编号：SEC/GZ-01-BCMS-2021

业务连续性管理体系

认证实施规则

第 1.1 版

2021 年 10 月 28 日发布　　2021 年 10 月 28 日实施

2025 年 6 月 3 日修订

前　　言

为了保证东南标准认证中心业务连续性管理体系认证工作顺利开展，确保认证各项工作符合相关文件要求，以及中心质量手册、程序文件汇编等的要求，使各项认证活动得以规范有序进行，制定本实施规则。

制定单位：　福建东南标准认证中心有限公司

主要起草人：李东山、杨瑾、陈芳燕、吴晓丹

验收人员：令狐菲、叶春梅、邓霄、蔡有坤、洪城春、张孙现、戴浩亮

批准人员：令狐菲

目录

1 目的和适用范围

业务连续性管理体系（BusinessContinuityManagementSystems，BCMS）是组织整体管理体系的一个部分，用于建立、实施、运行、监视、评审、保持和改进组织自身业务连续性，是识别对组织的潜在威胁以及这些威胁一旦发生可能对业务运行带来的影响的一整套管理过程。该认证的实施是基于国际标准 GB/T30146/ISO22301。

GB/T30146/ISO22301 是建立和维护业务连续性管理体系的标准，为策划、建立、实施、运行、监视、评审、保持和持续改进一个文件化的业务连续性管理体系规定了要求，用以实施保护，减少中断事件发生的可能性，以及当中断事件发生时准备、响应并恢复。

本实施规则可用于评估一个组织满足自身连续性需求和要求的能力，适用于各种类型、规模和特性的组织或组织的一部分（包括大、中、小型从事工业，商业，公共和非盈利等所有规模和类型的组织）所建立的业务连续性管理体系，包括但不限于对业务连续性要求较高的银行、证券等金融机构；制造业；软件和信息技术服务企业等，适用范围取决于组织的运行环境和复杂性。

2 规范性引用文件及认证依据

2.1 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本实施规则。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

ISO22301:2019 安全与韧性 业务连续性管理体系要求

GB/T 30146 安全与韧性 业务连续性管理体系 要求

2.2 认证依据

GB/T 30146 安全与韧性 业务连续性管理体系 要求

3 初次认证程序

3.1 受理认证申请

3.1.1 中心将向申请组织至少公开以下信息：

（1）本规则的完整内容。

（2）认证证书样式及使用规定。

（3）对认证过程的申投诉规定。

（4）维持认证证书有效性及变更的各项事宜。

注：以上内容同其他管理体系。

3.1.2 申请组织在申请时，至少应提交以下资料：

（1）认证申请书，申请书包括申请认证所涉及的各种运营管理活动范围。

（2）法律地位的证明文件的复印件。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）管理体系覆盖的活动所涉及法律法规要求的行政许可证明、资质证书、强制性认证证书等的复印件。

（4）已通过的其他体系认证(如有，提供复印件)。

（5）管理体系成文信息（适用时）。

3.1.3 申请评审

中心将对申请组织提交的申请资料进行评审，根据申请认证的活动范围及场所、员工人数、完成认证所需时间和其他影响认证活动的因素，综合确定是否有能力受理认证申请。

对被执法监管部门责令停业整顿或在“全国企业信用信息公示系统”中被列入“严重违法企业名单”的申请组织，中心将不受理其认证申请。

3.1.4 对符合 3.1.2、3.1.3 要求的，中心将决定受理认证申请；对不符合上述要求的，中心将通知申请组织补充和完善，或者不受理认证申请。

3.1.5 签订认证合同

在实施认证审核前，中心将与申请组织订立具有法律效力的书面认证合同，合同至少包含以下内容：

（1）申请组织获得认证后持续有效运行管理体系的承诺。

（2）申请组织对遵守相关法律法规，协助监管部门的监督检查，对有关事项的询问和调查如实提供相关材料和信息的承诺。

（3）申请组织承诺获得认证后发生以下情况时，应及时向本中心通报：

Ⅰ发生重大质量、环境、安全、食品安全等事故。

Ⅱ相关情况发生变更，包括：法律地位、生产经营状况、组织状态或所有权变更；取得的行政许可资格、强制性认证或其他资质证书变更；法定代表人、体系负责人变更；业务连续性过程活动所涉及的

工作场所变更；管理体系覆盖的活动范围变更；管理体系和重要过程的重大变更等。

III 出现影响管理体系运行的其他重要情况。

（4）申请组织承诺获得认证后正确使用认证证书和有关信息，证书范围只涉及审核地址所涉及的业务连续性过程活动。

（5）拟认证的管理体系覆盖的业务连续性过程活动。

（6）在认证实施过程及认证证书有效期内，中心和申请组织各自应当承担的责任、权利和义务。

（7）认证服务的费用、付费方式及违约条款。

3.2 审核策划

3.2.1 认证时间

3.2.1.1 为确保认证的完整有效，中心将以附录 A 所规定的审核时间为基础进行安排，但可根据申请组织管理体系覆盖的范围的复杂程度、体系覆盖范围内的有效人数等情况，核算并拟定完成认证工作需要的时间。在特殊情况下，可以减少认证时间，但减少的时间不超过附录 A 所规定的认证时间的 30％。

