ISO 22301-2019 中文版

Second edition

2019-10

业务连续性管理体系 要求

1、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。
可接受水平：可接受水平程度阈值：不同组织的“接受水平”不一样；最终的阈值是关于“时间”程度（RTO、RPO）；非时间量的间值需要转换为时间流转率；
连续交付产品能力：可测量指标：无间断运行时间；财务指标；产品数量；运营效率；产品流转周期；库存；流转率；
2、业务连续性计划 Business continuity Plan;BCP
--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、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。
RPO：是指业务系统所允许的灾难过程中的最大数据丢失量，用来衡量容灾系统的数据冗余备份能力。
4、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。
RTO：是指信息系统从灾难状态恢复到可运行状态所需的时间，用来衡量容灾系统的业务恢复能力。
5、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。
6、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。
7、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。
8、业务影响分析 Business impact analysis; BIA
分析活动和业务中断可能带来的影响的过程。
9、风险评估 Risk Assessment; RA
风险识别、风险分析和风险评价的整个过程。
10、事态：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”。
11、事件：可能或将导致中断、损失、紧急状况或危机的情况。

4. 组织环境

4.1 理解组织及其环境

组织应确定与其宗旨相关并影响其实现 BCMS 预期结果的能力的各种外部和内部因素。

--注：这些因素将受到组织的总体目标、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)这些相关方的相关要求。

4.2.2 法律和法规要求

组织应：

a)实施并保持一个过程，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适用的法律和法规要求；

b)确保在实施和保持 BCMS 时考虑到这些适用的法律、法规和其他要求；

c)这些信息应形成文件化，并保持更新。

4.3 确定管理体系范围

4.3.1 总则

组织应确定 BCMS 的边界和适用性，以确定其范围。

组织在确定范围时应考虑：

a)在 4.1 中提及的各种外部和内部因素；

b)在 4.2 中提及的相关方的要求；

c)组织的使命、总目标、内部和外部责任。

BCMS 范围应作为文件化信息，可获得。

4.3.2 BCMS 的范围

组织应：

a)考虑到组织的所处地理位置、规模、性质和复杂程度，确定将组织相关组成部分包纳入 BCMS 中；

b)识别包含在 BCMS 范围内的产品和服务；

在确定范围时，组织应将删减理由形成文件化并加以说明。任何删减应不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 业务连续性管理体系

组织应按照本标准的要求，建立、实施、保持和持续改进 BCMS，包括所需过程及其相互作用。

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相一致；

b)确保 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)沟通有效的业务连续性和符合 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 的有效性作出贡献；
g)推动持续改进；
h)支持其他相关管理者在其职责范围内展示其领导力和承诺。
注：本标准使用的“业务”一词可广义地理解为涉及组织存在目的的核心活动。

5.2 方针

5.2.1 建立业务连续性方针

最高管理者应制定业务连续性方针，业务连续性方针应：
a) 与组织的宗旨相适应；
b) 为建立业务连续性目标提供框架；
c) 包含满足适用要求的承诺；
d) 包含持续改进 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) 作为文件化信息可获取；
b) 在组织内得到沟通；
c) 适宜时，可为相关方所获取。

5.3 角色、职责和权限

最高管理者应该确保相关角色的职责和权限在组织内部得到分配和沟通。
最高管理者应分配职责和权限，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 应对风险和机遇的措施

6.1.1 确定风险和机遇

当策划 BCMS 时，组织应考虑到 4.1 所提及的因素和 4.2 所提及的要求，并确定需要应对的风险和机遇，以：
a) 确保 BCMS 能够实现其预期结果；
b) 预防或减少不利影响；
c) 实现持续改进。

6.1.2 应对风险和机遇

组织应策划：
a) 应对这些风险和机遇的措施；
b) 如何：
1)在 BCMS 过程中整合并实施这些措施（见 8.1）；
2) 评价这些措施的有效性（见 9.1）。
注：风险和机遇与管理体系的有效性有关。与业务中断相关的风险，在 8.2 中有相应说明。

