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
A/0	崔海军	张京梅	郑宇兵	20251203	20251203

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
A/0	新编	20250722	20250724
A/0	认证证书及认证标志的要求	20250828	20250828
A/0	认证依据文件加中文描述	20251203	20251203

目录

一、前言

本规则依据《中华人民共和国认证认可条例》等相关法律法规，以及 GB/T 30146-2023/ISO 22301:2019《安全与韧性 业务连续性管理体系 要求》制定。其目的是规范业务连续性管理体系（BCMS）认证活动，确保认证过程的公正性、客观性和有效性，为组织提供统一的认证实施规范，也为认证机构、审核员以及申请认证的组织提供明确的指引。

本规则旨在通过明确的认证流程和要求，推动组织建立、实施、保持和持续改进 BCMS，增强组织在面对中断事件时的韧性，保障组织业务的连续运营，保护相关方的利益。

二、适用范围

本规则适用于各类组织的业务连续性管理体系认证活动，包括但不限于企业、事业单位、社会团体、行政机构等不同类型和规模的组织及其组成部分。

无论组织所处的行业、领域，只要其希望通过认证证明自身的业务连续性管理体系符合 GB/T 30146-2023/ISO 22301:2019《安全与韧性 业务连续性管理体系 要求》 标准的要求，均可适用本规则。

本规则同样适用于从事业务连续性管理体系认证的认证机构及其认证人员，指导其开展认证审核、认证决定、监督、再认证等相关工作。

三、认证依据用技术规范、技术规范强制性要求或者标准

本业务连续性管理体系认证的依据为国家标准 GB/T 30146-2023/ISO 22301:2019《安全与韧性 业务连续性管理体系 要求》。

该标准规定了实施、保持和改进业务连续性管理体系的要求，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。标准中的所有要求具有通用性，适用于各种类型、规模和特性的组织或其组成部分，其适用范围取决于组织的运行环境和复杂性。

在认证过程中，应严格遵循该标准的各项要求，确保认证结果的准确性和权威性。

四、对认证人员的要求

认证审核员应具备必要的专业知识和技能，包括但不限于：

1. 熟悉 GB/T 30146-2023/ISO 22301:2019《安全与韧性 业务连续性管理体系 要求》标准的内容和要求，理解业务连续性管理体系的原理和方法。
2. 具备相关的行业知识和经验，了解不同行业组织的业务特点、潜在的中断风险以及相应的业务连续性策略。
3. 掌握审核的原则、方法和技巧，能够独立开展审核工作，客观评价组织的业务连续性管理体系。
4. 认证审核员应取得国家认可的业务连续性审核员资格证书，并在认证机构注册。
5. 审核员应遵守职业道德规范，保持公正、客观、保密的态度，不得与被审核组织存在任何可能影响审核公正性的利益关系。
6. 审核员应定期参加持续教育培训，不断更新知识和技能，以适应业务连续性管理领域的发展和变化。
7. 认证机构应对审核员的能力进行定期评价和监督，确保其持续满足认证工作的要求。
8. 业务连续性管理体系认证人员专业能力进行评价。

五、认证实施程序

5.1 申请

5.1.1 组织要求：

申请认证的组织应具有明确的法律地位，如企业法人需提供营业执照等合法注册证明；非法人组织需提供相应的登记注册文件或批准成立文件。组织应已按照认证依据标准建立了业务连续性管理体系，且体系文件涵盖了认证范围内的所有活动和流程。

5.1.2 申请材料：

（1）正式的认证申请书，应详细填写组织名称、地址、联系方式、场所分布、人员情况、申请认证范围、组织简介、业务范围等基本信息。

（2）组织的法律地位证明文件复印件，如营业执照副本、事业单位法人证书等。若管理体系覆盖多场所活动，应附每个场所的法律地位证明文件的复印件（适用时）；

（3）有关法律法规规定的行政许可证明、资质证书、强制性认证证书、备案证明等的复

印件（适用时）；诚信守法记录或认证人员身份背景的要求。并在有需要情况下即时更新该说明，以便 ZXB 判断其是否具备对该客户实施认证活动的资格或条件。

（4）业务连续性管理体系文件，包括方针、目标、手册、程序文件等。业务连续性计划、应急预案等相关文件。需清晰展示体系如何满足认证依据标准的各项要求。

（5）体系运行的相关记录，如内部审核报告、管理评审报告、业务影响分析、风险评估报告及相关记录，以证明体系已有效运行至少 3 个月。

（6）适用的法律法规清单，以及组织对这些法律法规合规性的说明，表明组织了解并遵循与业务连续性管理相关的国家和地方法规。

（7）认证机构要求的其他与认证审核有关的必要文件。

5.2 申请评审及方案策划

5.2.1 申请评审

认证机构收到申请材料后，将组织专业人员对申请材料进行全面评审。评审内容包括：

（1）申请完整性审查：确认申请材料是否齐全，各项信息填写是否完整、准确，如申请书上的组织信息与法律地位证明文件是否一致，体系文件是否涵盖了标准要求的所有要素等。

（2）认证范围合理性评估：审核申请的认证范围是否明确、合理，与组织的实际业务活动是否相符。

（3）体系文件符合性审查：组织提交的体系文件是否满足认证审核的基本要求，文件之间的逻辑关系是否清晰，内部审核程序是否规定了审核的频率、方法、人员职责等。内部审核报告是否显示按照计划进行了审核，且对发现的不符合项采取了相应的纠正措施。