3.2.1.2 整个认证时间中，现场认证时间不应少于总认证时间的 80％，也可采用远程认证的方式获取认证证据，但不超过现场认证时间的 30%，且应保存相应的证据，如音频、视频、电子文件等，使用远程审核的条件应符合中心相关的规定要求。

3.2.2 审核组

3.2.2.1 中心将选择具备相关能力的审核员组成审核组，必要时可以选择技术专家参加审核组。审核组中的审核员承担认证任务和责任。

3.2.2.2 技术专家主要负责提供认证过程的技术支持，不作为审核员实施认证，不计入认证时间，其在认证过程中的活动由审核组中的审核员承担责任。

备注：**审核员应具备 CCAA 确认的资格**，应理解 ISO22301:2019《安全与韧性 业务连续性管理体系 要求》的术语及每项条款的内容和要求，如风险管理的基本原理和常用风险评估技术及其在业务连续性管理中的应用、业务影响分析的基本方法及其在业务连续性管理中的应用、灾备技术、业务连续性管理的基本过程、业务连续性计划的编制与演练等，理解业务连续性管理体系与其他管理体系的关系，并了解我国相关的法律法规体系的构成、安全与恢复相关法律法规要求及其与业务连续性管理体系的关系，了解其在审核中的应用，了解国家认证认可法规、规章要求等。

3.2.3 审核计划

3.2.3.1 中心将为每次认证制定书面的审核计划。审核计划至少包括但不限于以下内容：认证目的，认证准则，认证范围，现场认证的日期和场所，现场认证持续时间，审核组成员。

3.2.3.2 如果管理体系覆盖范围包括在多个场所进行相同或相近的活动，且这些场所都处于申请组织授权和控制下，中心可以在审核过程中对这些场所进行抽样，但应根据相关要求实施抽样，以确保对所抽样本进行的审核对体系包含的所有场所具有代表性。如果不同场所

的活动存在明显差异、或不同场所间存在可能对业务连续性管理有显著影响的区域性因素，则不能采用抽样审核的方法，将逐一到各现场进行审核，查看业务连续性管理和控制情况。

3.2.3.4 在审核活动开始前，审核组应将审核计划交申请组织确认，遇特殊情况临时变更计划时，应及时将变更情况通知申请组织，并协商一致。

3.3 实施审核

3.3.1 审核组将按照审核计划的安排完成审核工作。除不可预见的特殊情况外，审核过程中不得更换审核计划确定的审核员。

3.3.2 审核组将会同申请组织按照程序召开首、末次会议，申请组织的最高管理者及各职能部门负责人员，包括体系负责人均应参加会议。参会人员应签到，审核组应当保留首、末次会议签到表。当申请组织要求时，审核组成员应向申请组织出示身份证明文件。

注：2021 年 12 月 1 日起，首末次会议签到将**参照**“认监委关于认证人员现场审核网络签到监管系统上线运行的通知（国认监【2021】3 号）”及中心相关的要求进行，如拍照。

3.3.3 审核过程及环节

初次认证审核，分为第一、二阶段实施审核。

3.3.3.1 第一阶段审核

（1）结合申请组织的业务连续性管理实施情况，确认与管理体系成文信息描述的一致性。

（2）结合现场情况，认证申请组织理解和实施 ISO22301:2019《安全与韧性 业务连续性管理体系 要求》标准要求的情况，评价管理体系运行过程中是否实施了内部审核与管理评审，确认管理体系是否已运行并且超过 3 个月。

（3）与申请组织讨论确定第二阶段审核安排。对管理体系成文信息不符合现场实际、相关体系运行尚未超过 3 个月或者无法证明超过 3 个月的，以及其他不具备二阶段审核条件的，不应实施二阶段审核。

在下列情况，第一阶段审核可以不在申请组织现场进行，但应记录未在现场进行的原因：

（1）申请组织已获本中心颁发的其他有效认证证书，本中心已对申请组织质量管理体系有充分了解。

（2）有充足的理由证明申请组织的生产经营或服务的技术特征明显、过程简单，通过对其提交文件和资料的审查可以达到第一阶段审核的目的和要求。

除以上情况之外，第一阶段审核应在受审核方的生产经营或服务现场进行。

审核组应将第一阶段审核情况形成书面文件告知申请组织。对在第二阶段审核中可能被判定为不符合项的重要关键点，要及时提醒申请组织特别关注。

3.3.3.2 第二阶段审核

第二阶段审核应当在申请组织现场进行。重点是审核质量管理体系符合 ISO22301:2019《安全与韧性 业务连续性管理体系 要求》标准要求和有效运行情况，应至少覆盖以下内容：

