ISO/ 22301:2019

INTERNATIONAL

ISO 22301

Second edition第二版

2019-10

Security and resilience —Business continuity management systems —Requirements

安全性和弹性—业务连续性管理系统—要求

Sécurité et résilience —Systèmes de management de la continuité d'activité—Exigences

Reference number

Reference number
参考编号
ISO 22301:2019(CN)

目 录

前 言

ISO（国际标准化组织）是国家标准机构（ISO成员机构）的全球联合会。制定国际标准的工作通常是通过ISO技术委员会来进行的。对建立了技术委员会的主题感兴趣的每个成员机构均有权代表该委员会。与ISO联络的政府和非政府国际组织也参加了这项工作。在电子技术标准化的所有问题上，ISO与国际电子技术委员会（IEC）紧密合作。

ISO / IEC指令第1部分中描述了用于开发本文档的过程以及打算进一步维护的过程。特别是，应注意不同类型的ISO文档所需的不同批准标准。本文档是根据ISO / IEC指令第2部分的编辑规则起草的（请参阅www.iso.org/directives）。

请注意，本文档的某些内容可能是专利权的主题。ISO对识别任何或所有此类专利权概不负责。在文档开发过程中确定的任何专利权的详细信息将在“简介”和/或ISO收到的专利声明清单中（请参见www.iso.org/patents）。

本文档中使用的任何商标名称都是为了方便用户而提供的信息，并不构成背书。

有关标准的自愿性质的解释，与合格评定有关的ISO特定术语和表达的含义，以及有关ISO在贸易技术壁垒（TBT）中遵守世界贸易组织（WTO）原则的信息，请访问www .iso.org / iso / foreword.html。

该文件由技术委员会ISO / TC 292，安全性和弹性编写。

此第二版取消并替代了经过技术修订的第一版（ISO 22301：2012）。与上一版本相比的主要变化如下：

? • -自2012年起已采用ISO对管理体系标准的要求；

? • —要求已明确，未添加新要求；

? • –现在，特定学科的业务连续性要求几乎完全在第8条之内；

? • — 第8条进行了重组，以更清晰地理解关键要求；

? • -修改了一些特定领域的业务连续性术语，以提高清晰度并反映当前的想法。

对本文档的任何反馈或问题应直接发送给用户的国家标准机构。这些机构的完整列表可以在www.iso.org/members.html上找到。

内容介绍

0.1总则

本文档指定了实施和维护业务连续性管理系统（BCMS）的结构和要求，该系统可以开发适合于组织在中断后可能会或可能不会接受的影响的数量和类型的业务连续性。

维持BCMS的结果取决于组织的法律，法规，组织和行业要求，提供的产品和服务，采用的流程，组织的规模和结构以及相关方的要求。

BCMS强调以下方面的重要性：

—了解组织的需求以及建立业务连续性方针和目标的必要性；

—运营和维护流程，能力和响应结构，以确保组织能够在中断中生存下来；

—监视和审查BCMS的绩效和有效性；

-基于定性和定量措施的持续改进。

与其他任何管理系统一样，BCMS包括以下组件：

a）方针；

b）具有明确职责的主管人员；

c）与以下方面有关的管理过程：

1）方针；

2）计划；

3）实施与运作；

4）绩效考核；

5）管理评审；

6）持续改进；

d）支持运营控制并进行绩效评估的文件化信息。

0.2业务连续性管理系统的好处

BCMS的目的是准备，提供和维护控制和能力，以管理组织在中断期间继续运行的整体能力。为了实现这一目标，该组织是：

a）从业务角度：

1）支持其战略目标；

2）创造竞争优势；

3）保护和提高其声誉和信誉；

4）促进组织的应变能力；

b）从财务角度：

1）减少法律和财务风险；

2）减少中断的直接和间接成本；

c）从有关方面的角度：

1）保护生命，财产和环境；

2）考虑有关方面的期望；

3）对组织的成能力力充满信心；

d）从内部流程的角度：

1）提高其在中断期间保持有效的能力；

2）展示出对风险的积极主动控制；

3）解决运作漏洞。

0.3计划**-**执行**-**检查**-**执行（**PDCA**）循环

本文档应用计划（建立），执行（执行和运作），检查（监视和审查）和法案（维护和改进）（PDCA）周期来实施，维护和不断提高组织BCMS的有效性。

这样可确保与其他管理系统标准（例如ISO 9001，ISO 14001，ISO / IEC 20000-1，ISO / IEC 27001和ISO 28000）保持一定程度的一致性，从而支持与相关管理系统的一致且集成的实施和运作。

