认 证 规 则

业务连续性管理体系认证规则

编　　号：ZXB-BCMS-01-2025

受 控 状 态：　受 控

版本	编修	审核	批准	编写/修订日期	发布日期
A/0	崔海军	张京梅	郑宇兵	20250722	20250724
A/0	崔海军	张京梅	郑宇兵	20250828	20250828

管理体系手册编制/修订履历

版本	修订内容	编写日期/修订日期	发布日期
A0	新编	20250722	20250724
A0	认证证书及认证标志的要求	20250828	20250828

目录

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；

c) 确保 BCMS 所需的资源是可获得的；
d) 就业务连续性的有效性和符合 BCMS 要求的重要性进行沟通；
e) 确保 BCMS 实现其预期结果；
f) 指导和支持人员为 BCMS 的有效性做出贡献；
g) 推动持续改进；
h) 支持其他相关管理角色展示其在职责领域内的领导力和承诺。

注：本文件中的“业务”可能被广义地理解为对组织存在的目的至关重要的活动。

5.2 方针

5.2.1 建立业务连续性方针

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设置提供框架；
c) 包括满足适用要求的承诺；
d) 包括持续改进 BCMS 的承诺。

5.2.2 沟通业务连续性方针

业务连续性方针应：
a) 为可获得的成文信息；
b) 在组织内进行传达；
c) 适当时，使相关方能够获得。

5.3 角色、职责和权限

最高管理者应确保组织相关角色的职责、权限得到分配、沟通。
最高管理者应分配职责和权限以：
a) 确保 BCMS 符合本文件的要求；
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

6.1.1 确定风险和机会

当进行 BCMS 策划时，组织应考量 4.1 提到的情况和 4.2 提到的要求，并确定需要应对的风险和机会以：
a) 确保 BCMS 能实现其预期结果；
b) 防止或减少不良影响；
c) 实现持续改进。

6.1.2 应对风险和机会

组织应策划：

a) 应对这些风险和机会的措施；

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) 评估措施的有效性(见 9.1)。

注：风险和机会与管理体系的有效性相关。与业务中断有关的风险在 8.2 中讨论。

6.2 业务连续性目标及其实现的策划

6.2.1 建立业务连续性目标

组织应针对相关职能、层次建立业务连续性目标。

业务连续性目标应：

a) 与业务连续性方针保持一致；

b) 可测量(如可行)；

c) 考虑适用的要求(见 4.1 和 4.2)；

d) 予以监视；

e) 予以沟通；

f) 适时更新。

组织应保留业务连续性目标相关的成文信息。

6.2.2 确定业务连续性目标

策划如何实现业务连续性目标时，组织应确定：

a) 要做什么；

b) 所需资源；

c) 由谁负责；

d) 何时完成；

e) 如何评价结果。

6.3 业务连续性管理体系变更的策划

当组织确定需要对 BCMS 进行变更时(包括第 10 章中确定的变更)，应对变更进行策划。

组织应考量：

a) 变更目的及其潜在结果；

b) BCMS 的完整性；

c) 资源的可获得性；

d) 职责和权限的分配或再分配。

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) 根据对业务连续性绩效的影响，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、培训或实践经验的基础上能够胜任；
c) 适当时，采取措施以获得必要的能力，并评价措施的有效性；
d) 保留适当的成文信息，作为人员能力的证据。

注：适用措施可能包括对在职人员进行培训、辅导或重新分配工作，或聘用、外包胜任的人员。

7.3 意识

组织应确保在其控制下的工作人员了解：
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绩效的益处；
c) 不符合 BCMS 要求的后果；
d) 他们在中断发生之前、期间和之后的角色和职责。

7.4 沟通

组织应确定与 BCMS 相关的内部和外部沟通，包括：
a) 沟通的内容；
b) 沟通的时间；
c) 沟通的对象；
d) 沟通的方式；
e) 沟通的执行人员。

7.5 成文信息

7.5.1 总则

组织的 BCMS 应包括：
a) 本文件要求的成文信息；
b) 由组织确定的为实现 BCMS 绩效而必需的成文信息。

注：对于不同组织，BCMS 成文信息的范围可以不同，取决于：
——组织的规模，活动、过程、产品和服务的类型，以及资源；
——过程及其相互作用的复杂程度；
——人员的能力。

7.5.2 创建和更新

在创建和更新成文信息时，组织应确保适当的：
a) 标识和说明（如标题、日期、作者或索引编号）；
b) 形式（如语言、软件版本、图表）和载体（如纸质的、电子的）；
c) 评审和批准，以保持适宜性和充分性。

7.5.3 成文信息的控制

7.5.3.1 应控制 BCMS 和本文件所要求的成文信息，以确保：
a) 在需要的场合和时机，均可获得并适用；
b) 予以妥善保护（如防止泄密、不当使用或缺失）。

