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

客或代表他们的其他人。第三方审核由外部独立审核机构开展，如提供符合认证/注册的机构或政府机构。

注6:这是ISO管理体系标准高级结构的通用术语和核心定义之一。通过加入注4和注5对原始定义进行了修改。

3.3

业务连续性 business continuity

在中断(3.10)期间，组织(3.21)以预先设定的能力在可接受的时间内连续交付产品和服务(3.27)的能力。

［来源：ISO 22300:2018,3.24,有修改］

3.4

业务连续性计划 business continuity plan

指导组织(3.21)响应中断(3.10)并重新开始、恢复和还原产品和服务(3.27)的交付以符合其业务连续性(3.3)目标(3.20)的成文信息(3.11)。

［来源：ISO 22300:2018,3.27,有修改，注已被删除］

3.5

业务影响分析 business impact analysis

分析一段时间内中断(3.10)对组织(3.21)造成的影响(3.13)的过程(3.26)。

注：产出是业务连续性(3.3)要求(3.28)的陈述和理由。

［来源：ISO 22300:2018,3.29,有修改，注已被删除］

3.6

能力 competence

运用知识和技能实现预期结果的本领。

注：这是ISO管理体系标准高级结构的通用术语和核心定义之一。

3.7

符合 conformity

满足要求(3.28)。

注：这是ISO管理体系标准高级结构的通用术语和核心定义之一。

3.8

持续改进 continual improvement

为提高绩效(3.23)开展的循环活动(3.1)。

注：这是ISO管理体系标准高级结构的通用术语和核心定义之一。

3.9

纠正措施 corrective action

为消除不符合(3.19)的原因并预防其再次发生所采取的行动。

注：这是ISO管理体系标准高级结构的通用术语和核心定义之一。

3.10

中断 disruption

导致产品和服务(3.27)预期交付与组织(3.21)目标(3.20)相比出现非计划负偏差的预期或非预期事件(3.14)。

［来源：ISO 22300:2018,3.70,有修改］

3.11

成文信息 documented information

需要被组织(3.21)控制和保持的信息及其载体。

注1:成文信息可以任何格式和载体存在，并可来自任何来源。

注2:成文信息可涉及:

——管理体系(3.16),包括相关过程(3.26);

——为组织运行产生的信息(文档);

——结果实现的证据(记录)。

注3:这是ISO管理体系标准高级结构的通用术语和核心定义之一。

3.12

有效性 effectiveness

完成策划的活动(3.1)并得到策划结果的程度。

注:这是ISO管理体系标准高级结构的通用术语和核心定义之一。

3.13

影响 impact

影响目标(3.20)的中断(3.10)的结果。

[来源:ISO 22300:2018,3.107,有修改]

3.14

事件 incident

导致或可能导致中断(3.10)、损失、紧急情况或危机的事态。

[来源:ISO 22300:2018,3.111,有修改]

3.15

相关方 interested party

利益相关者 stakeholder

可影响决策或活动(3.1)、受决策或活动所影响、或自认为受决策或活动影响的个人或组织(3.21)。

示例:客户、所有者、组织内的人员、供方、银行、监管者、工会、合作伙伴以及可包括竞争对手或相对立的社会群体。

注1:决策者可以是相关方之一。

注2:受影响的社区和当地居民被视为相关方。

注3:这是ISO 管理体系标准高级结构的通用术语和核心定义之一。最初的定义通过增加示例、注1和注2被修改。

3.16

管理体系 management systems

组织(3.21)建立方针(3.24)和目标(3.20)以及实现这些目标的过程(3.26)的相互关联或相互作用的一组要素。

注1:一个管理体系可以针对单一领域或几个领域。

注2:管理体系要素包括组织结构、角色和职责、策划和运行。

注3:管理体系的范围可能包括整个组织,组织中特定的职能或特定的部分,以及跨多个组织的一个或多个职能。

注4:这是ISO管理体系标准高级结构的通用术语和核心定义之一。

3.17

测量 measurement

确定数值的过程(3.26)。

注:这是ISO管理体系标准高级结构的通用术语和核心定义之一。

3.18

监视 monitoring

确定体系、过程(3.26)或活动(3.1)的状态。

注1:要确定状态,可能需要检查、监督或严格观察。

注2:这是ISO管理体系标准高级结构的通用术语和核心定义之一。

3.19

不符合 nonconformity

未满足要求(3.28)。

注：这是ISO管理体系标准高级结构的通用术语和核心定义之一。

3.20

目标 objective

要实现的结果。

注1:目标可以是战略的、战术的或操作层面的。

注2:目标可以涉及不同的领域(如财务的、健康与安全和环境的目标),并可应用于不同的层次[如战略的、组织整体的、项目、产品和过程(3.26)的]。

注3:可以采用其他的方式表述目标，例如：采用预期的结果、目的或行动准则作为业务连续性(3.3)目标，或使用其他有类似含义的词(如目的、重点或标的)。

注4:在业务连续性管理体系(3.16)环境中，组织(3.21)制定的业务连续性目标与业务连续性方针(3.24)保持一致，以实现特定的结果。

注5:这是ISO管理体系标准高级结构的通用术语和核心定义之一。

3.21

组织 organization

为实现目标(3.20),由职责、权限和相互关系构成自身功能的一个人或一组人。

注1:组织的概念包括但不限于代理商、公司、集团、商行、企事业单位、行政机构、合营公司、协会、慈善机构或研究机构，或上述组织的部分或组合，无论是否为法人组织，公有的或私有的。