根据PDCA周期，第4至第10条涵盖以下组成部分。

— 第4条介绍了建立适用于该组织的BCMS上下文所必需的要求，以及需求，要求和范围。

— 第5条总结了最高管理者在BCMS中的特定角色要求，以及领导层如何通过方针声明向组织表达其对组织的期望。

— 第6条描述了为整个BCMS建立战略目标和指导原则的要求。

— 条款7支持BCMS运作，该运作涉及与利益相关方反复/根据需要建立能力和沟通，同时记录，控制，维护和保留所需的书面信息。

— 第8条定义了业务连续性需求，确定了解决方法，并制定了在中断期间管理组织的程序。

— 第9条总结了衡量业务连续性绩效，BCMS与本文档的符合性以及进行管理评审所必需的要求。

— 第10条确定并采取纠正措施，以应对BCMS不合格和持续改进。

0.4文件的内容

本文档符合ISO对管理系统标准的要求。这些要求包括高级结构，相同的核心文本以及带有核心定义的通用术语，旨在使实施多种ISO管理系统标准的用户受益。

尽管本文档的要素可以与其他管理系统的要素保持一致或集成，但本文档不包括特定于其他管理系统的需求。

本文档包含组织可以用来实施BCMS和评估合格性的要求。希望证明符合本文档要求的组织可以通过以下方式做到这一点：

—做一个自决和自我声明; 要么

—寻求与组织有利益关系的各方（例如客户）确认其符合性；要么

—寻求组织外部的一方对其自我声明的确认；要么

—寻求外部组织对其BCMS的认证/注册。

本文档中的第1至3节列出了适用于本文档使用的范围，规范性参考以及术语和定义。第4至第10条包含了用于评估本文件符合性的要求。

在本文档中，使用以下语言形式：

a） “应”表示一项要求；

b） “应”表示一项建议；

c） “可以”表示允许；

d） “可以”表示可能性或能力。

标有“注意”的信息用于指导您理解或阐明相关要求。第3条中使用的“进入注释” 提供了补充术语数据的附加信息，并且可以包含有关术语使用的规定。

1范围

本文档规定了实施，维护和改进管理系统的要求，以防止，减少发生中断的可能性，对中断进行准备，做出响应并从中恢复。

本文档中指定的要求是通用的，旨在适用于所有组织或其部分，无论组织的类型，规模和性质如何。这些要求的应用范围取决于组织的运营环境和复杂性。

本文档适用于以下所有类型和规模的组织：

a）实施，维护和改进BCMS；

b）寻求确保符合规定的业务连续性方针；

c）在中断期间必须能够继续以可接受的预定容量交付产品和服务；

d）寻求通过有效应用BCMS来增强其弹性。

该文档可用于评估组织满足其自身业务连续性需求和义务的能力。

2规范性引用文件

本文中引用以下文件的方式，使其中的某些或全部内容构成本文件的要求。凡是注日期的引用文件，仅所引用的版本适用。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本标准。

• ISO 22300，安全性和弹性—词汇

3术语和定义

就本文档而言，适用ISO 22300及以下内容中的术语和定义。

ISO和IEC在以下地址维护用于标准化的术语数据库：

• — ISO在线浏览平台：可在https://www.iso.org/obp获得

• — IEC Electropedia：可在http://www.electropedia.org/获得

注意以下给出的术语和定义将取代ISO 22300：2018中给出的术语和定义。

3.1活动

具有定义的输出的一组一个或多个任务

[来源：ISO 22300：2018，3.1，已修改-定义已替换，示例已删除。]

3.2审核

系统的，独立的和有文件记录的过程 （3.26），用于获取审核证据并对其进行客观评估，以确定满足审核标准的程度

注释1：审核可以是内部审核（第一方）或外部审核（第二方或第三方），并且可以是组合审核（组合两个或多个学科）。

注释2：内部审核由组织 （3.21）本身或由外部方代表进行。

注释3： “审核证据”和“审核标准”在ISO 19011中定义。

注释4：审核的基本要素包括根据不负责审核对象的人员执行的程序确定对象的合格性 （3.7）。

注释5：内部审核可以用于管理评审和其他内部目的，并且可以构成组织符合性声明的基础。可以通过对所审核活动 （3.1）的责任免于承担责任来证明独立性。外部审核包括第二方和第三方审核。第三方审核是由与组织有利益关系的各方（例如客户）或由其他人代表他们进行的。第三方审核由外部的独立审核组织进行，例如提供合格证明/注册的组织或政府机构。