（4）组织的法律资质是否有效。

若申请材料存在不完整、不准确或不符合要求的情况，认证机构将通知组织进行补充或修改。只有在申请材料通过评审后，经评审符合要求的，认证机构应与组织签订认证合同，明确双方的权利和义务、认证费用、认证周期等内容。

5.2.2 方案策划

认证机构应根据组织的规模、业务特点、认证范围等因素，制定认证审核方案。审核方案应包括审核的目的、范围、准则、方法、审核组成员、审核时间安排等内容。认证周期的审核方案应覆盖全部的管理体系要求。

通用审核方案（包括程序、通用要求等）由技术部负责组织制定，针对特定认证项目的项目审核方案由运营部负责策划。

初次认证审核方案包括两阶段初次审核、认证决定之后的第一年与第二年的监督审核和第三年在认证到期前进行的再认证审核。一个认证周期一般为三年，第一个三年的认证周期从初次认证决定算起，以后的周期从再认证决定算起。如果特定的行业认证方案有规定，认证周期可以不为 3 年。

对每个认证项目，应策划项目审核方案。在策划项目审核方案以及后续的调整时，应考虑申请客户的规模，其管理体系、产品和过程的范围与复杂程度，其生产过程和产品的安全风险程度，以及经过证实的管理体系有效性水平和以前审核的结果。

如果运营部鉴于申请客户已获的认证或由另一认证机构实施的审核，则应获取并保留充足的证据，例如报告和对不符合采取的纠正措施的文件。所获取的文件应为满足要求提供支持。运营部应根据获取的信息证明对审核方案的任何调整的合理性，并予以记录，并对以前不符合的纠正措施的实施进行跟踪。如果申请客户采用轮班作业，应在建立审核方案和编制审核计划时考虑在轮班工作中发生的活动。

ZXB 在建立或修改审核方案时可能需要考虑的其他事项，如：收到的对申请客户的投诉；结合、一体化或联合审核；认证要求的变化；法律要求的变化；组织的绩效数据（例如缺陷水平、关键绩效指标（KPI）数据等）；利益相关方的关注。在确定审核范围和编制审核计划时可能也需要考虑这些事项。

5.3 文件评审

5.3.1 文件评审的目的是：文件审核的目的是评价组织的业务连续性管理体系文件是否符合 GB/T 30146-2023/ISO 22301:2019《安全与韧性 业务连续性管理体系 要求》 标准的要求，是否具有可操作性和适宜性。

5.3.2 文件审核的范围包括组织的业务连续性管理体系手册、程序文件、作业指导书、记录表格以及与业务连续性管理相关的其他文件。

5.3.3 文件审核的主要内容：

- 业务连续性方针是否与组织的宗旨相适应，是否为目标的制定提供了框架，是否包含满足适用要求和持续改进的承诺。

- 业务连续性目标是否与方针一致，是否可测量，是否考虑了适用的要求，是否得到监视和沟通。
- 体系文件的结构是否合理，层次是否清晰，是否覆盖了标准的所有要求。
- 业务影响分析和风险评估的方法是否适当，结果是否合理，是否为业务连续性策略的制定提供了依据。
- 业务连续性计划是否具有针对性和可操作性，是否涵盖了可能发生的中断事件，是否明确了应急响应的流程、职责和资源保障。
- 程序文件是否明确了各项活动的目的、范围、职责、工作流程和记录要求。

5.3.4 文件审核中发现的问题，认证机构应及时与组织沟通，组织应在规定的时间内进行修改和完善。如文件存在重大不符合项，认证机构可暂停审核，直至组织完成整改。文件审核通过后，认证机构方可安排现场审核。

5.3.5 文件审核其它关注点：

标准条款	审核要点
1. 组织环境	是否明确了组织的内外部环境，包括影响业务连续性的因素；是否识别了相关方及其需求和期望；是否确定了业务连续性管理体系的范围，范围的确定是否合理。
2. 领导力	最高管理者是否对业务连续性管理体系做出了承诺，是否建立了业务连续性方针和目标；是否明确了各级人员的职责和权限，是否确保了资源的提供。
3. 策划	是否识别了影响业务连续性的风险和机会，并制定了应对措施；业务连续性目标是否明确、可测量，是否制定了实现目标的计划；是否对体系的变更进行了策划。
4. 支持	是否提供了必要的资源，包括人员、基础设施、信息等；是否确保人员具备必要的能力和意识；是否建立了有效的沟通机制；体

标准条款	审核要点
	系文件是否完整、适宜、有效。
5. 运行	是否对业务连续性管理的运行过程进行了策划和控制；业务影响分析和风险评估是否定期开展和更新；是否制定了业务连续性策略和解决方案，并有效实施；是否建立了事件响应机制和业务连续性计划；是否进行了演练和测试。
6. 绩效评价	是否建立了监视、测量、分析和评价体系绩效的机制；是否定期进行内部审核，审核结果是否得到有效利用；最高管理者是否定期进行管理评审，以确保体系的适宜性、充分性和有效性。
7. 改进	是否对发现的不符合项采取了纠正措施，并验证其有效性；是否持续改进体系的绩效。