7.5.3.2 为控制成文信息，适用时，组织应关注下列活动：

a) 分发、访问、检索和使用；

b) 存储和防护，包括保持可读性；

c) 更改控制（如版本控制）；

d) 保留和处置。

对于组织确定的策划和运行 BCMS 所必需的来自外部的成文信息，组织应进行适当识别，并予以控制。

注：对成文信息的访问可能意味着仅允许查阅，或允许查阅并授权修改。

8 运行

8.1 运行的策划和控制

为满足要求，并实施 6.1 中所确定的措施，组织应通过以下措施对所需的过程进行策划、实施和控制：

a) 建立过程准则；

b) 按照准则实施过程控制；

c) 为了确信过程按策划进行，在必要的范围内保留成文信息。

组织应控制策划的变更，评审非预期变更的后果，必要时，采取措施减轻负面影响。

组织应确保外包过程和供应链得到控制。

8.2 业务影响分析和风险评估

8.2.1 总则

组织应：

a) 实施并保持分析业务影响和评估中断风险的系统过程；

b) 在策划的时间间隔及当组织或其所处的环境发生重大变化时，对业务影响分析和风险评估进行评审。

注：由组织确定业务影响分析和风险评估的先后顺序。

8.2.2 业务影响分析

组织应使用该过程分析业务影响，以确定业务连续性优先级和要求。该过程应：

a) 定义与组织环境相关的影响类型和准则；

b) 识别支持提供产品和服务的活动；

c) 使用影响类型和标准来评估这些活动中断随着时间的推移造成的影响；

d) 识别不恢复活动令组织无法接受的时间范围；

注：该时间范围可称为“最长可容忍中断时间（MTPD）”。

e) 在 d）中确定的时间内设置优先级时间范围，以便在确定的最低可接受能力上恢复中断活动；

注：该时间范围可称为“恢复时间目标（RTO）”。

f) 运用业务影响分析来识别优先活动；

g) 确定支持优先活动所需的资源；

h) 确定包括合作伙伴和供应商在内的依赖关系，以及优先活动间的依赖关系。

8.2.3 风险评估

组织应实施并保持一个风险评估过程。

注：ISO 31000 阐述了该风险评估过程。

组织应：

a) 识别中断对于组织的优先活动及其所需资源所带来的风险；

b) 分析和评价已识别的风险；

c) 确定需要处置的风险。

注：本条款中的风险与业务活动中断有关。与管理体系有效性相关的风险和机会见 6.1。

8.3 业务连续性策略和解决方案

8.3.1 总则

基于业务影响分析和风险评估的输出，组织应识别和选择业务连续性策略，这些策略考虑了中断之前、期间和之后的可选项。业务连续性策略应包含一个或多个解决方案。

8.3.2 识别策略和解决方案

识别应基于策略和解决方案的程度，以：

a) 在确定的时间范围和约定的能力上，满足连续和恢复优先活动的要求；

b) 保护组织的优先活动；

c) 降低中断的可能性；

d) 缩短中断时间；

e) 限制中断对组织的产品和服务的影响；

f) 提供充足、可得的资源。

8.3.3 选择策略和解决方案

选择应基于策略和解决方案的程度，以：

a) 在确定的时间范围和约定的能力上，满足连续和恢复优先活动的要求；

b) 考虑组织可承担或不可承担的风险的数量和类型；

c) 考虑相应的成本和收益。

8.3.4 资源要求

组织应确定资源要求以实施所选择的业务连续性解决方案。涉及的资源类型应包括但不限于：

a) 人员；

b) 信息和数据；

c) 基础设施，如建筑物、工作场所或其他设施及相关公用设施；

d) 设备和消耗品；

e) 信息通信技术(ICT)系统；

f) 运输和物流；

g) 资金；

h) 合作方和供应商。

8.3.5 实施解决方案

组织应实施并保持选定的业务连续性解决方案，以便在需要时能启动这些解决方案。

8.4 业务连续性计划和程序

8.4.1 总则

组织应实施并保持响应机制以便于及时预警并与有关相关方进行沟通。响应机制应在中断期间提供计划和程序来管理组织。当需要时，应使用计划和程序来启动业务连续性解决方案。

注：业务连续性计划包括不同类型的程序。

组织应基于选择的策略和解决方案输出业务连续性计划和程序，并形成文件。

程序应：

a) 明确规定中断期间应立即采取的步骤；

b) 灵活应对中断期间不断变化的内部和外部环境；

c) 关注可能导致中断的事件的影响；

d) 通过实施适当的解决方案，将影响降到最小化；

e) 为其中的任务分配角色和职责。

8.4.2 事件响应机制

8.4.2.1 组织应实施和保持一个结构，确定一个或多个负责对中断进行响应的团队。

8.4.2.2 每个团队的角色和责任以及团队之间的关系应明确说明。

8.4.2.3 总体的，这些团队应具备以下能力：

a) 评估中断的性质和程度及其潜在影响；

b) 根据预先定义的阈值评估影响，以证明启动正式响应是合理的；

c) 启动适当的业务连续性响应；

d) 策划需要采取的行动；

e) 建立优先级（以生命安全为第一要务）；

f) 监视中断的影响以及组织的响应；

g) 启动业务连续性解决方案；

h) 与相关方、权力机构和媒体进行沟通。

8.4.2.4 每个团队应有：

a) 具有履行指定角色所需责任、权限和能力的人员和候补人员；

b) 指导其行为的成文程序（见 8.4.4），包括响应措施的启动、操作、协调和沟通。

8.4.3 预警和沟通

8.4.3.1 组织应文件化并保持程序，以：

a) 与有关相关方进行内部和外部沟通，包括沟通内容、沟通时间、沟通对象以及沟通方法；

注：组织可以文件化并保持组织如何以及在何种情况下与员工及其紧急联系人沟通的程序。

b) 对来自相关方的沟通进行接收、记录和响应，包括任何国家或区域风险预警系统或类似系统；

c) 确保中断期间沟通手段可用；

d) 促进与应急响应人员的有序沟通；

e) 对事件发生后组织的媒体响应提供详细信息，包括沟通策略；

f) 对中断事件、采取的措施以及做出的决策进行详细记录。

8.4.3.2 适当时，下列事项应被考虑和实施：

a) 向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；

b) 确保多个响应组织之间的适当协调和沟通。

预警和沟通程序作为8.5中所述组织演练方案的一部分，应进行演练。

8.4.4 业务连续性计划

8.4.4.1 组织应文件化并保持业务连续性计划和程序。业务连续性计划应提供指导和信息，以协助团队应对中断，并协助组织进行响应和恢复。

8.4.4.2 总体的，业务连续性计划应包含：

a) 团队将采取的措施的细节，以：

1) 在预定时间内使优先活动连续或恢复；

2) 监视中断的影响以及组织对中断的响应。

b) 关于预先定义的阈值和启动响应的过程；

c) 以预定的能力交付产品和服务的程序；

d) 管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) 防止进一步损失或优先活动无法执行；