6.2 业务连续性目标和实现策划

6.2.1 建立业务连续性目标

组织应针对相关职能和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) 适当时更新。
组织应保留有关业务连续性目标的文件化信息。

6.2.2 确定业务连续性目标

在策划如何实现其业务连续性目标时，组织应确定：
a）采取的措施；
b）需要的资源；
c）由谁负责；
d）何时完成；
e）如何评价结果。

6.3 变更的策划

当组织确定需要对 BCMS 进行变更时，包括那些在第 10 章中确定的变更，变更应按照所策划的方式实施。
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

组织应确定并提供所需的资源，以建立、实施、保持和持续改进 BCMS。

7.2 能力

组织应：
a) 确定在其控制下工作的人员所需具备的能力，这些人员从事的工作影响组织的业务连续性绩效；
b) 基于适当的教育、培训或经验，确保这些人员是胜任的；
c) 适用时，采取措施以获得所需的能力，并评价措施的有效性；
d) 保留适当的文件化信息，作为人员能力的证据。
注：适用措施可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

在组织控制下工作的人员应知晓：
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) 在发生中断之前、中断期间和中断之后，他们各自承担的角色和职责。

7.4 沟通

组织应确定与
a) 沟通什么；
b) 何时沟通；
c) 与谁沟通；
d) 如何沟通；
e) 谁来沟通。

7.5 文件化信息

7.5.1 总则

组织的 BCMS 应包括：

a) 本标准所要求的文件化信息；

b) 组织所确定的、为确保 BCMS 绩效所需的文件化信息。

注：BCMS 的文件化信息程度可以因组织不同而有所差异，则取决于：

a) 组织的规模及其活动、过程、产品、服务和资源的类型；

b) 过程及其相互作用的复杂程度；

c) 人员的能力。

7.5.2 创建和更新

在创建和更新形成文件的信息时，组织应确保适当的：

a)标识和说明（如：标题、日期、作者、索引编号等）；

b)格式（如：语言、软件版本、图示）和媒介（如：纸质、电子格式）；

c)评审和批准，以确保适宜性和充分性。

7.5.3 形成文件的信息的控制

7.5.3.1 应控制 BCMS 和本标准所要求的形成文件的信息，以确保：

a)无论何时何处需要这些信息，均可获得并适用；

b)予以妥善保护（如:防止失密、不当使用或不完整）。

7.5.3.2 为控制形成文件的信息，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)变更控制（比如版本控制）；

d)保留和处置。

对确定策划和运行 BCMS 所必需的来自外部的原始的形成文件的信息，组织应进行适当识别和控制。

应对所保存的作为符合性证据的形成文件的信息予以保护，防止非预期的更改。

注：形成文件的信息的“访问”可能意味着仅允许查阅，或者意味着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 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)将文件化信息保持在足以确信过程已按照策划进行的程度上。

组织应控制策划的变更，评审非预期变更的后果，必要时，采取措施减轻不利影响

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)实施和保持系统化的业务影响分析和中断风险评估过程；

b)按计划的时间间隔以及当组织内部或其运行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：组织确定业务影响分析和风险评估的实施次序。

8.2.2 业务影响分析

组织应使用业务影响分析过程来确定业务连续性的优先事项和要求。该过程应：

a)确定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)使用影响类别和准则，评估这些活动中断后随时间推移所产生的影响；

d)识别不恢复这些活动所造成的影响对组织变得不可接受的时间范围；

注 1：该时间范围可称为“最大可容忍中断时间(MTPD)”。

e)在 d)中识别的时间范围内，在最低可接受水平上制定恢复中断优先级时间表；

注 2：此优先级时间表可称为“恢复时间目标（RTO)”。

f)使用该业务影响分析结果确定优先活动；

g)确定支持优先活动所需的资源；

h)确定包括合作方和供应商在内的依赖关系，以及优先活动之间的相互依赖关系。

8.2.3 风险评估

组织应实施并保持风险评估过程。

注：风险评估过程见 ISO31000。

组织应：

a)识别中断对组织的优先活动及其所需资源所带来的风险；

b)分析并评价已识别的风险；

c)确定需处置的风险。

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

8.3 业务连续性策略和解决方案

8.3.1 总则

组织应基于业务影响分析和风险评估的输出结果，确定并选择考虑中断之前、中断期间和中断之后备选方案的业务连续性策略。业务连续性策略应由一个或多个解决方案组成。

8.3.2 策略和解决方案的识别

对于策略和解决方案的识别，应基于以下策略和解决方案的程度：

a)在确定的时间表和商定的能力范围内，满足持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)缩短中断的时间；