5.4 审核计划

5.4.1 审核计划的编制及现场审核前的准备要求

(1) 审核范围与合同评审单及审核工作通知一致；

(2) 按运营部安排进行审核时间、审核人员、审核人日数的安排；

(3) 审核计划包括：审核的目的、范围、准则，审核组成员及分工，包括审核组长、审核员、技术专家等。审核的场所、部门和过程，审核所需的资源和支持条件等。

(4) 每天日程安排 8 小时，审核人员注明级别，按照要求实施评审、批准；

(5) 审核组长原则上应实施对最高管理层的审核；

(6) 审核组长应合理安排审核分工及审核时间。

除上述之外，在制定审核计划时，还应关注初次审核、监督审核、再注册及特殊项目审核时的要求。

组织应配合认证机构的审核计划安排，为审核组提供必要的工作条件和资源，包括办公场所、资料查阅、人员配合等。如组织对审核计划有异议，应在审核前与认证机构沟通，认

证机构应根据实际情况进行调整。

5.4.2 审核计划应提前 5 个工作日传至受审核方，并沟通确认。审核组长应将受审核方确认的审核计划及时通知审核组组员，并着手进行审核安排。计划最终应由受审核方签字盖章带回。

5.4.3 审核计划如果在审核过程中发生变化，审核组长应在审核组内部会议记录中进行说明，并在交回审核资料时告知运营部资料接受人员，但变化不应影响到专业审核员对重要部门及场所的审核。

5.4.4 审核组内部会议要求

从审核组进入驻地直至审核结束，组长应充分利用审核组内部会议做好审核安排、沟通及控制，审核组内部会议应在现场审核开始前、每天审核结束后、末次会议开始前进行，并应在每次会议结束后进行记录。下述方面应至少涉及：

(1) 审核前的必要专业培训；

(2) 相关文件的熟悉；

(3) 审核分工及安排；

(4) 审核进度掌握及审核信息沟通；

(5) 审核组的内部审核评价；

(6) 审核结果的确定（包括不符合项及审核结论）。

审核过程中与审核策划不一致的内容及处理情况应重点进行记录；

5.5 多现场审核

1. 对于存在多个现场的组织，认证机构应根据现场的分布情况、业务相关性、规模等因素，制定多现场审核方案。
2. 审核方案应明确各现场的审核范围、审核时间、审核内容和审核方式。对于具有相似业务过程和管理模式的现场，可采用抽样审核的方式，但抽样应具有代表性。
3. 审核组应在审核前了解各现场的基本情况，包括业务特点、潜在风险、管理体系运行情况等。
4. 多现场审核的结果应综合考虑各现场的审核情况，确保认证结论的准确性和公正性。

5.6 认证范围的确定要求

1. 认证范围应根据组织的业务活动、产品和服务、场所分布等因素确定，应准确反映组织业务连续性管理体系所覆盖的范围。
2. 认证范围的描述应清晰、明确，避免使用模糊、笼统的词汇。通常包括组织的名称、主要业务活动、认证依据的标准、覆盖的场所等内容。
3. 确定认证范围时，应考虑以下因素：

- 组织的宗旨和战略目标。
- 组织的业务过程和产品服务范围。
- 业务影响分析和风险评估的结果。
- 相关方的需求和期望。
- 法律法规的要求。

认证机构与组织应就认证范围达成一致，如组织对认证范围有特殊要求，应提供充分的理由和依据。

认证范围一旦确定，不得随意变更。如需变更，应按照本规则第十一章 “影响认证的变更” 的要求办理。

5.7 不符合项纠正和纠正措施及验证要求

5.7.1 审核过程中发现的不符合项，审核组应及时向组织发出不符合项报告，明确不符合项的性质、内容、不符合的标准条款以及整改要求。组织应在规定的时间内对不符合项进行分析，确定不符合的原因，并制定纠正和纠正措施。纠正措施应具有针对性和可操作性，能够有效防止不符合项的再次发生。组织应按照制定的纠正和纠正措施进行整改，并保存相关的记录，包括整改计划、实施证据、效果验证等。认证机构应在组织完成整改后，对纠正和纠正措施的有效性进行验证。验证方式可包括资料审查、现场核实等。经验证，纠正和纠正措施有效的，不符合项关闭；如纠正和纠正措施无效或未按期完成整改，认证机构应根据情况采取暂停认证、终止认证等措施。

5.7.2 当审核发现体系运行中存在明显的不符合时，应在检查单中详细记录该不符合事实。

5.7.3 根据不符合事实记录开出不符合项报告。不符合项报告的事实应经受审核方陪同人员的见证，并由受审核方代表确认。

5.7.4 不符合项跟踪方式有三种：

1. 书面验证；2.现场验证；3.下次监督时验证。

具体详见 ZXB-CX-07 不符合及纠正措施、预防措施控制程序

5.8 审核报告

审核组在完成现场审核和不符合项整改验证后，应进行综合评价。评价内容包括：

- 组织的业务连续性管理体系与 GB/T 30146-2023/ISO 22301:2019《安全与韧性 业务连续性管理体系 要求》 标准的符合程度。
- 体系的实施和运行效果，包括业务连续性目标的实现情况、应对中断事件的能力等。
- 不符合项的数量、性质及整改情况。
- 组织的持续改进能力。