（1）确认申请组织建立的管理体系覆盖的活动内容和范围、体系覆盖范围内有效人数、过程和场所，遵守适用的法律法规及强制性标准的情况。

（2）结合申请组织管理体系的特点，并结合其他因素，科学确定重要审核要点。

（3）重点是审核管理体系符合 ISO22301:2019《安全与韧性 业务连续性管理体系 要求》标准要求和有效运行情况，包括策划、建立、实施、运行、监视、评审、保持和持续改进业务连续性管理体系，是否进行了内部审核和管理评审，并核查申请组织实际工作文件、记录是否真实，对于审核发现的真实性存疑的证据应予以记录并在做出认证结论及认证决定时予以考虑。

主要审核要点及审核方法

序号	管理体系要求	对应标准条款	认证要点和认证方法
1	理解组织及其环境	4.1	组织是否确定了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，并在建立、实施和保持组织的BCMS时，这些情况是否已被考虑。 组织是否识别以下内容并形成文件： a)组织的活动、职能、服务、产品、合作方、供应链、与相关方的关系以及与中断事件有关的潜在影响； b)业务连续性方针和组织目标以及其他方针，包括其总体风险管理策略间的联系； c)组织的风险偏好。 在构建环境时，组织是否： 1)阐明其目标，包括与业务连续性有关的目标； 2)确定会造成增加风险不确定性的外部和内部因素； 3)根据风险偏好设定风险准则； 4)确定 BCMS 的目的。

2	理解相关方的需求和期望	4.2	
3	总则	4.2.1	在建立 BCMS 时，组织是否确定： a)与 BCMS 有关的相关方； b)这些相关方的要求（即阐明的、通常隐含的或强制性的需求和期望）。
4	法律和法规要求	4.2.2	组织是否建立、实施和维护保持了一个程序（或多个程序）用以识别、利用和评估与业务运行、产品和服务，以及相关方连续性要求相关的适用的法律和法规要求。 组织是否确保在建立、实施和维护保持其 BCMS 时考虑这些适用的法律、法规和经组织认同的其他要求。 组织是否将这些信息形成文件并保持更新，是否与受影响的员工和其他相关方沟通新立或变更的法律、法规和其他要求。
5	总则	4.3.1	组织是否通过确定 BCMS 的边界和适用性来建立其范围。 组织在确定范围时是否考虑： —在 4.1 中涉及的外部和内部因素； —在 4.2 中涉及的要求。 该范围是否为可获得的存档信息。
6	BCMS 的范围	4.3.2	组织是否： a)确定组织中被包含在 BCMS 范围内的部分； b)在考虑组织的任务、目标、内部和外部职责（包括与相关方有关的）以及法律和法规方面的责任下，建立 BCMS 的要求； c)识别 BCMS 范围内的产品、服务和所有相关活动； d)考虑相关方的需求和利益，例如客户、投资者、股东、供应链、公共和/或社区的投入和需求、期望和利益（如适用时）； e)按照组织规模、性质和复杂性确定合适的 BCMS 范围。 在定义范围时，组织是否将删减理由形成文件，任何删减应不影响组织提供达到 BCMS 要求的业务和运行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。
7	业务连续性管理体系	4.4	组织是否根据本标准的要求建立、实施、保持和持续改了进 BCMS，包括必需的过程及其相互作用。
8	领导力	5	
9	领导力和承诺	5.1	最高管理者是否通过以下方面展示对 BCMS 的领导力和承诺； a)确保建立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)确保将 BCMS 的要求集成到组织的业务过程中； c)确保 BCMS 必需的资源是可用的； d)传达有效业务连续性和遵守 BCMS 要求的重要性； e)确保 BCMS 达到其预期结果； 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)支持其它的管理角色，以展现他们在其职责范围内的领导力和承诺。 注：本文件中的“业务”可从广义上解释为对组织存在具有核心价值的活动。
10	方针	5.2	