注释6：这构成了ISO管理体系标准高层结构的通用术语和核心定义之一。原始定义已通过在条目中添加注释4和5进行了修改。

3. 3业务连续性

一个的能力组织 （3.21） ，继续的传送的产品和服务 （3.27）在预定义的容量可接受的时间范围内一个期间中断 （3.10）

[来源：ISO 22300：2018，3.24，已修改-定义已被替换。]

3.4业务连续性计划

指导组织 （3.21）响应中断 （3.10）并恢复，恢复和恢复与其业务连续性 （3.3）目标 （3.20）相一致的产品和服务 的交付（3.27）的文件化信息 （3.11 ）

[来源：ISO 22300：2018，3.27，已修改-定义已被替换，条目注释1已被删除。]

3.5业务影响分析

分析中断 （3.10）对组织 （3.21）的影响 时间（3.13）的过程 （3.26 ）

注释1：结果是对业务连续性 （3.3）要求 （3.28）的陈述和理由。

[来源：ISO 22300：2018，3.29，已修改-定义已被替换，条目注释1已添加。]

3.6能力

应用知识和技能以达到预期结果的能力

注释1：这构成了ISO管理体系标准高层结构的通用术语和核心定义之一。

3.7一致性

满足要求 （3.28）

注释1：这构成了ISO管理体系标准高层结构的通用术语和核心定义之一。

3.8持续改进

经常性活动 （3.1）以提高绩效 （3.23）

注释1：这构成了ISO管理体系标准高层结构的通用术语和核心定义之一。

3.9纠正措施

消除不合格的原因 （3.19）并防止再次发生的措施

注释1：这构成了ISO管理体系标准高层结构的通用术语和核心定义之一。

3.10中断

根据组织的 目标 （3.21）（3.20）导致预期或预期的产品和服务 交付（3.27）发生计划外的负偏差的事件 （3.14），无论是预期的还是未预期的

[来源：ISO 22300：2018，3.70，已修改-定义已被替换。]

3.11文件化信息

组织 （3.21）要求控制和维护的信息及其所包含的媒体

注释1：记录的信息可以采用任何格式和媒体，并且可以来自任何来源。

注释2：记录的信息可以参考：

- -所述管理系统 （3.16） ，包括相关的处理 （3.26） ；
- —为组织运作而创建的信息（文档）；
- -取得成果的证据（记录）。

注释3：这构成了ISO管理体系标准高层结构的通用术语和核心定义之一。

3.12有效性

计划活动 （3.1）的实现程度和计划成果的实现程度 ISO/DIS 22301:2019(E)

注释1：这构成了ISO管理体系标准高层结构的通用术语和核心定义之一。

3.13 影响

影响目标 （3.20）的中断 （3.10）的结果

[来源：ISO 22300：2018，3.107，已修改-定义已被替换。]

3.14事件

可能会或可能导致中断 （3.10），损失，紧急情况或危机的事件

[来源：ISO 22300：2018，3.111，已修改-定义已被替换。]

