ICS 03.100.01
CCS A 90

中华人民共和国国家标准

GB/T 30146—2023/ISO 22301:2019
代替 GB/T 30146—2013

安全与韧性　业务连续性管理体系　要求

Security and resilience—Business continuity management systems—Requirements

（ISO 22301:2019,IDT）

2023-03-17 发布　　2023-10-01 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 30146—2013《安全与韧性　业务连续性管理体系　要求》,与GB/T 30146—2013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,2013版的第1章);

——删除了部分术语和定义(见2013版的3.4、3.5、3.7、3.12、3.14、3.17、3.18、3.20、3.22、3.23、3.25、3.26、3.28、3.30、3.36、3.37、3.39、3.43～3.45、3.49～3.52、3.54、3.55);

——增加了术语"中断"和"影响"(见3.10、3.13);

——删除了"管理承诺"(见2013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7.4,2013版的7.4);

——将"存档信息"改为"成文信息"(见7.5,2013版的7.5);

——将"实施"改为"运行"(见第8章,2013版的第8章);

——更改了"业务连续性策略"的相关内容(见8.3,2013版的8.3);

——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,2013版的第9章);

——更改了"监视、测量、分析和评价"的相关内容(见9.1,2013版的9.1.1);

——删除了"业务连续性程序的评价"(见2013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9.3,2013版的9.3);

——更改了"持续改进"的相关内容(见10.2,2013版的10.2)。

本文件等同采用ISO 22301:2019《安全与韧性　业务连续性管理体系　要求》(英文版)。

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:北方工业大学、中国标准化研究院、阿里云计算有限公司、中国网络安全审查技术与认证中心、苏州苏大教育服务投资发展(集团)有限公司、国网四川省电力公司、中铁上海工程局集团有限公司、上海速邦信息科技有限公司、北京安创信达科技有限公司、湖北省标准化与质量研究院、北京科技大学、北京市科学技术研究院、北京市科学技术研究院城市安全与环境科学研究所、浙江圣雪休闲用品有限公司、和也健康科技有限公司、厦门市九安安全检测评价事务所有限公司、中国家用电器研究院、标准联合咨询中心股份公司。

本文件主要起草人:秦挺鑫、周倩、柳长安、李津、徐术坤、孙晓鲲、王皖、魏军、董晓媛、史运涛、尤其、陆庆、常政威、万兴权、刘玉节、张英华、徐凤娇、张超、王晶晶、邓哲、张卓、代宝乾、羊静、高玉坤、梁育刚、万谊平、董哲、徐然、姚卫华、邱有富、朱晓辉、方志财、廖钟财、卢成绪。

本文件及其所代替文件的历次版本发布情况为:

——2013年首次发布为GB/T 30146—2013;

——本次为第一次修订。

引　言

0.1　总则

本文件提出了实施和保持业务连续性管理体系(BCMS)的架构和要求,其建立业务连续性与组织中断发生后可以或不可以接受的影响的数量和类型相适应。

保持 BCMS 的结果取决于组织所处环境的法律法规、组织和行业要求、提供的产品和服务、采用的过程、组织的规模和架构以及相关方要求。

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方针和目标的必要性;

——运行并保持过程、能力和响应框架确保组织经受住干扰;

——监视和评审业务连续性管理体系的绩效和有效性;

——基于定性和定量测量的持续改进。

和其他管理体系一样,BCMS 包括以下部分:

a) 方针;

b) 具有明确职责、具备相应能力的人员;

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) 绩效评价;

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。

0.2　业务连续性管理体系的效益

BCMS 的目标是准备、提供并保持组织在中断期间持续运营的整体能力。为了实现这一目标,组织要:

a) 从业务角度:

1) 支持其战略目标;

2) 建立竞争优势;

3) 保护并提高其声誉和信誉;

4) 促进组织韧性。

b) 从财务角度:

1) 降低法律和财务风险;

2) 减少直接和间接的中断成本。

c) 从相关方角度:

1) 保护生命、财产和环境;

2) 考虑相关方的期望;