审核组应根据综合评价的结果，编写审核报告。审核报告应包括以下内容：

- 审核的目的、范围、准则、方法。
- 审核组成员及审核时间。
- 组织的基本情况。
- 审核发现，包括符合项和不符合项。
- 综合评价结论。
- 对组织的改进建议。

审核报告应提交给认证机构，经审核机构审核批准后，发送给组织。组织如对审核报告有异议，应在规定的时间内提出，认证机构应进行复核和处理。

六、初次认证审核：

6.1 第一阶段审核

6.1.1 第一阶段审核的目的是：

- 了解组织的业务连续性管理体系的建立和运行情况，确认体系文件与标准的符合性。
- 评估组织的现场情况，确定第二阶段审核的重点和范围。

- 验证组织是否具备进入第二阶段审核的条件。

6.1.2 第一阶段审核的内容包括：

- 审查组织的业务连续性管理体系文件，重点关注方针、目标、手册、程序文件的符合性和适宜性。
- 了解组织的业务流程、业务影响分析和风险评估的开展情况。
- 与组织的最高管理者、业务连续性管理负责人等进行沟通，了解其对体系的认识和重视程度。
- 查看组织的现场环境、基础设施、资源配置等情况。
- 评估组织的内部审核和管理评审的开展情况。

6.1.3 第一阶段审核可以采用现场审核、文件审核相结合的方式进行。对于规模较小、业务简单的组织，可适当简化审核流程。

6.1.4 审核组在第一阶段审核结束后，应编写第一阶段审核报告，明确审核发现、存在的问题以及对第二阶段审核的建议。如发现组织存在影响第二阶段审核的重大问题，应要求组织在规定的时间内进行整改，整改合格后方可进行第二阶段审核。

6.2 第二阶段审核

6.2.1 第二阶段审核的目的是全面评价组织的业务连续性管理体系的实施和运行效果，确认其是否符合 GB/T 30146-2023/ISO 22301:2019《安全与韧性 业务连续性管理体系 要求》标准的要求，是否具备认证注册的条件。6.2.2 第二阶段审核的内容包括：

- 对组织的业务连续性管理体系的所有过程进行全面审核，包括方针、策划、实施、检查、改进等环节。
- 验证业务影响分析和风险评估的有效性，以及业务连续性策略和解决方案的实施情况。
- 检查业务连续性计划的制定、演练和更新情况，评估组织应对中断事件的能力。
- 审核内部审核和管理评审的有效性，以及对不符合项的纠正和预防措施的实施情况。
- 核实第一阶段审核中发现问题的整改情况。

6.2.3 第二阶段审核应在组织的现场进行，审核组应按照审核计划和审核准则，采用抽样、面谈、查阅记录、现场观察等方法收集审核证据。

6.2.4 审核组在第二阶段审核结束后，应汇总审核发现，形成审核结论，并编写第二阶段审核报告。报告应包括审核的范围、方法、发现的不符合项、体系的符合程度和运行效果等内容。

七、复核、认证决定

7.1 复核

审核组完成现场审核后，将审核资料提交给认证机构的技术委员会或相关专业人员进行复核。复核的主要内容包括：

审核过程合规性审查：检查审核组的审核活动是否按照认证机构的审核程序和相关标准要求进行，审核计划的执行是否严格，审核方法是否得当，审核证据的收集是否充分、有效。例如，复核审核员在现场检查时是否对标准要求的所有条款都进行了合理的抽样检查，审核记录是否清晰、准确地反映了审核过程和发现的问题。

不符合项判定准确性评估：对审核组判定的不符合项进行重新评估，确认不符合项的描述是否准确、清晰，判定依据是否充分，不符合项的性质划分是否合理。例如，复核严重不符合项的判定是否确实符合严重不符合项的定义，是否有足够的证据支持该判定。

审核结论合理性审查：审查审核组给出的审核结论是否客观、公正，是否基于充分的审核证据。审核结论通常包括推荐通过认证、有条件通过认证（需在规定时间内完成不符合项整改并经审核组验证）、不通过认证三种情况。复核人员将综合考虑审核过程中的各项因素，判断审核结论是否恰当。