3) 对环境的影响。

8.4.4.3 每个计划应包括：

a) 目的、范围和目标；

b) 执行计划的团队的角色和职责；

c) 执行解决方案的措施；

d) 启动(包括启动准则)、运行、协调和沟通团队行动所需的支持信息；

e) 内部和外部相互依赖关系；

f) 资源要求；

g) 报告要求；

h) 退出过程。

每个计划都应在需要的时间和地点可用。

8.4.5 恢复

组织应具有用以在中断期间和之后从所采用的临时措施中恢复并重新开始业务活动的成文过程。

8.5 演练规划

组织应实施并保持一套演练和测试规划，从而随着时间的推移验证其业务连续性策略和解决方案的有效性。

组织开展的演练和测试应：

a) 与其业务连续性目标一致；

b) 基于适当的、精心策划、具有明确的目标和目的的场景；

c) 培养那些在中断中发挥作用的人员的团队合作精神、能力、信心和知识；

d) 随着时间的推移，一起实施，审定其业务连续性策略和解决方案；

e) 形成正式的演练评估报告，包括结果、建议和实施改进的措施；
f) 在促进持续改进的情况下进行评审；
g) 按策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。

组织应根据其演练和测试的结果采取措施，以实施变更和改进。

8.6 业务连续性文件和能力评价

组织应：
a) 评价其业务影响分析、风险评估、策略、解决方案、计划和程序的适宜性、充分性和有效性；
b) 通过评审、分析、演练、测试、事后报告和绩效评价开展评价；
c) 对合作伙伴或供应商的业务连续性能力进行评价；
d) 评价是否符合适用的法律法规要求、行业最佳实践，以及是否符合其自身的业务连续性方针和目标；
e) 及时更新文件和程序。

评价应定期、事件发生或响应启动后以及发生重大变化时开展。

9 绩效评价

9.1 监视、测量、分析和评价

组织应确定：
a) 需要监视和测量的内容；
b) 监视、测量、分析和评价方法，适用时，确保得到有效的结果；
c) 何时以及何人进行监视和测量；
d) 何时以及何人对监视和测量结果进行分析和评价。

组织应保留适当的成文信息作为结果的证据。

组织应评价 BCMS 绩效和有效性。

9.2 内部审核

9.2.1 总则

组织应按照策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) 组织自身的业务连续性管理体系要求；
   2) 本文件的要求。
b) 得到有效的实施和保持。

9.2.2 审核方案

组织应：
a) 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，审核方案应考虑到所关注过程的重要性和以往审核的结果；
b) 规定每次审核的审核准则和范围；
c) 选择审核员并实施审核，确保审核过程的客观性和公正性；
d) 确保将审核结果报告给相关管理者；

e) 保留成文信息，作为实施审核方案以及审核结果的证据；
f) 确保及时采取任何必要的纠正措施，以消除发现的不符合及其原因；
g) 确保后续审核活动包括所采取的措施的验证和报告验证结果。

9.3 管理评审

9.3.1 总则

最高管理者应按照策划的时间间隔对组织的 BCMS 进行评审，以确保其持续的适宜性、充分性和有效性。

9.3.2 管理评审输入

管理评审应考虑以下内容：
a) 以往管理评审所采取措施的状态；
b) 与 BCMS 相关的内外部因素变化；
c) BCMS 绩效信息，包括以下趋势：
   1) 不符合和纠正措施；
   2) 监视和测量评价结果；
   3) 审核结果。
d) 相关方的反馈；
e) BCMS 调整的需要，包括方针和目标；
f) 组织中可用于提高 BCMS 绩效和有效性的程序和资源；
g) 业务影响分析和风险评估信息；
h) 业务连续性文档和能力评价的输出(见 8.6)；
i) 在以往的风险评估中未充分解决的风险或问题；
j) 从未遂和中断中吸取的教训和采取的行动；
k) 持续改进的机会。

9.3.3 管理评审输出

9.3.3.1 管理评审的输出应包括与持续改进机会相关的决定，以及为提高 BCMS 的效率和有效性而对 BCMS 进行变更的任何需求，包括以下方面：
a) BCMS 范围的变化；
b) 更新业务影响分析、风险评估、业务连续性策略和解决方案以及业务连续性计划；
c) 修改可能会影响 BCMS 内外部问题响应的程序和控制；
d) 如何衡量控制措施的有效性。

9.3.3.2 组织应保留成文信息，作为管理评审结果的证据。组织应：
a) 向相关方沟通管理评审的结果；
b) 针对结果采取适当的措施。

10 改进

10.1 不符合和纠正措施

10.1.1 组织应确定改进机会，并采取必要措施，以实现其 BCMS 的预期结果。

10.1.2 当出现不符合时，组织应：

a) 对不符合做出应对，并在适用时：

1) 采取措施以控制和纠正不符合；

2) 处置后果。

b) 通过下列活动，评价是否需要采取措施消除不符合的原因，以避免其再次发生或在其他场合发生：

1) 评审不符合；

2) 确定不符合的原因；

3) 确定是否存在或可能发生类似的不符合。

c) 实施需要的任何措施；

d) 评审所采取的任何纠正措施的有效性；

e) 必要时，变更 BCMS。

纠正措施应与不符合所产生的影响程度相适应。

10.1.3 组织应保留成文信息，以证明：

a) 不符合的性质以及任何所采取的后续措施；

b) 纠正措施的结果。

10.2 持续改进

组织应根据定性和定量测量，持续改进 BCMS 的适宜性、充分性和有效性。

组织应考虑分析和评价的结果以及管理评审的输出，以确定是否存在与业务或 BCMS 相关的需求或机会，这些需求或机会应作为持续改进的一部分加以应对。

注：组织可运用 BCMS 的过程来实现改进，例如领导力、策划和绩效评价。

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 22313 Societal security—Business continuity management systems—Guidance

[5] ISO 22316 Security and resilience—Organizational resilience—Principles and attributes

[6] ISO 28000 Specification for security management systems for the supply chain

[7] ISO 31000 Risk Management—Guidelines

[8] ISO/IEC 20000-1 Information Technology—Service Management—Part 1: Service management system requirements