3） 增强组织有能力成功的信心。

d） 从内部过程角度：

1） 提高组织在业务中断期间保持有效的能力；

2） 证明有效和高效地主动控制风险；

3） 解决运行脆弱性。

0.3 策划—实施—检查—改进循环

本文件使用策划（建立）、实施（执行和运行）、检查（监控和评审）和改进（保持和改进）（PDCA）循环来建立、保持并持续改进组织 BCMS 的有效性。

这确保了与 ISO 9001、ISO 14001、ISO/IEC 20000-1、ISO/IEC 27001 和 ISO 28000 等其他管理体系标准在一定程度上的一致性，从而支持了与相关管理体系的一致和整合的实施和运作。

根据 PDCA 循环，第 4 章至第 10 章包括以下内容：

——第 4 章介绍了组织建立 BCMS 环境、需求、要求和范围时的必要要求；

——第 5 章总结了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述其期望；

——第 6 章描述了制定整个 BCMS 战略目标和指导原则的要求；

——第 7 章支撑 BCMS 运行，在记录、控制、保持和保留所需的成文信息的同时，建立能力，定期/根据需要与相关方建立沟通；

——第 8 章定义了业务连续性需求，确定了如何解决这些需求，并制定了在中断期间管理组织的程序；

——第 9 章总结了测量业务连续性绩效、BCMS 与本文件的符合性以及进行管理评审所需的要求；

——第 10 章识别和纠正 BCMS 的不符合，并通过采取纠正措施持续改进。

0.4 本文件内容

本文件符合 ISO 管理体系标准要求。这些要求包括高层架构、相同的核心内容以及具有核心概念的通用术语，旨在使实施多个 ISO 管理体系标准的使用者受益。

本文件不包括特定于其他管理体系的要求，尽管本文件的要素可以与其他管理体系的要素保持一致或集成。

本文件包含组织可用于实施 BCMS 和符合评定的要求。组织可通过以下方式证明其符合本文件：

——做出自我决定和自我声明；

——寻求与组织有利益关系的各方（如客户）确认其符合性；

——寻求组织外部的一方确认其自我声明；

——寻求外部组织对其 BCMS 进行认证/注册。

本文件中第 1 章至第 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 章至第 10 章包含用于评估是否符合本文件的要求。

本文件运用了下列助动词：

a） “应”表示要求；

b） “宜”表示建议；

c） “可”表示许可；

d） “能”表示可能性或能力。

标记为“注”的信息用于指导理解或澄清相关要求。第 3 章使用的“注”提供了补充术语数据的附加信息，可以包含与术语使用有关的规定。

安全与韧性　业务连续性管理体系　要求

1　范围

本文件规定了实施、保持和改进管理体系的要求，以防止、减少中断事件发生的可能性，为中断做好准备，做出响应并从中恢复。

本文件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其组成部分。这些要求的适用范围取决于组织的运行环境和复杂性。

本文件适用于有如下需求的各种类型和规模的组织：

a)　实施、保持和改进 BCMS；

b)　确保符合该组织声明的业务连续性方针；

c)　需要能够在中断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 BCMS 增强其韧性。

本文件可用于评估一个组织满足自身业务连续性需求和责任的能力。

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 resilience—Vocabulary)

3　术语和定义

ISO 22300 界定的以及下列术语和定义适用于本文件。

3.1

活动　activity

实现预定输出结果的一个或多个任务的集合。

[来源：ISO 22300:2018，3.1，有修改，示例已被删除]

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(3.26)。

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：内部审核由组织(3.21)自己或代表组织的外部机构开展。

注 3：ISO 19011 中定义了“审核证据”和“审核准则”。

注 4：审核的基本要素是由对被审核客体不承担责任的人员，对客体是否按程序执行来确定其是否符合(3.7)。

注 5：内部审核可用于管理评审和其他内部目的，并可构成组织符合性声明的基础。独立性可以通过不承担被审核活动(3.1)的责任来证明。外部审核包括第二方和第三方审核。第二方审核由组织的利益相关方开展，如顾