3.15

利益相关方（优先条款）

利益相关者（允许的期限）

可能会影响决策或活动 （3.1）或受其影响的个人或组织 （3.21 ）

例：

客户，所有者，人员，提供者，银行家，监管者，工会，合作伙伴或社会，可能包括竞争对手或压力集团。

注释1：决策者可以是感兴趣的一方。

注2：受影响的社区和当地居民被视为感兴趣的团体。

注释3：这构成了ISO管理体系标准高层结构的通用术语和核心定义之一。通过添加示例以及注释1和2来修改原始定义。

3.16管理系统

组织 （3.21）的一组相互关联或相互作用的元素，以建立策略 （3.24）和目标 （3.20）和过程 （3.26）以实现这些目标

注释1：管理系统可以处理一个或多个学科。

注释2：系统元素包括组织的结构，角色和职责，计划和运营。

注释3：管理系统的范围可以包括整个组织，组织的特定和确定的能力，组织的特定和确定的部分，或一组组织中的一个或多个能力。

注释4：这是ISO管理体系标准高层结构的通用术语和核心定义之一。

3.17测量

过程 （3.26）确定一个值

注释1：这构成了ISO管理体系标准高层结构的通用术语和核心定义之一。

3.18监控

确定系统，过程 （3.26）或活动 （3.1）的状态

注释1：要确定状态，可能需要检查，监督或严格观察。

注释2：这构成了ISO管理体系标准高层结构的通用术语和核心定义之一。

3.19不合格

未满足要求 （3.28）

注释1：这构成了ISO管理体系标准高层结构的通用术语和核心定义之一。

3.20目的

要达到的结果

注释1：目标可以是战略，战术或运作上的。

注释2：目标可以涉及不同的学科（例如财务，健康和安全以及环境目标），并且可以在不同的级别应用（例如战略，组织范围，项目，产品和过程 （3.26））。

注释3：可以用其他方式表达目标，例如，作为预期结果，目的，运营标准，作为业务连续性（3.3）目标，或使用具有类似含义的其他词语（例如，目标，目标）。

注释4：在业务连续性管理系统 （3.16）中，组织 （3.21）根据业务连续性策略 （3.24）设置业务连续性目标，以实现特定的结果。

注释5：这构成了ISO管理体系标准高层结构的通用术语和核心定义之一。

3.21组织

具有职责、权限和关系以实现其目标 的能力的个人或一群人（3.20）

注释1：组织的概念包括但不限于独资，公司，公司，公司，企业，机构，合伙企业，慈善机构或机构，或其一部分或组合，无论是否成立，公共或私人的。

注释2：对于具有多个运作单位的组织，可以将一个运作单位定义为组织。

注释3：这构成了ISO管理体系标准高层结构的通用术语和核心定义之一。通过在条目中添加注释2来修改原始定义。

3.22外包

安排外部组织 （3.21）履行组织职能或流程 （3.26）的一部分

注释1：外部组织不在管理系统 （3.16）的范围内，尽管外包的能力或过程在该范围之内。

注释2：这构成了ISO管理体系标准高层结构的通用术语和核心定义之一。

3.23绩效

可测量的结果

注释1：绩效可能与定量或定性发现有关。

注释2：绩效可能与管理活动 （3.1），流程 （3.26），产品（包括服务），系统或组织 （3.21）有关。

注释3：这构成了ISO管理体系标准高层结构的通用术语和核心定义之一。

3.24方针

组织最高管理层 （3.31）正式表达的组织的 意图和方向（3.21 ）

注释1：这构成了ISO管理体系标准高层结构的通用术语和核心定义之一。

3.25优先活动

为了避免业务中断 （3.10）对业务造成不可接受的影响 （3.13）而给予紧迫性的活动 （3.1 ）

[来源：ISO 22300：2018，3.176，已修改-定义已被替换，条目注释1已被删除。]

3.26处理

一组相互关联或相互作用的活动 （3.1），将输入转化为输出

注释1：这构成了ISO管理体系标准高层结构的通用术语和核心定义之一。

3.27产品与服务

组织 （3.21）向相关方 （3.15）提供的输出或结果

例：

制成品，汽车保险，社区护理。

[来源：ISO 22300：2018，3.181，已修改-术语“产品和服务”已替换为“产品或服务”，并且定义也已替换。]

3.28需求

陈述的需求或期望，通常隐含或强制性

条目注释1： “一般隐含”是指隐含在考虑中的需求或期望对于组织 （3.21）和相关方 （3.15）是惯例或惯例。

注释2：规定的要求是已陈述的要求，例如在书面信息 （3.11）中。

注释3：这构成了ISO管理体系标准高层结构的通用术语和核心定义之一。

3.29资源

组织 （3.21）在需要时必须可使用的所有资产（包括工厂和设备），人员，技能，技术，场所以及供应和信息（无论是否为电子），以便运营和满足其要求物镜 （3.20）

[来源：ISO 22300：2018，3.193，已修改-定义已被替换。]