[9] ISO/IEC 27001 Information technology—Security techniques—Information security management systems—Requirements

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

[11] ISO Guide 73 Risk management—Vocabulary

[12] ISO/TS 22317 Societal security—Business continuity management systems—Guidelines for business impact analysis(BIA)

[13] ISO/TS 22318 Societal security—Business continuity management systems—Guidelines for supply chain continuity

[14] ISO/TS 22330 Security and resilience—Business continuity management systems—Guidelines for people aspects of business continuity

[15] ISO/TS 22331 Security and resilience—Business continuity management systems—Guidelines for business continuity strategy

[16] ISO/IEC/TS 17021-6 Conformity assessment—Requirements for bodies providing audit and certification of management systems—Part 6: Competence requirements for auditing and certification of business continuity management systems

[17] IEC 31010 Risk management—Risk assessment techniques

ISO

22301

第二版
2019-10

安全性及恢复能力 —

业务连续性管理体系—要求

目录

引言

0. 1 总则

本文件规定了实施和维护业务连续性管理体系(BCMS)的结构和要求，以根据组织在业务中断后可能接受或不接受的影响的数量和类型来开展业务连续性

保持 BCMS 的结果由组织的法律、法规、组织和行业要求、产品和服务的提供、采用的过程、组织的规模和结构，以及相关方的要求所决定。

本标准规定了建立和保持一个有效的业务连续性管理体系（BCMS）的结构及要求。

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；

■一实施和保持过程，能力和响应结构以确保组织能免于中断；

■—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 包括以下关键部分：

a） 方针；

b） 职责明确的能够胜任的人员；

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） 持续改进；

d） 支持运行控制和能够进行绩效评估的文件化信息

0.2 实施业务连续性管理体系的益处

BCMS 的目的是准备、提供和保持控制和能力，为组织，做好准备，提供并保持控制，并有能力在中断期间管理其持续运行的整体能力。为了实现这一目标，组织应

a) 从业务的角度来：

1)支持公司的战略目标;

2)创造竞争的优势;

3) 维护和提高企业的声誉和信誉

4）有助于组织的恢复能力

b)从财务的角度来：

1)减少法律和金融风险;

2)降低中断的直接和间接成本;

c)从利益相关方的角度:

1)保护生命、财产和环境;

2)考虑利益相关方的期望;

3) 对组织具备成功的能力提供了信心;

d)从内部流程的角度:

1)提高网络中断时的有效运行能力;

2)证明组织主动并有效、高效地控制风险；

3)解决运行的脆弱性。

0.3 PDCA 循环

本文件应用 PLAN(建立)、Do(实施和运行)、CHECK(监督和评审)和 ACT(保持和改进)(PDCA)循环来实施、保持和持续改进组织的 BCMS 的有效性。

PDCA 模型的采用确保了与其他管理体系标准（如 ISO 9001，ISO 14001, ISO/ iec20000- 1, ISO/ iec27001 和 ISO 28000）的一致性，从而支持该标准与相关管理体系的实施和运行保持一致性并能够整合。

根据 PDCA 循环，第 4 至 10 条涵盖了以下部分。

——章节 4 介绍了建立适用于组织的 BCMS 环境所必需的要求，以及需求、要求和范围。

——章节 5 总结了 BCMS 中针对最高管理层角色的具体要求，以及领导层如何通过组织所声明的方针来阐述对组织的期望

——章节 6 阐述了建立 BCMS 总的战略目标和指导原则的要求

——章节 7 支持 BCMS 的运行，包括与建立能力和与相关方经常性/必要的沟——同时文件化，控制、保持和留存必须的文件化信息

——章节 8 定义了业务连续性的需求，决定了如何解决这些需求，并制定了程序以在业务中断期间管理组织

——章节 9 总结了在业务连续性绩效测量、BCMS 对本文件的符合性，及进行管理评审的必要要求

——章节 10 对 BCMS 不符合项进行识别并采取措施，并通过纠正措施进行持续改进。

0.5 本文件的内容

本文件符合 ISO 管理体系标准的要求。这些要求包括都采用了高层结构、相同的核心内容及有核心定义的通用的条款，旨在助于有多个 ISO 管理体系标准的用户的应用 。

本文件包含了可用于对组织建立 BCMS 和评估其符合性的要求。组织为证明符合本文件，可通过以下方式：

——自我鉴定或自我声明，或

——寻求组织利益相关方(如顾客)对其一致性的确认;或

——寻求外部组织对其自我声明的确认

——寻求外部组织对 BCMS 认证、注册

本文件第 1 章至第 3 章规定了本文件的范围、引用文件，以及本文件应用的术语和定义。第 4 章至 10 章是评估是否符合本文件的评定要求。

本文件中以下文字的意思是：

a) “应”表示必须性要求；

b) “宜”表示推荐性要求

c) “可以”表示允许

d) “能”表示可以或有能力

标记为“注”的信息用于对相关要求的理解或解释进行指导。第 3 章中使用的“条款注释”提供了对术语文本以外的补充附加信息，并可能包含与该术语有关的规定。

安全及恢复力——业务连续性管理体系—要求

1 范围

本标准为实施、保持和改进一个管理体系，以保护、减少中断事件发生的可能性，以及为中断事件的发生作好准备，在中断事件发生时予以响应并恢复。

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。

本标准适用于有如下期望的各种类型和规模的组织：

a） 实施、保持和改进 BCMS；

b） 确保能符合声明的业务连续性方针；

c） 需要在中断过程中按可接受的、预先确定的能力来持续的提供产品和服务

d） 通过有效应用贯行 BCMS，意求增强其恢复能力

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

本文提及的下述文件，其部分或全部内容适用于本文件的要求。带有版本号的参考文献的，仅其引用版本适用于本文件。未注明版本日期的引用文件，其最新版本(包括修订)适用于本文件。

3 术语和定义

下列术语和定义适用于本文件。

基于本文件的目的，ISO 22300 中的术语和定义，以及以下内容适用于本文件。

ISO 和 IEC 对标准应用术语的数据库在以下地址:

— ISO 在线 浏览平台: https:// www .iso .org/ obp

— IEC Electropedia:t http:// www .electropedia .org/

注：以下术语和定义取代了 ISO 22300:2018 中的相应术语和定义.