11	建立管理方针	5.2.1	最高管理层是否建立业务连续性方针，该方针是否： a)与组织意图相适宜； b)为设定服务管理目标提供框架； c)包括对满足适用要求的承诺； d)包括持续改进 BCMS 的承诺。
12	沟通管理方针	5.2.2	管理方针是否： a)形成文档化信息并可用； b)在组织内得到沟通； c)适当时，对相关方可用。 d）在规定的时间间隔内或当重大变化发生时对持续适用性进行评审。 组织是否保留了业务连续性方针方面的存档信息。
13	角色、责任和权力	5.3	最高管理层是否确保与管理体系相关角色的责任和权限得到分配和沟通。 最高管理层是否分配了责任和权限，以： a)确保管理体系符合本标准的要求； b)向最高管理者报告管理体系绩效。 注：最高管理层也可为组织内报告管理体系绩效，分配责任和权限。
14	规划	6	
15	应对风险和机会的措施	6.1	
16	确定风险和机会	6.1.1	在规划 BCMS 时，组织是否考虑 4.1 提到的问题和 4.2 提到的要求，并确定需要应对的风险和机会； a)确保 BCMS 能达到其预期结果； b)预防，或减少不良影响； c)实现持续改进。
17	应对风险和机会	6.1.2	组织是否计划： a)应对这些风险和机会的措施； b)如何： 1）将这些措施集成和实现到 BCMS 过程中； 2）评价这些措施的有效性。 注：风险和机会与管理体系的有效性有关。与业务中断相关的风险在 8.2 中说明。
18	业务连续性目标和实现计划	6.2	
19	建立业务连续性目标	6.2.1	最高管理者是否确保制定业务连续性目标并将其传达给组织内具有相关职责的人员。 业务连续性目标是否： a)与业务连续性方针保持一致； b)考虑组织为实现目标所能接受的产品和服务的最低级别； c)是可测量的； d)考虑适用的要求； e)进行监视和适当的更新。 组织是否保留与业务连续性目标有关的存档信息。

20	确定业务连续性目标	6.2.2	为了达到业务连续性目标，组织是否确定： — 谁将负责； — 要做什么； — 需要什么资源； — 什么时候完成； —怎样评估结果。
21	BCMS 变更规划	6.3	当组织确定需要变更 BCMS 时，包括第 10 章中确定的变更，变更是否按计划进行。 组织是否考虑： a)变更的目的和它们可能的后果； b)BCMS 的完整性； c)资源可能性； d)责任和权力的分配或再分配。
22	支持	7	
23	资源	7.1	组织应确定并提供建立、实现、维护和持续改进管理体系所需的资源。
24	能力	7.2	组织是否： a)确定在组织控制下从事会影响组织相关绩效的工作人员的必要能力； b)确保上述人员在适当的教育、培训或经验的基础上能够胜任其工作； c)适用时，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)保留适当的文件化信息作为能力的证据。 注：适用的措施可包括，例如针对现有雇员提供培训、指导或重新分配；雇佣或签约有能力的人员。
25	意识	7.3	在组织管理下的工作人员是否了解： 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)在发生中断事件时各自的角色。
26	沟通	7.4	组织是否确定与 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。 组织是否建立、实施和维护保持一个程序（或多个程序）以实现： — 与组织的相关方和雇员之间的内部沟通； — 与顾客、合作伙伴合作方、当地社区和包括媒体在内的其他相关方的外部沟通； — 收集、存档和回应来自相关方的信息； — 在适当的情况下，采用和纳入国家或地区的威胁预警体系（或类似的体系），供规划和运行使用； — 发生中断事件时，确保沟通手段的可用性； — 在合适的情况下，促进与相关政府机构进行有组织的沟通，确保多个响应机构和人员之间的协作； — 对于正常通信中断期间所需要的备用通信方式进行操作和测试。 注：关于应对事件的更多沟通要求，参见 8.4.3。
27	文件化信息	7.5	

28	总则	7.5.1	组织的管理体系是否包括： a)本标准要求的文件化信息； b)为管理体系的有效性，组织所确定的必要的文件化信息。 注：不同组织有关管理体系文件化信息的详略程度可以是不同的，这是由于： 1)组织的规模及其活动、过程、产品和服务的类型； 2)过程及其相互作用的复杂性； 3)人员的能力。
29	创建和更新	7.5.2	创建和更新文件化信息时，组织是否确保适当的： a)标识和描述（例如标题、日期、作者或引用编号）； b)格式（例如语言、软件版本、图表）和介质（例如纸质的、电子的）； c)对适宜性和充分性的评审和批准。
30	文件化信息的控制	7.5.3	管理体系及本标准所要求的文件化信息是否得到控制，以确保： a)在需要的地点和时间，是可用的和适宜使用的； b)得到充分的保护（如避免保密性损失、不恰当使用、完整性损失等）。 为控制文件化信息，适用时，组织是否强调以下活动： a)分发，访问，检索和使用； b)存储和保护，包括保持可读性； c)控制变更（例如版本控制）； d)保留和处理。 组织确定的为规划和运行管理体系所必需的外来的文件化信息，是否得到适当的识别，并予以控制。 注：访问隐含着仅允许浏览文件化信息，或允许和授权浏览及更改文件化信息等决定。
31	运行	8	
32	运行的规划和控制	8.1	组织是否通过以下方式策划、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，在必要的范围内留存保留存档信息。 组织是否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。 如有外包，组织采取何种措施，确保外包过程的受控。
33	业务影响分析和风险评估	8.2	
34	总则	8.2.1	组织是否： a)实施和保持系统化的过程分析中断的影响和评估中断的风险； b)定期或在组织内或其运行环境有重大变更时，评审业务影响分析和风险评估。 注：组织确定业务影响分析和风险评估的执行顺序。