注2:对于具有多个运营单元的组织，单个运营单元可以定义为组织。

注3:这是ISO管理体系标准高级结构的通用术语和核心定义之一。最初的定义通过增加注2被修改。

3.22

外包 outsource

安排外部组织(3.21)承担组织的部分职能或过程(3.26)。

注1:虽然外包的职能或过程是在组织的管理体系(3.16)范围内，但是外部组织处在管理体系(3.16)范围之外。

注2:这是ISO 管理体系标准高级结构的通用术语和核心定义之一。

3.23

绩效 performance

可测量的结果。

注1:绩效可能涉及定量的或定性的结果。

注2:绩效可能涉及活动(3.1)、过程(3.26)、产品(包括服务)、体系或组织(3.21)。

注3:这是ISO管理体系标准高级结构的通用术语和核心定义之一。

3.24

方针 policy

由最高管理者(3.31)正式发布的组织(3.21)的宗旨和方向。

注：这是ISO 管理体系标准高级结构的通用术语和核心定义之一。

3.25

优先活动 prioritized activity

在中断(3.10)期间，为避免对业务造成不可接受的影响(3.13)而被赋予紧急性的活动(3.1)。

[来源：ISO 22300:2018,3.176,有修改，注已被删除]

3.26

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(3.1)。

注：这是 ISO管理体系标准高级结构的通用术语和核心定义之一。

3.27

产品和服务 product and service

组织(3.21)向相关方(3.15)提供的产出和成果。

示例：制造品、汽车保险、社区护理。

[来源：ISO 22300:2018,3.181,有修改，“产品或服务”替换为“产品和服务”]

3.28

要求 requirement

明示的、通常隐含的或强制履行的需求或期望。

注1:“通常隐含”是指组织(3.21)和相关方(3.15)的惯例或一般做法，所考虑的需求或期望是不言而喻的。

注2:规定要求是经明示的要求，如：在成文信息(3.11)中阐明。

注3:这是ISO管理体系标准高级结构的通用术语和核心定义之一。

3.29

资源 resource

为了运行和实现目标(3.20),组织(3.21)在需要时保证具备的、可供使用的所有资产(包括工厂和设备)、人员、技能、技术、场所、供应和信息(无论是否电子化)。

[来源：ISO 22300:2018,3.193,有修改]

3.30

风险 risk

不确定性对目标(3,20)的影响。

注1:影响是指偏离预期，可能是正面的或负面的。

注2:不确定性是对某个事件，及其后果或可能性的相关信息缺失或了解片面的状态。

注3:通常，风险是通过有关可能事件(如 ISO Guide 73所定义)和后果(如 ISO Guide 73所定义)或两者的组合来描述其特性的。

注4:通常，风险是以某个事件的后果(包括情况的变化)及其发生的可能性(如ISO Guide 73所定义)的组合来表述的。

注5:这是 ISO管理体系标准高级结构的通用术语和核心定义之一。最初的定义通过增加“对目标”进行修改，从而保持与ISO 31000的一致性。

3.31

最高管理者 top management

在最高层指挥和控制组织(3.21)的一个人或一组人。

注1:最高管理者在组织内有授权和提供资源(3.29)的权力。

注2:如果管理体系(3.16)的范围仅覆盖组织的一部分，在这种情况下，最高管理者是指管理和控制组织的这部分的一个人或一组人。

注3:这是ISO管理体系标准高级结构的通用术语和核心定义之一。

4 组织环境

4.1 理解组织和组织环境

组织应确定与其意图相关且影响其达到业务连续性管理体系(BCMS) 预期结果能力的外部和内部情况。

注：这些情况受组织总体目标、产品和服务以及可能承担或不承担的风险的数量和类型的影响。

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) 相关方的要求。

4.2.2 法律和法规要求

组织应：

a) 实施并保持一个过程，用以识别、获取和评估与其产品和服务、活动和资源的连续性相关的、适用的法律和法规要求；

b) 确保在实施和保持其 BCMS时考虑这些适用的法律、法规以及经组织认同的其他要求；

c) 将这些信息形成文件并保持更新。

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：

a)4.1 涉及的外部和内部情况；

b)4.2 涉及的要求；

c) 其使命、目标以及内外部责任。

该范围应为可获得的成文信息。

4.3.2 业务连续性管理体系的范围

组织应：

a) 在考虑组织的地点、规模、性质和复杂性的情况下，确定组织中BCMS 覆盖的部分；

b) 识别包含在BCMS范围内的产品和服务。

在定义范围时，组织应记录并解释删减情况，任何删减应不影响根据业务影响分析或风险评估以及适用的法律或法规要求而确定的组织的业务连续性能力和责任。

4.4 业务连续性管理体系

组织应根据本文件的要求，建立、实施、保持并持续改进 BCMS,包括所需的过程以及过程间的相互作用。

5 领导力

5.1 领导力和承诺

最高管理者应通过以下方面证实其对 BCMS 的领导力和承诺：

a) 确保建立业务连续性方针和目标，并与组织的战略方向相一致；

b) 确保将BCMS要求融入组织的业务过程；