3.30风险

不确定性对目标的影响 （3.20）

注释1：影响是与预期的偏差-正或负。

注2：不确定性是指与事件，其后果或可能性有关的信息，了解或知识的缺乏状态，甚至是部分的。

注释3：风险的特征通常是参考潜在的“事件”（如ISO指南73所定义）和“后果”（如ISO指南73所定义），或两者结合。

注释4：风险通常用事件的后果（包括环境变化）和相关的发生可能性（如ISO指南73中定义）的组合表示。

注释5：这构成了ISO管理体系标准高层结构的通用术语和核心定义之一。对该定义进行了修改，以添加“目标”，以与ISO 31000保持一致。

3.31最高管理者

在最高级别指导和控制组织 （3.21）的个人或一群人

注释1：最高管理者有权在组织内委派权限并提供资源 （3.29）。

注释2：如果管理系统 （3.16）的范围仅涵盖组织的一部分，则最高管理者是指指导和控制组织的该部分的人员。

注释3：这构成了ISO管理体系标准高层结构的通用术语和核心定义之一。

4组织环境

4.1了解组织及其背景

组织应确定与其目的相关并影响其实现BCMS预期结果的能力的外部和内部问题。

注：这些问题将受到组织的总体目标，组织的产品和服务以及组织可能承担或可能不会承担的风险的数量和类型的影响。

4.2了解相关方的需求和期望

4.2.1总则

建立BCMS时，组织应确定：

a）与BCMS有关的利益相关方；

b）这些有关方面的相关要求。

4.2.2法律法规要求

组织应：

a）实施和维护一个过程，以识别，获取和评估与其产品和服务，活动和资源的连续性有关的适用法律和法规要求；

b）确保在实施和维护其BCMS时考虑到这些适用的法律，法规和其他要求；

c）记录此信息并保持最新。

4.3确定业务连续性管理系统的范围

4.3.1总则

组织应确定BCMS的范围和适用性以建立其范围。

在确定此范围时，组织应考虑：

a）4.1中提到的外部和内部问题；

b）4.2中提到的要求；

c）其使命，目标以及内部和外部义务。

该范围应作为文档信息提供。

4.3.2业务连续性管理系统的范围

组织应：

a）考虑到组织的位置，规模，性质和复杂性，确定要纳入BCMS的组织部分；

b）确定要包含在BCMS中的产品和服务。

在定义范围时，组织应记录并解释排除情况。它们不应影响组织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所确定的提供业务连续性的能力和责任。