e)限制中断对组织产品和服务的影响；

f)提供可获得的足够资源。

8.3.3 策略和解决方案的选择

对于策略和解决方案的选择，应基于以下策略和解决方案的程度：

a)在确定的时间框架和商定的能力范围内，满足继续和恢复优先活动的要求；

b)考虑组织可能承受或不可能承受风险的类型和数量；

c)考虑相应的成本和收益。

8.3.4 资源要求

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

a)人员；

b)信息和数据；

c)物理基础设施，例如建筑物，工作场所或其它设施和相关的配套设备；

d)设备和耗材；

e)信息和通信技术(ICT)系统；

f)运输和后勤；

g)财务；

h)合作伙伴和供应商。

8.3.5 解决方案的实施

组织应实施并保持选定的业务连续性解决方案，以便在需要时启动这些解决方案。

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机制，以便及时向有关相关方预警和沟通。应提供在中断期间对组织进行管理的计划和程序。这些计划和程序，应在需要启动业务连续性解决方案时使用。

注：有不同类型的程序，包含有业务连续性计划。

组织应基于所选定的策略和解决方案的输出结果，识别并制定业务连续性计划和程序。这些程序应：

a)详细说明在中断期间需要采取的紧急步骤；

b)灵活应对中断所带来的不断变化的内部和外部环境；

c)关注可能导致中断事件的影响；

d)通过实施适当的解决方案，有效地将影响降到最低程度；

e)为业务连续性计划和程序所规定的任务分配角色和职责。

8.4.2 响应机制

8.4.2.1 组织应实施并保持一种机制，即确定一个或多个团队负责响应各种中断。

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相互关系。

8.4.2.3 总体而言，各个团队应有能力，以：

a)评估中断的性质、程度及其潜在影响；

b)根据预先确定的临界值对影响进行评估，以此作为启动证实相应的理由；

c)启动适当的业务连续性响应；

d)计划需要采取的措施；

e)确定优先事项（将生命安全作为第一优先事项）；

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)与有关相关方、监管机构和媒体进行沟通。

8.4.2.4 每个团队都应有：

a)已确定的具有履行其指派角色所必需的职责、权限和能力的人员及其候补人员；

b)指导其行动的文件化程序（见 8.4.4），包括启动、运行、协调和沟通响应的程序。

8.4.3 预警和沟通

8.4.3.1 组织应制定和保持用于下列方面的程序：

a) 与有关相关方进行内部和外部沟通，包括沟通什么、何时沟通、与谁沟通以及如何沟通；

注：组织可以制定和保持如何以及在何种情况下与员工及其紧急联系人进行沟通的程序。

b) 接收、记录和响应来自相关方的沟通，包括国家或地区性的风险预警系统或类似系统；

c) 确保沟通手段在中断期间可用；

d) 促进与应急响应人员的结构化沟通；

e) 提供事件发生后组织对媒体响应的详细说明，包括沟通策略；

f) 记录中断的详细情况、采取的措施以及所做出的决定

8.4.3.2 在适用的情况下，还应考虑和实施下列事项：

a) 向可能受到实际发生或即将发生中断影响的相关方发出预警；

b) 确保多个响应组织之间适当的协调和沟通。

预警和沟通程序应作为 8.5 描述的演练方案的一部分进行演练。

8.4.4 业务连续性计划

8.4.4.1 组织应制定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，以协助团队应对中断，并协助组织进行响应和恢复。