若复核过程中发现问题，认证机构将与审核组沟通，要求审核组进行补充说明或采取相应的纠正措施。只有在复核通过后，认证机构才能根据审核结果做出认证决定。

7.2 认证决定

7.2.1 ZXB 在对审核报告、不符合项的纠正和纠正措施及其结果进行综合评价基础上，作出认证决定。

7.2.2 审核组成员不得参与对审核项目的认证决定。

7.2.3 认证决定人员在作出认证决定前应确认如下情形：

（1）审核报告符合本规则要求，能够满足作出认证决定所需要的信息；

（2）反映以下问题的不符合项，ZXB 已评审、接受并验证了纠正和纠正措施及其结果的有效性：

① 未能满足管理体系标准的要求；

② 制定的目标不可测量、或测量方法不明确；

③ 对实现目标具有重要影响的关键点的监视和测量未有效运行，或者对这些关键点的报告或评审记录不完整或无效；

④ 在持续改进管理体系的有效性方面存在缺陷，实现业务连续性目标有重大疑问。

（3）ZXB 对其他不符合项已评审，并接受了申请组织计划采取的纠正和纠正措施。

7.2.4 认证决定包括以下几种情况：

- 批准认证注册，颁发认证证书。
- 有条件批准认证注册，要求组织在规定的时间内完成特定的整改措施，并经验证合格后颁发认证证书。
- 不批准认证注册，说明原因，并告知组织可采取的申诉途径。

7.2.5 申请组织不能满足上述要求的，评定该申请组织不符合认证要求，以书面形式告知申请组织并说明其未通过认证的原因。

7.2.6 ZXB 在颁发认证证书后 30 个工作日内按照规定的要求将相关信息报送国家认监委。证书信息可在：国家认证认可监督管理委员会官方网站（www.cnca.gov.cn）或众信标（北京）认证有限公司官方网站（www.zhongxinbiao.com/）上查询。

7.2.7 ZXB 不得将申请组织是否获得认证与参与认证审核的审核员及其他人员的薪酬挂钩。

八、监督

8.1 监督审核的目的：验证获证组织的业务连续性管理体系是否持续满足认证标准的要求，或考察组织运行引起的变化是否符合认证要求。

8.2 监督审核的要求：

8.2.1 监督审核可采用抽样的方式进行。对各部门、相同的现场的抽样须三年内全部覆盖。重要部门每次都应进行审核。如果获证组织上的分布于几个不同的场所，每监督审核可针

对不同的现场进行抽样，但应确保在三年中覆盖全部现场，其中每年对其总部的审核应至少一次。

8.2.2 每次监督审核应涉及全部业务连续性管理体系要素，三年内的不同次监督审核对各个要素审查的深度和广度可各有侧重，应注意对上次现场审核遗留问题的验证。

8.2.3 较之初次审核，监督审核的要求不仅不应放松，反而应适度从严，如发现与上次审核相同的问题，应考虑不符合项性质的升级。

8.2.4 监督审核的内容包括：

- 组织的业务连续性管理体系的运行情况，包括方针、目标的实现情况。
- 内部审核和管理评审的开展情况。
- 对上次审核中发现不符合项的整改情况的验证。
- 业务连续性计划的演练和更新情况。
- 组织的业务活动、内外部环境等发生变化时，体系的适应性和有效性。

  其他与体系运行相关的重要事项。

8.3 监督审核时间间隔每两次不应超过12个月，若企业由于季节性生产或其他原因不能按原计划进行复查，需调整时间安排时，应由受审核方提出书面文件（传真件也可）说明推迟理由，由运营部相应人员将书面文件提交公司领导批准。相关资料应保存至运营部，最多可以延长1个月，涉及如认证合格证书上覆盖产品范围扩大类别等重大事由，应通知运营部办理相关补充合同。若企业变更地址、名称时，由审核组长在现场审核时确认并带回证据。

8.4 监督审核的现场审核与初审程序一致，审核组长在监督审核现场审核时，将监督审核收费通知单交与受审核方。

8.5 监督审核结论为：a）证书继续有效；b）证书暂停；c）证书撤销。

8.6 在监督审核现场审核末次会议上，监督审核组长应向获证单位清楚说明对不合格项的纠正期限及以下相关内容：

证书继续有效：

a）一般不符合项：一般一个月内完成纠正措施且有效；

b）严重不符合项：一般半个月内完成纠正措施且有效。

证书暂停：

a）获证组织私自对证书进行了更改；

b）获证组织体系运行达不到规定的要求，但严重程度并不构成撤销认证资格。

证书撤消：

a）证书暂停后，在规定时间内按规定要求采取适当纠正措施；

b）存在严重不符合规定要求的情况。

8.7 监督审核后做好资料整理上报工作，提交审核案卷的时限要求是现场审核结束后25天内。

8.8 审核组长负责编写监督审核报告，并交技术部审查。技术部资料审查内容按照《管理体系认证决定审批意见》进行。

8.9 监督审核资料经授权评定人员审查后，技术部将监督审核的全部资料进行归档。

九、再认证

9.1 运营部根据签订合同后的复评企业汇总情况，结合实际情况制定具体的再认证工作实施计划。

9.2 运营部根据审核任务及计划下发审核通知单，指定组长。获证单位的任何变更信息，应根据合同评审单中的内容，在委任中中写明,并要求做文件审查。

9.3 再认证工作所需人日数在认证基础无更改的情况下，按相当于初次审核的 2/3 人日数进行。若有变动应根据实际情况加大力度。

9.4 再认证工作程序与正式审核程序相同。

9.5 文件审核。

9.6 审核准备。

9.7 现场审核。

9.8 审核报告的编写、发放与批准。

9.9 再认证的审核内容应结合初次认证注册审核第一阶段和第二阶段的审核内容，应考虑上次审核的结果并至少包括文件的审核和所有认证范围的现场审核；还应检查组织投诉、申诉及其所采取的纠正措施记录。