35	业务影响分析	8.2.2	组织是否使用分析业务影响的过程来确定业务连续性优先级和要求。这个过程应： a)明确与组织环境相关的影响类别和准则； 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的影响； d)识别不恢复这些活动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)中识别时间范围内，制定以指定的最低可接受生产能力恢复中断活动的优先时间表； 注 2：该时间范围可称为“恢复时间目标（RTO）”。 f)使用此分析确定优先活动； g)确定支持优先活动的必备资源； h)确定包括合作方和供应商在内的依赖关系，以及优先活动的相互依赖关系。
36	风险评估	8.2.3	组织是否建立、实施和保持一个正式的形成文件的风险评估过程。该过程能系统地识别、分析和评价中断事件给组织带来的风险。 注：这一过程可以参照 ISO 31000 来制定。 组织应： a)识别中断对于组织的优先活动以及过程、系统、信息、人员、资产、外包方和其他支持资源所带来的风险； b)系统地分析风险； c)评价哪种中断风险需要处理； d)识别与业务连续性目标相符以及与组织的风险偏好一致的处理措施。 注：组织必须意识到特定金融或政府部门会对这些风险披露的信息程度有要求。另外，特定的社会需求也要求在适当程度上共享此类信息。
37	业务连续性策略和方案	8.3	
38	总则	8.3.1	根据业务影响分析和风险评估的结果，组织是否确定和选择考虑中断前、中断中和中断后的业务连续性策略选项。业务连续性策略应由一个或多个解决方案组成。
39	识别策略和方案	8.3.2	组织是否基于其在以下方面的程度识别策略和方案： a)满足连续和恢复优先活动的要求（在确定的时间范围和约定的能力内）； b)保护组织的优先活动； c)降低中断可能性； d)缩短中断的时间； e)限制中断对组织的产品和服务的影响； f)提供足够的资源。
40	选择策略和方案	8.3.3	组织是否基于其在以下方面的程度选择策略和方案： a)满足连续和恢复优先活动的要求（在确定的时间范围和约定的能力内）； b)考虑组织可能承受或不可承受风险的类型和数量； c)考虑相应的成本和收益。

41	资源要求	8.3.4	组织是否为执行所选择的策略设置资源要求。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、工作环境和配套设施； d) 设施、设备和耗材； e) 信息通信技术系统； f) 交通工具； g) 资金； h) 合作方和供应商。
42	方案实施	8.3.5	组织是否实施并保持选定的业务连续性方案，以便在需要时启用它们。
43	业务连续性计划和程序	8.4	
44	总则	8.4.1	组织是否以业务影响分析中已识别的恢复目标为基础，建立、实施和保持业务连续性程序，来管理中断事件和保证活动的连续性。 组织是否将程序（包括必要的安排）形成文件，以确保活动的连续性和对中断事件的管理。 程序是否： a)建立适当的内部和外部沟通协议； b)针对业务中断期间需要采取的紧急步骤进行详细规定； c)灵活地应对非预期的威胁和不断变化的内部和外部环境； d)关注可能导致潜在运行中断的事态影响； e)在已提出的假设和在相互依赖关系分析的基础上进行开发； f)通过实施适当的减缓策略有效地将后果最小化。
45	响应结构	8.4.2	组织是否利用对事件管理有职责、权力和能力的人员来建立并实施中断事件响应程序和管理机制，并将其形成文件。 响应机制是否： a)识别开始采取正式响应措施的影响阀值； b)评估中断事件的性质和范围以及潜在影响； c)启动适当的业务连续性响应； d)具备用于启动、运行、协调和沟通的响应过程和程序； e)具备可用于支持过程和程序的资源来处理中断事件以减轻影响； f)与相关方、权力机构以及媒体进行沟通。 组织是否采取人身安全第一优先的原则，通过与相关方进行协商来决定是否就其重大风险和影响进行外部沟通，并将其决定形成文件。如果决定要进行外部沟通，组织应建立和实施针对此类与外部以及在适当情况下与媒体进行沟通、预警的程序。