3. 1

活动 activity

具有确定输出的一个或多个任务的集合。

[来源: ISO 22300:2018, 3.1,修订— 定义已被替换，示例已被取消.]3.2

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：内审由组织自身，或代表组织的外部组织来进行。

注 3：“审核证据”和“审核准则”定义见 ISO19011

注 4：审核的基本要素包括按程序来确定目标的符合性(3.7)，该确定过程要由与被审核对象职责无关的人员执行。

注 5：内部审核可能是基于管理评审和组织自身的其他目的，可作为组织的符合性声明的基础。独立性可以通过由与被审核活动责无关的人实施审核来体现(3.1)。外部审核包括第二方和第三方审核。第二方审核由与组织有利害关系的组织(如顾客，或代表其顾客的组织进行。第三方审核是由外部独立的审核机构进行的，例如提供符合性认证/注册的机构或政府机构

注 6:本定义是 ISO 管理体系标准高级结构的通用术语和核心定义之一。其最初的定义已被修改，增加了注 4 和注 5。

3.3 .

业务连续性 business continuity

在中断过程中，组织在可接受的时间框架内，以预先确定的能力持续提供产品或服务的能力。

[来自 ISO 22300:2018, 3.24, 修订 ——该定义已被修改]

3.4

业务连续性策划 business continuity plan

文件化的信息(3.11)，指导组织(3.21)应对中断(3.10)，重启、还原和修复产品和服务的提供活动 (3.27)，以符合其业务连续性(3.3)目标(3.20)

[来源: ISO 22300:2018, 3.27,修订 — 定义已被替换，注 1 已被删除]

3.5

业务影响分析过程 business impact analysis

对中断事件(3.10)随时间推移对组织（3.21）的影响(3.13)的分析过程(3.26)，分析中断随时间推移对组织的影响

注 1:其输入是业务连续性(3.3)要求(3.28)的陈述和判断理由。

[来源:ISO 223:00:2018, 3.29，修改-该定义已被替换，已添加注 1。]

3.6

能力 competence

应用知识和技能以达成预期结果的能力

注 1：本定义为组成 ISO 管理体系标准高层结构的常见术语和核心定义之一

3.7

符合 conformity

满足要求(3.28)

注 1：本定义为组成 ISO 管理体系标准高层结构的常见术语和核心定义之一

3.8

持续改进 continual improvement

提升绩效（3.23）的循复活动（3.1）

注 1：本定义为组成 ISO 管理体系标准高层结构的常见术语和核心定义之一

3.9

纠正措施 corrective action

采取措施消除不符合的原因(3.19)，防止不符合的再次发生

注 1：本定义为组成 ISO 管理体系标准高层结构的常见术语和核心定义之一

3.10

中断 disruption

预期或非预期事件(3.14)，引发非策划的、负面的偏离，即偏离组织的(3.21)依据目标(3.20)既定的对产品和服务的交付(3.27) 的期望

[来源:ISO 223:00:2018, 3.70，修改-该定义已被替换。]

3.11

文件化信息 documented information

组织(3.21)需要控制和保持的信息及其媒介

注 1:文档信息可以是任何格式、媒体和来源。

注 2:文件化信息可与以下事项相关:

-管理体系(3.16),包括相关流程(3.26);

-为组织运行而编制的资料(文件);

-取得成果的证据(记录)。

注 3:本定义为组成 ISO 管理体系标准高层结构的常见术语和核心定义之一

3.12

有效性 effectiveness

所策划的活动(3.1)得以实现,所策划结果得以达成的程度

注 1: 本定义为组成 ISO 管理体系标准高层结构的常见术语和核心定义之一。

3.13

影响 impact

中断（3.10）产生的结果对目标（3.20）的影响

3.14

事件 incident

可能或将导致中断（3.10）、损失、紧急状况或危机的情况。

[来自 ISO 223:00:2018, 3.111,修改-该定义已被替换]

3.15

相关方(首选的定义) interested party (preferred term)

利益相关者（公认的术语）

能够影响、受组织影响,或认为受组织决策或活动（3.1）影响的个人或组织(3.21)

3.16

管理体系 management system

组织内一组相互关联或相互作用的要素,用以制定方针(3.24)、目标(3.20)和过程(3.26)以实现这些目标

注 1:一个管理体系可以关注一类活动或多类活动。

注 2:系统要素包括组织的结构、岗位和职责、策划及运行。

注 3:管理体系的范围可以包括整个组织、组织内特定和确定的职能部门、组织内特定和确定的部分,或跨越多个组织的一个或多个职能。

3.17

测量 measurement

确定数值的过程

注 1: 本定义为组成 ISO 管理体系标准高层结构的常见术语和核心定义之一。

3.18

监视 monitoring

对体系、过程(3.26)或活动的状态进行确定的活动

注 1: 确定状态可能是需要检查、监督和密切观察。

注 2:本定义为组成 ISO 管理体系标准高层结构的常见术语和核心定义之一。

3.19

不符合 nonconformity

不满足要求 (3.28)

注 1:本定义为组成 ISO 管理体系标准高层结构的常见术语和核心定义之一。

3.20

目标 objective

达到的结果

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、业务连续性(3.3)目标，或使用其他意义相近的词语表达（如，aim, goal, or target）

注 4:在业务连续性管理体系的背景下(3.16)，业务连续性管理体系目标由组织设定(3.21)，与业务连续性方针(3.24)相一致，以达到特定的结果。

注 5：本定义为组成 ISO 管理体系标准高层结构的常见术语和核心定义之一。

3.21

组织 organization

具有自身职责、权限和关系以实现其目标(3.20) 的一个人或一组人员

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、authority、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。