9.10 审核资料的上报、审查、评定、归档与上相同

9.11 再认证换证后对获证单位每年进行一资监督审核。

十、认证证书状态管理规定、要求

认证的批准、拒绝、保持、扩大、缩小、暂停、恢复或撤销认证证书

10.1 批准认证资格

10.1.1 批准认证资格条件：

（1）认证申请材料真实、准确、有效；

（2）受审核方建立和实施的业务连续性管理体系符合认证标准/规范性文件要求，审核组提出推荐认证的结论意见；

（3）受审核方审核的认证范围在法律地位文件和资质规定的范围内；

（4）国家或地方或行业有要求时，受审核方申请的认证范围内的组织单元、产品、服务及其过程和多动以满足使用额法律法规要求；

（5）审核证据表明管理评审和内部审核的安排已实施、有效且得到保持，并已进行了一次覆盖业务连续性管理体系所有要求的完整内部审核和管理评审；

（6）审核中发现的不符合在规定期限内已采取纠正/纠正措施，经认证机构验证有效；

（7）认证申请方已与 ZXB 签订认证合同，承诺始终遵守认证有关规定，并按认证合同规定缴纳认证费用。

10.1.2 批准认证

（1）满足批准认证资格的条件，经 ZXB 评定，认为认证客户在认证范围内已满足批准认证资格的条件，同意批准认证注册；

（2）ZXB 向认证客户颁发认证证书，要求获证客户按规定使用认证标志。

10.2 拒绝认证

（1）经 ZXB 技术部评定，被认证客户的业务连续性管理体系不满足批准认证注册的条件，不予批准认证注册。运营部制作《不予认证注册通知》；

（2）ZXB 法定代表人或授权人签发《不予认证注册通知》；

（3）运营部向被认证客户发出《不予认证注册通知》；

（4）经评审不予受理的认证申请，有运营部通知认证申请组织；

（5）现场审核为“不推荐注册”结论的，有 ZXB 法定代表人或授权人签发《不予认证注册通知》。

10.3 保持资格

10.3.1 保持认证资格的条件：

（1）获证组织的法律地位、资质持续符合国家的最新要求，并且认证范围在法律地位文件和资质规定的范围内；

(2)获证组织的业务连续性管理体系持续符合认证标准/规范性文件要求；

（3）获证组织持续避守认证有关的规定，包括变更的规定；

（4）获证组织在认证范内的组织单元、产品、服务及其过程和活动持续满足适用的最新法律法规的要求，如发生不满足时及时采取有效的措施；

（5）获证组织于获证期间在认证范围内未发生重大事故和国家检查不合格；

（6）获证组织在获证期间未发生误用认证证书和认证标志，如有发生能及时有效地采取纠正和纠正措施，并将误用产生的影响降至最少程度；

（7）获证组织对顾客或相关方的重大投诉和关切能及时有效地处理；

（8）管理评审、内审每年至少进行一次，原则上两次内审时间不超过 12 个月；

（9）按时接受监督审核的；

（10）获证组织能按照 ZXB 要求向 ZXB 通报业务连续性管理体系和重要过程变更等信息；

（11）获证组织履行与 ZXB 签订认证合同中规定的责任和义务，并按照认证合同规定缴纳认证费用。

10.3.2 保持认证资格：

(1)满足保持认证资格的条件，监督审核后经 ZXB 的审核组长确认后，认为获证组织在认证范围内能持续满足保持认证资格的条件，同意保持认证资格，由 ZXB 签发确证书并向获证组织发放；

(2)在认证证书有效期内如有认证要求变，获证组织接受变更的认证要求，并经 ZXB 验证在认证范围内管理体系满足变更的要求，可保持认证资格。

10.4 扩大认证范围

10.4.1 扩大认证范围的条件：

（1）获证组织保持认证资格有效；

（2）国家、地方或行业有要求时，获证组织在扩大认证范围内具有规定的资质

（3）获证组织申请扩大认证范围在法律地位文件和资质规定的范围内；

（4）获证组织的管理体系覆盖申请扩大的认证范围，并符合认证标准/规范性文件要求 ；

（5）国家或地方或行业有要求时，获证组织在申请扩大认证范围内的组织单元、产品、服务及其过程和活动已满足适用的法律法规的要求；

(6)获证组织按照认证规定缴纳补充认证费用。

10.4.2 扩大认证范围：

（1）获证组织向 ZXB 正式提交扩大认证范围的申请和相关附件；

（2）满足扩大认证范围的条件，经 ZXB 审核、评定，认为获证组织在申请扩大认证范围内已满足批准认证资格的条件，同意批准扩大认证范围，认证证书的注册号和有效期保持不变。