46	预警和沟通	8.4.3	组织是否建立、实施和保持程序以： a)发现事件； b)对事件进行日常监视； c)进行组织内部沟通并接收、存档和响应来自相关方的反馈； d)对国家或地区的威胁预警体系（或类似的体系）进行接收、记录和响应； e)确保在中断事件期间沟通手段的可用； f)为同应急响应人员进行有序的沟通提供便利； g)记录与事件、采取的措施和所做的决定相关的重要信息，适当时，下列事项应被考虑和实施： —向将要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； —确保多个响应组织和人员之间的协同； —通信设施的运行。 沟通和预警程序是否定期进行演练总结，有无形成文件化信息。
47	业务连续性计划	8.4.4	组织是否建立响应中断事件，以及如何在预定的时间内继续或恢复其活动的文件化程序。此程序是否能针对使用者提出要求。 业务连续性计划是否全部包含： a)确定在事件发生时和发生后相关人员和团队的角色和职责； b)一个启动响应的过程； c)处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)响应中断的策略、战术和执行方案的选择； 3)防止进一步损失或优先活动无法执行； d)如何以及在何种情况下组织与员工及其亲属、关键相关方、以及紧急联络人进行沟通； e)组织将如何在预定的时间里继续或恢复其优先活动； f)事件发生后，组织的媒体响应的详细说明包括： 1)沟通策略； 2)首选的媒体接口； 3)起草媒体声明的方针或模板； 4)合适的发言人。 g)事件一旦结束后的退出过程。 每个计划应确定： —目的和范围； —目标； —启动的准则和程序； —实施程序； —角色、职责和职权； —沟通的要求和程序； —内部和外部的依赖关系和相互作用； —资源的要求； —信息流和存档过程。 每个计划是否在需要它的时间和地点可使用和可得到。
48	恢复	8.4.5	组织是否有用以在事件发生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。

49	演练项目集	8.5	组织是否演练和测试其业务连续性程序，以确保它们和业务连续性目标相一致。 组织进行的演练和测试是否： a)与 BCMS 的范围和目标保持一致； b)基于适当的，有周密计划以及明确目的和目标的场景； c)持续实施并召集相关方对其整套业务连续性安排进行验证； d)最大限度降低运行中断的风险； 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。 组织是否按照其演练和测试的结果，以实施变更和改进。
50	业务连续性文档和能力评价	8.6	组织是否： a)评价业务影响分析、风险评估、策略、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、事故报告和绩效评价进行评价； c)对相关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法规要求、行业最佳实践，以及其是否符合自己的业务连续性方针和目标； e)及时更新文档记录和程序。 这些评价是否在事故后或启用后，和有重大变更发生时，按计划间隔进行。
51	绩效评价	9	

52	监视、测量、分析和评价	9.1	**一、总则** 组织是否确定： 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)何时进行监视和测量； d)何时进行监视和测量结果的分析和评价。 组织是否保留适当的存档信息作为结果的证据。 组织是否评价 BCMS 的绩效和 BCMS 的有效性。 另外，组织是否： — 在不符合项发生前采取必要措施以应对不利的趋势和结果； — 保留相关的存档信息作为结果的证据。 用于监视绩效的程序应提供： — 制定符合组织需求的绩效指标； — 对组织的业务连续性方针、目标和指标完成程度的监视； — 保护其优先级活动的过程、程序和职能的绩效； — 对本标准和业务连续性目标符合性的监视； — 对 BCMS 缺陷绩效的历史证据的监视； — 记录监视和测量的数据和结果，为采取后续纠正措施提供便利。 注：缺陷绩效包括不符合项、未遂事件、错误警报和实际发生的事件。 **二、业务连续性程序的评价** a)组织是否对其业务连续性程序和能力进行评价，以确保其持续的适宜性、充分性和有效性； b)这些评价是否通过定期评审、演练、测试、事件总结报告和绩效评估来进行。重大变更应在一个（或多个）程序中得到及时的反映； c)组织是否定期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； d)组织是否按计划的时间间隔或者当组织或运营环境出现重大变化时进行评估。 当中断事件发生并导致业务连续性程序的启动时，组织是否进行事后评审并记录其结果。
53	内部审核	9.2	组织是否按计划的时间间隔进行内部审核，以提供信息，确定管理体系： a)是否符合; 1)组织自身对管理体系的要求； 2)本标准的要求。 b)是否得到有效实现和维护。 组织是否： c)规划、建立、实现和维护审核方案（一个或多个），包括审核频次、方法、责任、规划要求和报告。审核方案应考虑相关过程的重要性和以往审核的结果； d)定义每次审核的审核准则和范围； e)选择审核员并实施审核，确保审核过程的客观性和公正性； f)确保将审核结果报告至相关管理层； 保留文件化信息是否作为审核方案和审核结果的证据。