注 3：本定义为组成 ISO 管理体系标准高层结构的常见术语和核心定义之一。原定义已被修改，增加了注 2

3.22

外包 outsource

把组织（3.21）的部分职能或过程（3.26）安排给外部组织。

注 1：虽然外包的职能和过程属于管理体系（3.16）的范围，但外部组织则在此范围之外。

注 2：本定义为组成 ISO 管理体系标准高层结构的常见术语和核心定义之一。

3.23

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。

注 3：本定义为组成 ISO 管理体系标准高层结构的常见术语和核心定义之一。

3.24

方针 policy

由组织（3.21）最高管理者（3.31）正式发布的意图和方向。

注 1：本定义为组成 ISO 管理体系标准高层结构的常见术语和核心定义之一。

3.25

优先活动 prioritized activity

事件发生后为了减轻影响必须优先执行的活动。

为避免在中断（3.10）期间对业务造成不可接受的影响（3.13）而给予的紧急活动(3.1)

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。

注 1：本定义为组成 ISO 管理体系标准高层结构的常见术语和核心定义之一。

3.27

产品和服务 product and service

组织（3.21）提供给相关方（3.15）的输出或外包

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。

［来源： ISO 22300:2018, 3.181，修改 —术语“产品和服务”替代了“产品或服务” 定义已被取代］

3.28

要求 requirement

明示的、通常隐含的或必须覆行的需求或期望

注 1：“通常隐含的”意思是对组织及相关方来说，对这种需求和期望的考虑是必然的，组织经常或惯例性的要考虑此内容。

注 2：特定要求是指规定的要求。如在文件化信息里规定的内容

注 3：本定义为组成 ISO 管理体系标准高层结构的常见术语和核心定义之一。

3.29

资源 resource

组织(3.21)为了运行和实现其目标(3.20)在需要时必须能够使用的所有资产(包括厂房和设备)、人员、知识、技术、房屋、用品和信息(无论电子化与否)

3.30

风险 risk

对目标(3.20)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：不确定性是指对某事件、事件结果、发生的可能性完全或部分地缺乏了解或认识的情况。

注 3：风险的特性是通常与事件（见 ISO/IEC 指南 73 中的定义 ）和后果（见 ISO/IEC 指南 73 中的定义），或它们的组合相关。

注 4：:风险通常被表述为事件的后果（包括其变化情况）及发生的可能性的组合（见 ISO/IEC 指南 73 中的定义）

注 5:本定义为组成 ISO 管理体系标准高层结构的常见术语和核心定义之一。原定义已被修改,增加了“对目标的(on objectives)”以与 ISO31000 一致

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：最高管理者有权力在组织内进行授权,并提供资源（3.29）。

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。

注 3：本定义为组成 ISO 管理体系标准高层结构的常见术语和核心定义之一。

4. 组织环境

4.1 理解组织及其环境

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。

注：这些情况将受到该组织的总体目标、其产品和服务以及它可承担或不可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

在建立业务连续性管理体系时,组织应确定：

a）与 BCMS 有关的相关方；

b）这些相关方的有关要求。

4.2.2 法律和法规要求

组织应：

a）实施和保持一个程序用以识别、利用和评估与其产品和服务、活动和资源的连续性要求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、法规和其他要求；

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）在 4.1 中涉及的外部和内部因素；

b）在 4.2 中涉及的要求；

c）它的使命、目标以及内部和外部义务。

该范围应为可获得的存档信息。

4.3.2 业务连续性管理体系的范围

组织应：

a）在考虑到组织的地点、规模、性质和复杂性的情况下，确定组织中被包含在 BCMS 范围内的部分；

b）确定要包含在 BCMS 中的产品和服务。

在定义范围时,组织应将删减理由形成文件。它们不应影响组织提供业务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

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：

a）确保制定了业务连续性方针和业务连续性目标，并确保

方针和目标与组织的战略方向是一致的；

b）确保业务连续性管理体系的要求纳入组织的业务过程 中；

c）确保业务连续性管理体系所需的资源可用；

d）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；

e）确保业务连续性管理体系达到预期结果；

f）指导和支持员工为提高业务连续性管理体系的有效性作贡献；

g）推动持续改进；

h）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: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功。

5.2 方针

5.2.1 建立业务连续性方针

最高管理者应建立业务连续性方针，以便：

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。

5.2.2 沟通业务连续性方针

业务连续性方针应：

a）为可获得的存档信息；

b）在组织内部传达；

c）适当时使相关方能够获得。

5.3 角色、职责和权力

最高管理者应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 BCMS 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

6.1.1 确定风险和机会

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 BCMS 能达到预期结果；

b)防止或减少不良影响；

c)实现持续改进。

6.1.2 应对风险和机会

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)。

注：风险和机会与管理体系的有效性有关。与业务中断有关的风险在 8.2 中讨论。

6.2 业务连续性目标和实现计划

6.2.1 制定业务连续性目标

组织应在相关职能和层次上制定业务连续性目标。

业务连续性目标应：

a）与业务连续性方针保持一致；

b）是可测量的（如可行）；

c）考虑适用的要求（见 4.1 和 4.2）；

d）进行监视；

e）进行传达；

f）进行适当的更新。

组织应保留与业务连续性目标有关的存档信息。

6.2.2 确定业务连续性目标

在规划如何实现业务连续性目标时，组织应确定：

a）要做什么；

b）需要什么资源；

c）谁将负责；
d）什么时候完成；
e）怎样评估结果。

6.3 规划业务连续性管理体系的变更

当组织确定需要对 BCMS 进行变更时，包括那些在第 10 章确定的变更，应有计划的进行变更。
组织应考虑：
a）变更的目的及其潜在后果；
b）BCMS 的完整性；
c）资源的可得性；
d）责任和权利的分配或重新分配。

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)根据业务连续性绩效影响,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)在发生中断之前、期间和之后，各自的角色和责任。

