 20000-1, Information Technology—Service Management.

[5] ISO 22300, Societal security—Terminology.

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

[7] ISO/IEC 24762, Information technology—Security techniques—Guidelines for Information and communications technology disaster recovery services.

[8] ISO/IEC 27001, Information Security Management Systems.

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

[10] ISO 31000, Risk Management—Principles and Guidelines.

[11] ISO/IEC 31010, Risk management—Risk assessment techniques.

[12] ISO/IEC Guide 73, Risk management—Vocabulary.

[13] BS 25999-1, Business continuity management—Code of practice, British Standards Institution (BSI).

[14] BS 25999-2, Business continuity management—Specification, British Standards Institution (BSI).

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

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

[17] BusinessContinuity Plan Drafting Guideline, Ministry of Economy, Trade and Industry (Japan), 2005.

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

[19] ANSI/ASIS SPC. 1, Organizational Resilience: Security, Preparedness, and Continuity Managements Systems—Requirements with Guidance for UseSS 540: 2008, Singapore Standard for Business Continuity Management.

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

中 华 人 民 共 和 国
国 家 标 准
公共安全 业务连续性管理体系 要求
GB/T 30146—2013/ISO 22301:2012
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100013)
北京市西城区三里河北街16号(100045)
网址 www.spc.net.cn
总编室:(010)64275323 发行中心:(010)51780235
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 1.75 字数 40 千字
2013年12月第一版 2013年12月第一次印刷
*
书号:155066·1-47985 定价 27.00元

GB/T 30146-2013

打印日期:2013年12月26日 F009