4.4业务连续性管理系统

组织应根据本文件的要求建立，实施，维护和持续改进BCMS，包括所需的过程及其相互作用。

5领导能力

5.1领导和承诺

最高管理者应通过以下方式表现出对BCMS的领导和承诺：

a）确保制定业务连续性方针和业务连续性目标，并与组织的战略方向保持一致；

b）确保将BCMS要求集成到组织的业务流程中；

c）确保BCMS所需的资源可用；

d）传达有效业务连续性和符合BCMS要求的重要性；

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）促进持续改进；

h）支持其他相关的管理角色，以显示其在其职责范围内的领导能力和承诺。

注意：本文档中对“业务”的引用可以广义地解释为那些对于组织的生存目的至关重要的活动。

5.2方针

5.2.1建立业务连续性策略

最高管理者应制定业务连续性方针，以：

a）适合组织的目的；

b）提供设定业务连续性目标的框架；

c）包括满足适用要求的承诺；

d）包括对BCMS持续改进的承诺。

5.2.2传达业务连续性策略

业务连续性策略应：

a）可作为文件化信息提供；

b）在组织内部进行沟通；

c）适当时可供有关各方使用。

5.3角色，职责和权限

最高管理者应确保在组织内部分配和传达有关角色的职责和权限。

最高管理者应为以下方面分配职责和权限：

a）确保BCMS符合本文件的要求；

b）向最高管理层报告BCMS的绩效。

6规划

6.1应对风险和机遇的措施

6.1.1确定风险和机遇

在规划BCMS时，组织应考虑4.1中提到的问题和4.2中提到的要求，并确定需要解决的风险和机遇：

a）确保BCMS可以实现其预期结果；

b）预防或减少不良影响；

c）实现持续改进。

6.1.2应对风险和机遇

组织应计划：

a）应对这些风险和机遇的行动；

b）如何：

1）将动作整合并实施到其BCMS流程中（请参阅8.1）；

2）评估这些措施的有效性（参见9.1）。

注：风险和机会与管理系统的有效性有关。与业务中断有关的风险在8.2中解决。

6.2业务连续性目标和实现这些目标的计划

6.2.1建立业务连续性目标

组织应在相关职能和级别上建立业务连续性目标。

业务连续性目标应：

a）符合业务连续性方针；

b）是可衡量的（如果可行）；

c）考虑到适用的要求（见4.1和4.2）；

d）被监视；

e）被传达；

f）适当更新。

组织应保留有关业务连续性目标的书面信息。

6.2.2确定业务连续性目标

在计划如何实现业务连续性目标时，组织应确定：

a）将要做什么；

b）将需要哪些资源；

c）谁负责；

d）何时完成；

e）如何评估结果。

6.3规划业务连续性管理系统的变更

当组织确定需要变更BCMS（包括第10条中确定的变更）时，应以计划的方式进行变更。

组织应考虑：

a）变更的目的及其潜在后果；

b） BCMS的完整性；

c）资源的可用性；

d）职责和权限的分配或重新分配。

7支持

7.1资源

组织应确定并提供建立，实施，维护和持续改进BCMS所需的资源。

7.2能力

组织应：

a）确定影响其业务连续性表现的人员在其控制下从事工作的必要能力；

b）确保这些人在适当的教育，培训或经验的基础上胜任；

c）在适用的情况下，采取行动以获得必要的能力，并评估所采取行动的有效性；

d）保留适当的书面信息作为能力证明。

注：可采取的行动可包括，例如，向现有工作人员提供培训，指导或重新分配现有工作人员；或雇用或签约合格人员。

7.3意识

在组织控制下工作的人员应了解：

a）业务连续性方针；

b）它们对BCMS有效性的贡献，包括改善业务连续性绩效的好处；

c）不符合BCMS要求的含义；

d）他们在中断之前，之中和之后的角色和责任。

7.4沟通

组织应确定与BCMS有关的内部和外部通信，包括：

a）它将交流什么；

b）何时沟通；

c）与谁沟通；

d）如何沟通；

e）谁来沟通。

7.5文件信息

7.5.1总则

组织的BCMS应包括：

a）本文件要求的文件化信息；

b）组织确定为BCMS有效性所必需的文件化信息。

注意由于以下原因，一个BCMS的文档化信息范围可能因组织而异。

--组织的规模及其活动，过程，产品和服务以及资源的类型；

--流程及其相互作用的复杂性；

--人的能力。

7.5.2创建和更新

在创建和更新文档信息时，组织应确保适当：

a）标识和描述（例如标题，日期，作者或参考编号）；

b）格式（例如语言，软件版本，图形）和媒体（例如纸张，电子）；

c）审查和批准其适用性和适当性。

7.5.3文件信息的控制

7.5.3.1 BCMS和本文件要求的文件信息应受到控制，以确保：

a）在需要的地方和时间可用并且适合使用；

b）受到足够的保护（例如，避免机密性，使用不当或完整性受损）。

7.5.3.2 为了控制书面信息，组织应酌情开展以下活动：

a）分发，获取，检索和使用；

b）储存和保存，包括保持可读性；

c）变更控制（例如版本控制）；

d）保留和处置。

组织应确定适当的BCMS计划和运营所需的外部来源的书面信息，并加以控制。

注意访问可能意味着要决定是否仅允许查看文档信息，或者是有关查看和更改文档信息的权限。

8运作

8.1运作计划与控制

组织应通过以下方式计划，实施和控制满足要求和实施6.1中确定的措施所需的过程：

a）建立过程标准；

b）按照标准对过程进行控制；

c）保持必要的范围内的书面信息，以确保流程已按计划进行。

组织应控制计划的变更并审查意外变更的后果，并采取必要的措施以减轻不良影响。