54	管理评审	9.3	最高管理者层是否按计划的时间间隔评审组织的 BCMS，以确保其持续适宜性、充分性和有效性。 管理评审是否考虑以下内容： a)以往管理评审措施的状态状况； 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)持续改进的机会。 管理评审应是否考虑到组织的绩效，包括： —以往管理审核的后续跟进； —改变 BCMS 的变更需求，包括方针和目标； —改进机会； —BCMS 的审核和评审的结果，包括对关键供应商和合作伙伴合作方（适用时）； —可能用于改进组织的 BCMS 绩效和有效性的技术、产品或程序； —纠正措施的状态； —演练和测试的结果； —在以往的风险评估中没有引起足够重视的风险和问题； —无论是 BCMS 范围内部还是外部的任何能对 BCMS 的产生影响的变化； —方针的充分性； —改进建议； —在中断事件中采取的措施以及从中吸取的经验； —新出现的良好实践和指导。 管理评审的输出是否包括与持续改进机会相关的决定以及可能存在的对 BCMS 变更的需求，并且还包括： a)对 BCMS 范围的变化； b)对 BCMS 有效性的改进； c)对风险评估、业务影响分析、业务连续性计划和相关程序的更新； d)对用以响应可能对 BCMS 产生影响的内部或外部事件的程序和控制措施的修改，包括对下列事项的变更： 1)业务和运行要求； 2)风险降低和安全要求； 3)运行条件和过程； 4)法律和法规要求； 5)合同义务； 6)风险级别和/或风险接受准则； 7)资源需求； 8)资金和预算要求； e)对控制措施的有效性进行测量的方式。 组织是否保留存档信息作为管理评审结果的证据。 组织是否： — 向相关方传达管理评审的结果； — 针对这些结果采取适当的措施。
55	改进	10	

56	不符合和纠正措施	10.1	当发生不符合时，组织是否： a)对不符合做出反应，适用时： 1)采取措施，以控制并予以纠正； 2)处理后果； b)通过以下活动，评价采取消除不符合原因的措施的需求，以防止不符合再发生，或在其他地方发生：评审不符合；确定不符合的原因；确定类似的不符合是否存在，或可能发生； c)实现任何需要的措施； d)评审任何所采取的纠正措施的有效性； e)需要时，更新在策划期间确定的风险和机遇； f)必要时，对管理体系进行变更。 纠正措施是否与所遇到的不符合的影响相适合。 组织是否保留了文件化信息，以作为以下方面的证据： g)不符合的性质及所采取的任何后续措施； h)任何纠正措施的结果。
57	持续改进	10.2	组织是否持续改进 BCMS 的适宜性、充分性和有效性，基于定性和定量的方法。 组织是否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 有关的需要或机会，这些需要或机会应作为持续改进的一部分加以解决。 注：组织可以使用 BCMS 的过程来实现改进，如领导力、规划和绩效评价。

3.3.4 发生以下情况时，审核组应向本中心报告，经本中心同意后可终止审核。

（1）申请组织对认证活动不予配合，认证活动无法进行。

（2）申请组织实际情况与申请材料有重大不一致。

（3）其他导致认证程序无法完成的情况。

3.4 审核报告

3.4.1 审核组应对审核活动形成书面审核报告，由审核组组长签字。审核报告应准确、简明和清晰地描述审核活动的主要内容，至少包括以下内容：

（1）申请组织的名称和地址。

（2）申请组织业务连续性过程活动的范围和场所。

（3）审核的类型、准则和目的。

（4）审核组组长、审核组成员及其他个人信息，如技术专家。

（5）审核活动的实施日期和地点，包括固定现场和临时现场；对偏离审核计划情况的说明，包括对审核风险及影响审核结论的不确定性的客观陈述。

（6）叙述从 3.3 条列明的程序及各项要求的审核工作情况，其中：对 3.3.3 条的各项审核要求应逐项描述或引用审核证据、审核发现和审核结论，并对实现情况进行审核。

（7）识别出的不符合项。

（8）审核组对是否通过审核的意见建议。

3.4.2 中心将保留用于证实审核报告中相关信息的证据。

3.4.3 中心将在作出认证决定后 7 个工作日内将审核报告提交申请组织，并保留签收或提交的证据。

3.4.4 对终止审核的项目，审核组应将已开展的工作情况形成报告，中心将此报告及终止审核的原因提交给申请组织，并保留签收或提交的证据。

3.5 不符合项的纠正和纠正措施及其结果的验证

3.5.1 对审核中发现的不符合项，中心将要求申请组织分析原因，并提出纠正和纠正措施。对于严重不符合，应要求申请组织在最多不超过 3 个月期限内采取纠正和纠正措施。中心将对申请组织所采取的纠正和纠正措施及其结果的有效性进行验证。如果未能在第二阶段结束后 3 个月内验证对严重不符合实施的纠正和纠正措施，则应按 3.6.5 条处理，或者按照 3.3.3 条重新实施审核。

3.6 认证决定

3.6.1 中心将在对审核报告、不符合项的纠正和纠正措施及其结果进行综合评价的基础上，作出认证决定。

3.6.2 认证决定人员应为本中心管理控制下的人员（资格同审核员，详见 3.2.2.2 中备注），审核组成员不得参与对该审核项目的认证决定。

3.6.3 本中心在作出认证决定前将确认如下情形：

（1）审核报告符合本规则第 3.4 条要求，审核组提供的认证报告及其他信息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，中心已评审、接受并验证了纠正和纠正措施的有效性。