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；
d)如何沟通；
e)谁来沟通。

7.5 存档信息

7.5.1 总则

组织的 BCMS 应包括：

a) 本标准所要求的存档信息；

b) 由组织确定的为实现 BCMS 绩效而必需的存档信息。

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)和介质(例如纸质、电子的)；

c)对适宜性和充分性的评审和审批。

7.5.3 存档信息的管理

7.5.3.1 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)。

7.5.3.2 适当时,组织应采取以下措施对存档信息进行控制：

a)分发、访问、获取和使用；

b)存储和保存,包括保护可读性；

c)变更控制(例如版本控制)；

d)保留和处置。

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。

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和供应链得到控制。

8.2 业务影响分析和风险评估

8.2.1 总则

组织应：

a) 实施和保持系统的流程，以分析业务影响和评估中断的风险；

b) 在计划的时间间隔，当组织或其所处的环境发生重大变化时，评审业务影响分析和风险评估。

注:组织决定业务影响分析和风险评估的执行顺序。

8.2.2 业务影响分析

组织应使用业务影响分析的过程来确定业务连续性的优先级和要求。业务影响分析过程应：

a) 定义与组织环境相关的影响类型和准则；

b) 识别支持产品和服务交付的活动；

c) 使用影响类型和准则来评估这些活动中断后随时间推移的影响；

d) 确定组织无法接受不能恢复活动的影响的时间；

注 1 此时间可称为“最长可容忍中断时间（MTPD）”。

e) 在 d）所确定的时间内，设定恢复中断活动的优先时间，使其达到规定的最低可接受能力。

注 2 此时间可称为“恢复时间目标（RTO）”

f) 利用业务影响分析确定优先活动；

g) 确定需要哪些资源来支持优先活动；

h) 确定优先活动的相互依赖关系，确定与合作方和供应商的依赖关系。

8.2.3 风脸评估

组织应实施并保持一个风险评估过程。

注：ISO31000 标准阐述了风险评估过程。

组织应：

a) 识别中断对于组织的优先活动及其所需资源所带来的风险；

b) 分析和评估已识别的风险；

c) 确定哪些风险需要处理。

注：本小节中的风险与业务活动的中断有关。与管理体系有效性有关的风险和机会在 6.1 中讨论。

8.3 业务连续性策略和解决方案

8.3.1 总则

根据业务影响分析和风险评估的输出结果，组织应识别和选择业务连续性策略，这些策略考虑了中断之前、期间和之后的可选项。业务连续性策略应由一个或多个解决方案组成。

8.3.2 确定策略和解决方案

应根据下列策略和解决方案的程度来确定：

a) 满足在确定的时间和约定的能力范围内继续和恢复优先活动的要求；

b) 保护组织的优先活动；

c) 减少中断的可能性；

d) 缩短中断时间；

e) 限制中断对组织产品和服务的影响；

f) 提供充足的有效资源。

8.3.3 选择策略和解决方案

选择应基于策略和解决方案在多大程度上：

a) 满足在确定的时间和约定的能力范围内继续和恢复优先活动

的要求；

b) 考虑组织可承担或不可承担的风险的数量和类型；

c) 考虑相关的成本和效益。

8.3.4 资源要求

组织应为执行所选择的业务连续性解决方案设置资源要求。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、工作场所或其他设施及相关公用设施等基础设施；

d) 设备和耗材；

e) 信息通信技术系统；

f) 交通和物流；

g) 资金；

h) 合作方和供应商。

8.3.5 解决方案的实施

组织应实施和保持选定的业务连续性解决方案，以便在需要时能启动这些解决方案。

8.4 业务连续性计划和程序

8.4.1 总则

组织应实施并保持一个响应构架，使其能够及时向相关方发出警告并进行沟通。在中断期间，它应提供计划和程序来管理组织。当需要时，应使用计划和程序来启动业务连续性解决方案。