组织应确保对外包过程和供应链进行控制。

8.2业务影响分析和风险评估

8.2.1总则

组织应：

a）实施并维护系统的流程，以分析业务影响并评估中断的风险；

b）在计划的时间间隔以及组织内部或运营环境发生重大变化时，审查业务影响分析和风险评估。

注意：组织确定进行业务影响分析和风险评估的顺序。

8.2.2业务影响分析

组织应使用该过程来分析业务影响，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标准；

b）确定支持产品和服务提供的活动；

c）使用影响类型和标准来评估由于这些活动的中断而造成的长期影响；

d）确定不恢复活动的影响对组织而言将不可接受的时间范围；

注1：该时间范围可以称为“最大容许中断时间（MTPD）”。

e）在d）所确定的时间内设定优先时间框架，以便以规定的最小可接受能力恢复中断的活动；

注2：该时间范围可以称为“恢复时间目标（RTO）”。

f）使用此分析来确定优先活动；

g）确定需要哪些资源来支持优先活动；

h）确定依赖关系，包括合作伙伴和供应商，以及优先活动的相互依赖关系。

8.2.3风险评估

组织应实施并维持风险评估过程。

注意：ISO 31000规定了风险评估过程。

组织应：

a）确定中断组织的优先活动及其所需资源的风险；

b）分析和评估已识别的风险；

c）确定哪些风险需要治疗。

注：本节中的风险与业务活动的中断有关。与管理体系有效性相关的风险和机遇在6.1中进行了阐述。

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，组织应确定并选择考虑中断之前，期间和之后的选择的业

务连续性策略。业务连续性策略应包括一个或多个解决方案。

8.3.2确定战略和解决方案

识别应基于策略和解决方案的程度：

a）满足在确定的时限和商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）减少干扰的可能性；

d）缩短中断时间；

e）限制中断对组织产品和服务的影响；

f）提供足够的资源。

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：

a）满足在确定的时限和商定的能力范围内继续和恢复优先活动的要求；

b）考虑组织可能或可能不承担的风险的数量和类型；

c）考虑相关的成本和收益。

8.3.4资源需求

组织应确定实施所选业务连续性解决方案的资源要求。考虑的资源类型应包括但不限于：

a）人；

b）信息和数据；

c）物理基础设施，例如建筑物，工作场所或其他设施以及相关的公用事业；

d）设备和消耗品；

e）信息和通信技术（ICT）系统；

f）运输和物流；

g）财务；

h）合作伙伴和供应商。

8.3.5解决方案的实施

组织应实施和维护选定的业务连续性解决方案，以便可以在需要时开启它们。

8.4业务连续性计划和程序

8.4.1总则

组织应实施和维护响应结构，以使及时警告并与有关各方进行沟通。它应提供计划和程序以在中断期间管理组织。当需要开启业务连续性解决方案时，应使用计划和程序。

注意有组成业务连续性计划的不同类型的过程。

组织应基于所选策略和解决方案的输出，识别并记录业务连续性计划和程序。

程序应：

a）具体说明中断期间要立即采取的步骤；

b）灵活地应对不断变化的内部和外部状况；

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有效地将影响最小化；

e）为其中的任务分配角色和职责。

8.4.2响应结构

8.4.2.1 组织应实施和维护一个结构，确定一个或多个负责应对干扰的团队。

8.4.2.2 应明确说明每个团队的角色和职责以及团队之间的关系。

8.4.2.3 团队应共同负责：

a）评估中断的性质和程度及其潜在影响；

b）根据预先确定的阈值评估其影响，这些阈值可证明采取正式应对措施是合理的；

c）开启适当的业务连续性响应；

d）计划需要采取的行动；

e）确定优先事项（以生命安全为第一优先事项）；

f）监视中断的影响和组织的响应；

g）开启业务连续性解决方案；

h）与有关的有关方面，当局和媒体进行沟通。

8.4.2.4 对于每个团队，应有：

a）确定的人员及其候补人员具有履行其指定职责所必需的责任，权限和能力；

b）形成文件以指导其行动的程序（参见8.4.4），包括用于响应的开启，运作，协调和传达的程序。

8.4.3警告和通讯

8.4.3.1 组织应记录和维护以下程序：

a）与有关利益相关方进行内部和外部沟通，包括与谁，何时，与谁以及如何进行沟通；

注：组织可以记录和维护有关组织如何与员工以及其紧急联系人进行通信的程序。

b）接收，记录和回应来自有关方面的通信，包括任何国家或地区的风险咨询系统或同等系统；

c）确保中断期间通信手段的可用性；

d）促进与应急人员的结构化沟通；

e）提供事件发生后组织的媒体响应的详细信息，包括沟通策略；

f）记录中断的详细信息，采取的措施和做出的决定。

8.4.3.2 在适用的情况下，还应考虑和实施以下内容：

a）提醒可能受到实际或即将发生的干扰影响的有关方面；

b）确保多个响应组织之间的适当协调和沟通。

警告和通讯程序应作为8.5中所述的组织实施计划的一部分进行实施。

8.4.4业务连续性计划

8.4.4.1 组织应形成文件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，以帮助团队响应中断并协助组织响应和恢复。