10.5 缩小认证范围

10.5.1 缩小认证范的条件：

（1）组织的认证范围内部分产品服务范围、区域等不再符合认证标准/规范性文件和其他附加要求；

（2）获证组织不愿再继续保持认证范围内的部分产品服务范围、区域等认证资格；

（3）获证组织缩小认证范围应不包括为缩小认证风险的情况。

10.5.2 缩小认证范围

（1）获证组织向 ZXB 正式提交缩小认证范围的申请，或 ZXB 提出缩小获证组织认证范围的建议，并提供理由和证据 ZXB 的评定意见和日常监督结果也可作为认证范围缩小的信息来源和理由。经认证双方沟通后达成一致意见；

(2)经 ZXB 评定，认为获证组织在申请缩小认证范围不会对仍保持的认证范围产生影响，同意批准缩小认证范围，收回原认证证书，换发认证证书或附件，认证证书的注册号和有效期保持不变；

（3）需要时，获证组织与 ZXB 补充签订认证合同。

10.6 暂停证书

10.6.1 获证组织有以下情形之一的，ZXB 应在调查核实后的 5 个工作日内暂停其认证证书：

（1）业务连续性管理体系及管理体系持续或严重不满足认证要求，包括对业务连续性管理体系及管理体系运行有效性要求的；

（2）不承担、履行认证合同约定的责任和义务的；

（3）被有关执法监管部门责令停业整顿的；

（4）被地方认证监管部门发现体系运行存在问题，需要暂停证书的；

（5）持有的与行政许可证明、资质证书、强制性认证证书等过期失效，重新提交的申请已被受理但尚未换证的；

（6）主动请求暂停的；

（7）其他应当暂停认证证书的。

10.6.2 认证证书暂停期不得超过 6 个月。但属于 8.2.1 第（5）项情形的暂停期可至相关单位作出许可决定之日。

10.6.3 ZXB 暂停认证证书的信息，应明确暂停的起始日期和暂停期限，并声明在暂停期间获证组织不得以任何方式使用认证证书、认证标识或引用认证信息。

10.7 恢复认证资格

10.7.1 恢复认证资格的条件：

恢复认证资格的条件获证组织已针对暂停认证资格的原因采取了有效的纠正措施，产生原因已经消除，恢复符合相关的认证要求，同时已证实在暂停期内没有使用引用认证资格，广告宣传和使用标志。

10.7.2 恢复认证资格

在确定的认证资格暂停限期结束前，根据暂停原因，组织在规定期限内向 ZXB 运营部提出恢复认证资格的申请，并附相关纠正措施和有效性验证材料 ；

经 ZXB 评定，确认组织在暂停认证资格的认证范围内已恢复符合相关的认证要求，作出同意恢复认证资格的评定结论，颁发《恢复使用认证证书和标志的通知》并公告。

10.8 撤销证书

10.8.1 获证组织有以下情形之一的，ZXB 应在获得相关信息并调查核实后 5 个工作日内撤销其认证证书：

（1）被注销或撤销法律地位证明文件的；

（2）拒绝配合认证监管部门实施的监督检查，或者对有关事项的询问和调查提供了虚假材料或信息的；

（3）出现重大的与业务连续性管理体系相关的事故，经执法监管部门或经 ZXB 确认是获证组织违规造成的；

（4）有其他严重违反法律法规行为的；

（5）暂停认证证书的期限已满但导致暂停的问题未得到解决或纠正的（包括持有的行政许可证明、资质证书、强制性认证证书等已经过期失效但申请未获批准）；

（6）没有运行业务连续性管理体系及管理体系或者已不具备运行条件的；

（7）不按相关规定正确引用和宣传获得的认证信息，造成严重影响或后果，或者 ZXB 已要求其纠正但超过 6 个月仍未纠正的；

（8）其他应当撤销认证证书的。

10.8.2 撤销认证证书后，ZXB 应及时收回撤销的认证证书。若无法收回，ZXB 应及时在相关媒体和网站上公布或声明撤销决定。

10.9 ZXB 暂停或撤销认证证书应当在其网站上公布相关信息，同时按规定程序和要求报国家认监委。

10.10 ZXB 有义务和责任采取有效措施避免各类无效的认证证书和认证标志被继续使用。

10.11 ZXB 应制定批准、拒绝、保持、扩大、缩小、暂停、恢复或撤销认证证书或缩小认证范围的规定，并形成文件化的管理制度.

十一、影响认证的变更

11.1 变更地址。

11.2 变更名称：提供新法人执照、变更申请、体系变更申请表、更名后的方针文件、适用性声明、证书制作单、注册审定批准表。技术部将资料审核后报总经理批准。

11.3 扩大、缩小范围：

11.3.1. 单独扩项按照初审资料提供、填写和审查。

11.3.2. 结合监督按照监督资料提供、填写和审查，但须将扩项内容填在审核计划、审核报告中。

11.4 暂停、撤销后的审核要求：应根据暂停时间长短，由运营部适当增加人日数，并在审核通知单中明示告知组长。

十二、认证证书及认证标志的要求

12.1 认证证书应至少包含以下信息：

（1）获证组织名称、地址和组织机构代码。该信息应与其法律地位证明文件的信息一致；

（2）业务连续性管理体系覆盖的生产经营或服务的地址和业务范围。若认证的业务连续性管理体系覆盖多场所，表述覆盖的相关场所的名称和地址信息，该信息应与相应的法律地位证明文件信息一致；