8.4.4.2 总体而言，业务连续性计划应包括：

a)团队将采取措施的详细说明，以：

1)在预定时间内持续或恢复优先活动；

2)监控中断的影响和组织对中断的响应；

b)参考预先确定的临界值和启动响应过程；

c)以约定的能力交付产品和服务的程序；

d)管理中断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)实施计划团队的角色和职责；

c)实施解决方案的措施；

d)启动（包括启用准则）、运行、协调和沟通团队行动所需的支持性信息；

e)内部和外部相互依赖关系；

f)资源的要求；

g)报告的要求；

h)退出过程。

每个计划应在其需要的时间和地点均可使用和获得。

8.4.5 恢复

组织应有文件化过程，以便从在发生中断期间和发生中断之后所采用的临时措施中恢复和重新开始业务活动。

8.5 演练

方案组织应实施并保持一个演练和测试方案，以便随着时间的推移来确认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)发展那些在中断中发挥作用人员的团队合作、能力、信心和知识；

d)随着时间的推移，确认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，内容包含输出结果、建议和实施改进措施；

f)在促进持续改进的环境下得到评审；

g)按照计划的时间间隔以及当组织内部或其运行环境出现重大变化时进行。组织应按照其演练和测试的结果，实施变更和改进。

8.6 业务连续性文件化和能力评价

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)这些评价应通过评审、分析、演练、测试、事故后报告和绩效评价来进行；

c)对相关的合作伙伴和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。

这些评价应按照计划的时间间隔、事件发生或应急预案启动之后以及在发生重大变化时进行。

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)用什么方法进行监视、测量、分析和评价，如适用，以确保结果有效；

c)在何时和由谁实施监视和测量；

d)在何时和由何人对监视和测量的结果进行分析和评价；

组织应保留适当的文件化信息，以作为结果的证据；

组织应评价 BCMS 绩效和 BCMS 的有效性。

9.2 内部审核

9.2.1 总则

组织应按照计划的时间间隔进行内部审核，以提供有关 BCMS 的下列信息：

a)是否符合：

1)组织自身的 BCMS 要求；

2)本标准的要求。

b)是否得到有效的实施和保持。

9.2.2 审核方案

组织应：

a) 依据有关过程的重要性和以往的审核结果，策划、制定、实施和保持审核方案，审核方案包括频次、方法、职责、策划要求和报告；

b) 确定每次审核的审核准则和范围；

c) 选择审核员和实施审核，以确保审核过程客观公正；

d) 确保审核结果报告给相关管理者；
e) 保留文件化信息，作为实施审核方案以及审核结果的证据；
f) 确保及时采取必要的纠正措施，消除已发现的不合格及其原因；
g) 确保后续审核活动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

最高管理者应按照计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

管理评审应考虑下列内容：

a)以往管理评审所采取措施的情况；
b)与 BCMS 相关的内外部因素的变化；
c)下列有关 BCMS 绩效的信息，包括其趋势：
1)不合格及纠正措施；
2)监视和测量评价结果；
3)审核结果；
d)相关方的反馈；
e)BCMS 的变更需求，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)来自业务影响分析和风险评估的信息；
h)来自业务连续性文件化和能力评价的输出(见 8.6)；
i)在以往风险评估中未得到充分应对的风险或问题；
j)产生于未遂事件和中断的经验教训和措施；
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改进 BCMS 效率和有效性而对 BCMS 进行变更的需求，包括下列内容：

a)对 BCMS 范围的变更；
b)对业务影响分析、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的更新；
c)对可能影响 BCMS 的内部或外部因素的应对程序和控制措施的修改；
d)对控制措施的有效性进行测量的方式。

9.3.3.2 组织应保留文件化信息，作为管理评审的结果的证据。组织应：

a)与有关相关方沟通管理评审的结果；
b)针对这些管理评审结果采取适当的措施。

10 改进

10.1.1 组织应确定改进的机会，并采取必要的措施，以实现 BCMS 的预期结果。

10.1.2 当出现不合格时，组织应：

a) 对不合格做出反应，并在适当时：
1) 采取措施以控制和纠正不合格；
2) 处置后果；
b) 通过下列活动，评价是否需要采取措施，以消除产生不合格的原因，避免其再次发生或者在其他场合发生：
1) 评审不合格；