8.4.4.2 总体而言，业务连续性计划应包含：

a）团队将采取以下行动的详细信息：

1）在预定时间范围内继续或恢复优先活动；

2）监控中断的影响以及组织对中断的响应；

b）参考预定义的阈值和开启响应的过程；

c）能够以商定的能力交付产品和服务的程序；

d）应对中断的直接后果进行管理的细节，同时应适当考虑：

1）个人的福利；

2）防止优先活动进一步丢失或无法使用；

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）将执行计划的团队的角色和职责；

c）实施解决方案的行动；

d）开启（包括开启标准），运作，协调和传达团队行动所需的支持信息；

e）内部和外部相互依赖性；

f）资源需求；

g）报告要求；

h）站下来的过程。

每个计划应在需要的时间和地点可用并可用。

8.4.5恢复

组织应有形成文件的流程，以从中断期间和中断之后采取的临时措施中恢复和返回业务活动。

8.5演练计划

组织应实施并维护一项演练和测试计划，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。

组织应进行以下练习和测试：

a）与其业务连续性目标一致；

b）基于精心策划并有明确目的和目标的适当方案；

c）为那些与干扰有关的角色发展团队合作，能力，信心和知识；

d）随着时间的流逝，共同验证其业务连续性策略和解决方案；

e）制定正式的运动后报告，其中包含成果，建议和采取行动以实施改进措施；

f）在促进持续改进的背景下进行审查；

g）按计划的时间间隔执行，并且在组织内部或运营环境发生重大变化时执行。

组织应根据其执行和测试的结果采取行动，以实施更改和改进。

8.6业务连续性文档和能力评估

组织应：

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

b）通过审查、分析、演习、测试、事后报告和绩效评估进行评估；

c）对相关合作伙伴和供应商的业务连续绩效力进行评估；

d）评估是否符合适用的法律和法规要求，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。

这些评估应在事件或开启之后以及发生重大变化时按计划的间隔进行。

9绩效评估

9.1监控 测量 分析和评估

组织应确定：

a）需要监测和测量的内容；

b）为确保有效结果而进行的监测，测量，分析和评估方法；

c）何时和由谁进行监视和测量；

d）应在何时何地对监测和测量结果进行分析和评估。

组织应保留适当的书面信息作为结果的证据。

组织应评估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，以提供有关BCMS是否：

a）符合：

1）组织自身对其BCMS的要求；

2）本文件的要求；

b）得到有效实施和维护。

9.2.2审核计划

组织应：

a）计划，建立，实施和维护审核计划，包括频率，方法，职责，计划要求和报告，其中应考虑到相关过程的重要性以及先前审核的结果；

b）定义每次审核的审核标准和范围；

c）选择审核员并进行审核，以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人员；

e）保留文件化信息，作为审核计划和审核结果实施的证据；

f）确保及时采取必要的纠正措施，以消除发现的不合格及其原因；

g）确保后续审核措施包括对所采取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审查组织的BCMS，以确保其持续的适用性，充分性和有效性。

9.3.2管理评审输入

管理评审应包括以下方面的考虑：

a）先前管理评审所采取行动的状态；

b）与BCMS有关的外部和内部问题的变化；

c）有关BCMS绩效的信息，包括以下方面的趋势：

1）不合格和纠正措施；

2）监测测量评估结果；

3）审核结果；

d）有关方面的反馈；

e）需要更改BCMS，包括方针和目标；

f）组织中可用来提高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）业务连续性文档和能力评估的输出（请参阅8.6）；

i）先前任何风险评估中未充分解决的风险或问题；

j）因未遂事件和干扰而吸取的教训和采取的行动；

k）持续改进的机会。

9.3.3管理评审结果

9.3.3.1 管理评审的输出应包括与持续改进机会以及对BCMS进行任何更改以提高其效率和有效性的任何需要有关的决定，包括以下内容：

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）修改程序和控制措施，以应对可能影响BCMS的内部或外部问题；

d）如何衡量控制的有效性。

9.3.3.2 组织应保留文件化信息，作为管理评审结果的证据。它应：

a）将管理评审的结果传达给有关各方；

b）对那些结果采取适当的措施。

10改善

10.1不合格和纠正措施

10.1.1 组织应确定改进机会并采取必要措施以实现BCMS的预期结果。

10.1.2 发生不符合时，组织应：

a）对不符合项做出反应，并在适用情况下：

1）采取措施进行控制和更正；

2）处理后果；

b）通过以下方式评估采取行动消除不合格原因的必要性，以确保不发生不合格现象：

1）审查不符合项；

2）确定不合格的原因；

3）确定是否存在类似的不符合项或可能发生的不符合项；

c）采取任何必要的行动；

d）审查采取的任何纠正措施的有效性；

e）如有必要，对BCMS进行更改。

纠正措施应适合于所遇到的不合格的影响。

10.1.3 组织应保留文件化信息，以证明：

a）不合格的性质以及随后采取的任何措施；

b）任何纠正措施的结果。

10.2持续改进

组织应在定性和定量措施的基础上，不断提高BCMS的适用性，充分性和有效性。

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

注意组织可以使用BCMS的过程（例如领导力，计划和绩效评估）来实现改进。

参考书目 [1] ISO 9001，质量管理体系—要求

[2] ISO 14001，环境管理体系—要求和使用指南

[3] ISO 19011，审核管理系统准则

[4] ISO / IEC / TS 17021-6，合格评定—提供管理系统审核和认证的机构的要求—第*6*部分：业务连续性管理系统审核和认证的能力要求

[5] ISO / IEC 20000-1，信息技术—服务管理—第*1*部分：服务管理系统要求

[6] ISO 22313，社会安全性—业务连续性管理系统—指南

[7] ISO 22316，安全性和弹性-组织弹性-原理和属性

[8] ISO / TS 22317，社会安全性—业务连续性管理系统—业务影响分析（*BIA*）指南

[9] ISO / TS 22318，社会安全性—业务连续性管理系统—供应链连续性准则

[10] ISO / TS 22330，安全性和弹性—业务连续性管理系统—业务连续性的人员方面指南

[11] ISO / TS 22331，安全性和弹性—业务连续性管理系统—业务连续性策略准则

[12] ISO / IEC 27001，信息技术—安全技术—信息安全管理系统—要求

[13] ISO / IEC 27031，信息技术—安全技术—信息和通信技术为业务连续性做好准备的准则

[14] ISO 28000，供应链安全管理系统规范

[15] ISO 31000，风险管理-准则