（3）业务连续性管理体系及管理体系符合业务连续性管理体系标准的表述；

（4）证书编号；

（5）ZXB 名称；

（6）证书签发日期及有效期的起止年月日。

对初次认证以来未中断过的再认证证书，可表述该获证组织初次获得认证证书的年月日。

（7）相关的认可标识及认可注册号（适用时）；

（8）证书查询方式。ZXB 除公布认证证书在 ZXB 网站上的查询方式外，还应当在证书上注明：“本证书信息可在国家认证认可监督管理委员会官方网站（www.cnca.gov.cn）上查询”，以便于社会监督。

12.2 认证证书有效期最长为 3 年。

12.3 ZXB 建立证书信息披露制度。除向申请组织、认证监管部门等执法监管部门提供认证证书信息外，还应当根据社会相关方的请求向其提供证书信息，接受社会监督。

12.4 认证要求变更

认证要求变更时，ZXB 及时将认证要求变更的文件发给所有相关的获证组织，同时将认证要求的变更信息通过网络向社会公告。ZXB 根据认证要求变更的性质和内容，采取适当方式对获证组织实施变更后的认证要求有效性的验证，如文件审查、现场补充审核。ZXB 最终根据以上步骤确认认证要求变更后获证组织的证书有效性。

12.5 认证标志要求

a)获证客户在传播媒介(如互联网、宣传册或广告)或其他文件中引用认证状态时，应符合 ZXB 的要求。

b）使用 ZXB 的认证标志，需向 ZXB 提出申请。在使用时，其图案必须按照 ZXB 提供的图案的比例放大或缩小，并且做到颜色一致。未经 ZXB 许可不得使用认证标志；

c）不得在任何资料中有关于其认证资格的误导性说明； d）不得以误导性方式使用认证文件或其任何部分；

e）不得利用管理体系认证证书和相关文字、符号，暗示或误导公众认为认证证书覆盖 范围外的管理体系、产品或服务、过程、活动和场所获得 ZXB 的认证；

f）宣传认证结果时不得损害 ZXB 的声誉和（或）使认证制度声誉受损，失去公众信任；

g）不得擅自更改证书内容；

h）不得伪造、涂改、出借、出租、转让、倒卖、部分出示、部分复印证书；

i）获证客户应妥善保管好认证证书，以免丢失、损坏；

j）获证客户的管理体系若发生重大变化时，应及时报告 ZXB ，接受 ZXB 的调查或监督检查。对经监督检查不合格者，不得继续使用认证证书；

k）在认证范围被缩小时，应及时修改所有的广告宣传材料；

l）认证证书被暂停期间，相应的认证领域的管理体系认证暂时无效。认证客户应停止 使用认证证书和认证标志，直到造成暂停的问题得到解决。如果客户在规定的时限内未能解决造成暂停的问题，ZXB 将撤销或缩小相应领域的认证范围；

m）证书被 ZXB 撤销，获证客户应按 ZXB 的要求将证书交还给 ZXB ，并同时使用所有引用认证资格的广告材料。停止在文件、网站、广告和宣传资料中或广告宣传等商业活动，以 及在工作场所、销售场所展示认证证书；

n）不应允许其标志被获证客户用于实验室检测、校准或检验的报告或证书；

o）标志不应用于产品或产品包装之上，或以任何其它可解释为表示产品符合性的方式 使用；注：产品包装的判别标准是其可从产品上移除且不会导致产品分裂、破裂或损坏。

p）认证证书和认证标志的使用应符合规定；

q）认证标志使用时可以等比例放大或缩小，但不允许变形、变色；

r）证书持有人应对认证证书和认证标志的使用和展示进行有效的控制。

十三、信息通报

获证组织应建立向 ZXB 通报最新信息的程序，并及时通报顾客的重大投诉、国家监督检查结果、重大事故及组织变更的各种信息等变更信息包括(但不限于)以下:法律地位、经营状况、组织状态或所有权取得的行政许可资格、强制性认证或其他资质变更;组织和管理层(如关键的管理、决策或技术人员);联系地址和场所获证业务连续性管理体系覆盖的范围;业务连续性管理体系和重要过程的重大变更。

十四、受理申诉和投诉

获证组织对认证决定有异议时，ZXB 应接受获证组织申诉并且及时进行处理，在 60 日内将处理结果形成书面通知交获认证组织。书面通知应当告知获证组织，若认为 ZXB 未遵守认证相关法律法规或本规则并导致自身合法权益受到严重侵害的，可以直接向所在地认证监管部门或国家认监委投诉，也可以向相关认可机构投诉。

十五、记录管理

15.1 ZXB 应当建立认证纪录保持制度，记录认证活动全过程并妥善保存。

15.2 记录应当真实准确以正式认证活动得到有效实施。保存时间至少应当与认证证书有

效期一致。

15.3 记录可以用纸质或电子文档的方式加以保存。

附录 A：业务连续性管理体系认证审核时间表

有效人数	审核时间（第 1 阶段 + 第 2 阶段，天）
1 - 50	1.5
51- 100	2.5
101 - 150	3.5
151 - 200	4.5
>200	遵循上述递进规律

注：可根据因企业规模、复杂程度实际情况调整。

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