2) 确定不合格的原因；

3) 确定是否存在或可能发生类似的不合格；

c) 实施所需的措施；

d) 评审所采取的纠正措施的有效性；

e) 需要时，变更 BCMS。

纠正措施应与不合格所产生的影响程度相适应。

10.1.3 组织应保留文件化信息，作为下列事项的证据：

a) 不符合的性质以及随后所采取的措施；

b) 纠正措施的结果。

10.2 持续改进

组织应基于定性和定量的方法，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 有关的需求或机遇，这些需求或机遇应作为持续改进的一部分加以应对。

注：组织可以运用 BCMS 的过程来实现改进，例如领导力、策划和绩效评价。

以上内容均为孟凯老师 PPT 中翻译的中文标准摘抄，有几处遗漏，更正如下：

1. 8.1 条款下增加了“组织应确保外包过程和供应链得到控制。”； 英文标准里有； PPT 里没有对应的中文

2. 增加了 8.4.3 整个条款的内容

3. 9.3.2 处增加了“f)组织中可用于提高 BCMS 绩效和有效性的程序和资源”；英文标准里有； PPT 里没有对应的中文

4. PPT 中 10.2 的中文翻译和英文标准对不上。替换了。

5. 去掉了 10.3 条款；英文标准中无 10.3 条款。

6. 8.4.4.2 处“个人福祉”变更为“个人福利”

表 C.1　员工有效人数与审核时间的关系

有效人数	初次认证审核时间 （第 1 阶段＋第 2 阶段） 人日	有效人数	初次认证审核时间 （第 1 阶段＋第 2 阶段） 人日
1～25	4	1 176～1 550	15
26～45	5	1 551～2 025	16
46～65	6	2 026～2 675	17
66～85	7	2 676～3 450	18
86～125	8	3 451～4 350	19
126～175	9	4 351～5 450	20
176～275	10	5 451～6 800	21
276～425	11	6 801～8 500	22
426～625	12	8 501～10 700	23
626～875	13	＞10 700	遵循上述递进规律
876～1 175	14		

注：表中的人数宜视为连续变化的，而不是阶梯式变化的。

本标准所要求的文件化信息包括:
- 组织的环境(4.1);
- 法律、法规和其他要求以及符合性证据(4.2.2);
- BCMS 的范围和与范围有关的任何删减(4.3.2);
- 业务连续性方针(5.3);
- 业务连续性目标(6.2);
- 能力(7.2);
- 业务影响分析和风险评估过程(8.2);
- 业务连续性策略(8.3),包括供考虑的所有候选策略;
- 连续性,事件管理和恢复程序(8.4);
- 事后演练报告(8.5);
- BCMS 的监视(9.1);
- 内部审核(9.2);- 管理评审(9.3);
- 不符合和纠正措施(10.1)。

此外,为确保 BCMS 的有效性,文件化信息包含以下可能要求的信息:
- 业务影响分析的结果;
- 风险评估的结果;
- 业务连续性策略的确定和选择;
- 事件响应概述;
- 意识方案;
- 与员工和相关方就 BCMS 及事件进行的沟通,如通讯、会议纪要和警报;
- 组织和个人的培训方案;
- 演练进度表;
- 与供应商的合同和服务级别协议;
- 承包商和供应商的通知和响应程序;
- 检查、保持和校正的证据;
- 对已发生的事件和未遂事件的报告;
- BCMS 评审会议记录。

附录 A（规范性附录）

BCMS 认证业务范围分类表

大类编号	大类名称
1	制造业
2	电力、热力、燃气及水生产和供应业
3	交通运输、仓储和邮政业
4	信息传输、软件和信息技术服务业
5	金融业
6	其他

注：

1) 该分类表基于 GB/T 4754-2011 国民经济行业分类，重点关注了那些组织发生业务中断时将造成较大影响的行业，同时也考虑了现有的 BCMS 认证市场；
2) 基于对 BCMS 认证机构认可市场的分析，CNAS 目前仅在编号为 1-5 的大类内开展认可。