注：业务连续性计划包含不同类型的程序。

根据选定的策略和解决方案的输出成果，组织应确定并将业务连续性计划和程序形成文件。

程序应：

a) 针对业务中断期间需要采取的紧急步骤进行详细规定；

b) 灵活地应对不断变化的中断事件的内部和外部环境；

c) 关注可能导致中断的事态影响；

d) 通过实施适当的解决方案有效地将影响最小化；

e） 为其中的任务分配角色和责任。

8.4.2 响应机制

8.4.2.1 组织应实施和保持一个机制，确定一个或多个团队负责响应中断。

8.4.2.2 每个团队的角色和责任以及团队之间的关系应明确说明。

8.4.2.3 这些团队应共同具备以下能力：

a) 评估中断事件的性质和范围以及潜在影响；

b) 根据预先确定的阀值评估影响，以证明启动正式响应是合理的；

c) 启动适当的业务连续性响应；

d) 规划需要采取的措施；

e) 确定优先级（采取人身安全第一优先的原则）；

f) 监视中断的影响和组织的响应；

g) 启动业务连续性解决方案；

h) 与相关方、权力机构和媒体进行沟通。

8.4.2.4 每个团队应：

a) 确定具有履行指定角色的必要责任、权力和权限的人员及其候补人员；

b) 指导其行动的形成文件的程序（见 8.4.4） 包括响应的启动、操作、协调和沟通。

8.4.3 预警和沟通

8.4.3.1 该组织应记录和保持下列程序：

a) 与相关方进行内部和外部沟通，包括沟通内容、时间、与谁沟通以及如何沟通；

注：组织可以记录和维护程序，说明组织如何和在何种情况下与员工及其紧急联系人沟通。

b) 接收、存档和相应相关方的反馈，包括任何国家或地区风险咨询系统或同等机构的信息；

c) 确保在中断期间沟通手段的可用；

d) 为同应急相应人员进行有序的沟通提供便利；

e) 该提供组织在事件发生后的媒体相应细节，包括沟通策略；

f) 记录中断的细节、采取的措施和所做的决定。

8.4.3.2 适当时，下列事项应被考虑和实施：

a) 向将要受到正在发生或者即将发生的中断潜在影响的相关方进行预警；

b) 确保多个响应组织之间的适当协调和沟通。

作为 8.5 中所述组织演练方案的一部分，预警和沟通程序应进行演练。

8.4.4 业务连续性计划

8.4.4.1 组织应记录和保持业务连续性计划和程序。业务连续性计划应提供指导和信息，以协助各团队应对中断，并协助组织作出反应和恢复。

8.4.4.2 业务连续性计划应包括：

a) 团队将采取的行动的细节，以便：

1)在预定时间里继续或恢复优先活动；

2)监视中断的影响和组织对中断的响应；

b) 关于预先定义的阀值和启动响应的过程；

c) 以约定的能力交付产品和服务的程序；

d) 处理中断所造成的直接后果的详细说明，要考虑到：

1)个人福利；

2)防止进一步损失或优先活动无法执行；

3)对环境的影响。

8.4.4.3 每个计划应包括：

a) 目的、范围和目标；

b) 执行计划的团队的角色和职责；

c) 采取行动落实解决方案；

d) 启动（包括启动准则）、操作、协调和沟通团队行动所需的支持信息；

e) 内部和外部的依赖关系；

f) 资源的要求；

g) 汇报的要求；

h) 退出的过程。

每个计划应在需要的时间和地点是可用和可得的。

8.4.5 恢复

组织应有用以在中断期间和之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（processes）。

8.5 演练方案

组织应实施和保持一份演练和测试方案，以随着时间的推移验证其业务连续性策略和解决方案的有效性。

组织进行的演练和测试应：

a）与其业务连续性目标保持一致；

b）基于适当的，有周密计划以及明确目的和目标的场景；

c）培养团队合作精神、能力、信心和知识，为那些需要在中断有关的情况下发挥作用的人服务；

d）持续实施，以验证其业务连续性策略和解决方案；

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。

组织应根据其演练和测试的结果采取行动，以实施变更和改进。

8.6 业务连续性文件和能力评估

组织应：

a）评价其业务影响分析、风险评估、策略、解决方案、计划和程序的适宜性、充分性和有效性；

b）通过评审、分析、演练、测试、事件总结报告和绩效评估进行评价；

c）对相关合作方和供应商的业务连续性能力进行评估；

d）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；

e）及时更新文档和程序。

这些评估应在计划的时间间隔、事件或启动后以及发生重大变化时进行。

9 绩效评估

9.1 监视、测量、分析和评价

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）何时以及由何人进行监视和测量；

d）何时以及由何人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。

9.2 内部审核

9.2.1 总则

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。

9.2.2 审核方案

组织应：

a）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。

b）确定每次审核的审核准则和范围。

c）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。

d）确保审核结果被报告给相关管理者；

e）保留执行审核方案和审核结果的存档信息作为证据；

f）确保及时采取任何必要的纠正措施，以消除发现的不符合及其原因；

g）确保后续审核行动包括所采取的措施的验证和验证结果的报告。

9.3 管理评审

9.3.1 总则

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。

9.3.2 管理评审输入

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）相关方的反馈；
e）BCMS 变更的需要，包括方针和目标；
f）组织内可用于改善 BCMS 绩效和有效性的程序和资源；
g）来自业务影响分析和风险评估的信息；
h）业务连续性文件和能力评估的输出（见 8.6）；
i）在以往的风险评估中未充分处理的风险或问题；
j）从未遂事故和中断中吸取的教训和采取的行动；
k）持续改进的机会。

9.3.3 管理评审输出

9.3.3.1 管理审查的输出应包括与持续改进机会有关的决定，以及为提高业务连续性管理体系的效率和效力而对其进行任何更改的必要性，包括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任何为提高效率和有效性而需要对 BCMS 进行变更，并且还包括：

a)对 BCMS 范围的变化；
b）对业务影响分析、风险评估、业务连续性策略和解决方案、业务连续性计划的更新；
c）对用以响应可对 BCMS 产生影响的内部或外部问题的程序和控制措施的修改；
d）如何衡量控制措施的有效性。

9.3.3.2 组织应保留存档信息作为管理评审结果的证据。组织应：

a）向相关方传达管理评审的结果；
b）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

10.1.1 组织应确定改进的机会，并实施必要的措施，以实现其 BCMS 的预期结果。
10.1.2 当不符合发生时，组织应：

a）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。
b)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）评审不合符；
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；
c)实施需要的任何措施；
d)评审所采取的任何纠正措施的有效性；
e)必要时,对 BCMS 进行变更。

10.1.3 组织应保留下列存档信息作为证据：

a）不符合的性质和任何所采取的后续措施;

b）各项纠正措施的结果。

10.2 持续改进

组织应根据定性和定量措施，持续改进 BCMS 的适宜性、充分性和有效性。

组织应考虑分析和评价的结果以及管理评审的输出，以确定是否存在与业务或 BCMS 有关的需求或机会，并作为持续改进的一部分加以处理。

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/TS 17021-6, Conformity assessment — Requirements for bodies providing audit and certification of management systems — Part 6: Competence requirements for auditing and certification of business continuity management systems

[5] ISO/IEC 20000-1, Information technology — Service management — Part 1: Service managementsystem requirements

[6] ISO 22313, 公共 — Business continuity management systems — Guidance

[7] ISO 22316, Security and resilience — Organizational resilience — Principles and attributes

[8] ISO/TS 22317, Societal security — Business continuity management systems — Guidelines for business impact analysis (BIA)

[9] ISO/TS 22318, Societal security — Business continuity management systems — Guidelines for supply chain continuity

[10] ISO/TS 22330, Security and resilience — Business continuity management systems — Guidelines for people aspects of business continuity

[11] ISO/TS 22331, Security and resilience — Business continuity management systems — Guidelines for business continuity strategy

[12] ISO/IEC 27001, Information technology — Security techniques — Information security management systems — Requirements

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

[14] ISO 28000, Specification for security management systems for the supply chain

[15] ISO 31000, Risk management — Guidelines

[16] IEC 31010, Risk management — Risk assessment techniques

[17] ISO Guide 73, Risk management — Vocabulary1