①在持续改进管理体系的有效性方面存在缺陷。

②其他严重不符合项。

（3）中心对其他一般不符合项已评审，并接受了申请组织计划采取的纠正和纠正措施。

3.6.4 在满足 3.6.3 条要求的基础上，中心有充分的客观证据证明申请组织满足下列要求的，评定该申请组织符合认证要求，向其颁发认证证书。

（1）申请组织的管理体系符合 ISO22301:2019《安全与韧性 业务连续性管理体系 要求》和适用法律法规要求且运行有效。

（2）申请组织按照认证合同规定履行了相关义务。

3.6.5 申请组织不能满足上述要求或者管理体系存在重大缺陷，不符合 ISO22301:2019《安全与韧性 业务连续性管理体系 要求》标准的要求的，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。

3.6.6 中心在颁发认证证书后，将在 7 个工作日内将认证结果相关信息报送国家认监委及中心网站。

4 监督审核程序

4.1 中心将对持有其颁发的业务连续性管理体系认证证书的组织（以下称获证组织）进行有效跟踪，监督获证组织持续运行管理体系并符合认证要求。

4.2 为确保达到 4.1 条要求，中心将根据获证组织的业务连续性管理和履行情况，确定对获证组织的监督审核的频次。

4.2.1 作为最低要求，初次认证后的第一次监督审核将在上次审核结束之日起 12 个月内进行，之后每年必须接受一次监督至证书有效期止，时间间隔为 10 到 12 个月，最长不超过 12 个月。

特殊情况下，需由获证组织向本中心提出书面申请，说明推迟监督审核时间的理由，经审核管理部许可后可适当延长。监督时间间隔超过 12 个月的视为不能按期接受监督审核，具体按中心的 SEC/CX-08《认证资格变更管理程序》执行。若因疫情等特殊原因造成不能按期监督审核的，视具体情况处理。

4.2.2 超过期限而未能实施监督审核的，应按 6.2 或 6.3 条处理。

4.3 监督审核的时间，应不少于按 3.2.1 条计算认证时间人日数的 1/3。

4.4 监督审核的审核组，应符合 3.2.2 条和 3.3.1 条的要求。

4.5 监督审核也将在获证组织现场进行。

4.6 监督审核时至少应审核以下内容：

（1）上次认证以来管理体系覆盖的活动及影响体系的重要变更及运行体系的资源是否有变更。

（2）按 3.3.3 条要求已识别的重要关键点是否按管理体系的要求在正常和有效运行。

（3）对上次审核中确定的不符合项采取的纠正和纠正措施是否继续有效。

（4）管理体系覆盖的活动涉及法律法规规定的，是否持续符合相关规定。

（5）是否建立有效的改进机制。

（6）获证组织对获证资格的引用是否符合中心的相关规定。

（7）是否及时接受和处理投诉，及时制定并实施了有效的改进措施。

4.7 在监督审核中发现的不符合项，中心将要求获证组织分析原因，规定时限要求获证组织完成纠正和纠正措施并提供纠正和纠正措施有效性的证据。

中心将采用适宜的方式及时验证获证组织对不符合项进行处置的效果，如文件评审、现场评审或下次监督审核验证等方式。

4.8 监督审核的审核报告，按 4.6 条列明的认证要求逐项描述或引用审核证据、审核发现和审核结论。

4.9 中心根据监督审核报告及其他相关信息，作出继续保持或暂停、撤销认证证书的决定。

5 再认证程序

5.1 认证证书期满前，若获证组织申请继续持有认证证书，中心将实施再认证，并决定是否延续认证证书。

5.2 中心将按 3.2 条和 3.3.1 条要求组成审核组。按照 3.2.3 条要求并结合历次监督审核情况，制定再认证审核计划交审核组实施。审核时间将不少于按 3.2.1 条计算人日数的 2/3。

5.3 对再认证中发现的不符合项，获证组织将在 30 个工作日内实施纠正与纠正措施，且应在原证书到期前完成对纠正与纠正措施的验证，如超期未完成整改，或在原证书到期前未完成整改的，将按初次认证进行。

5.4 中心将按照 3.6 条要求作出再认证决定。获证组织继续满足认证要求并履行认证合同义务的，向其换发认证证书。

5.5 如果在当前认证证书的终止日期前完成了再认证活动（含不符合整改及验证），中心将换发认证证书，新认证证书的终止日期可以基于当前认证证书的终止日期。新认证证书上的颁证日期将不早于再认证决定日期。

6 暂停、注销或撤销认证证书

6.1 总则

参照中心其他管理体系，按 SEC/CX-08-2014《认证资格变更管理程序》的要求进行。

6.2 暂停证书

6.2.1 获证组织有以下情形之一的，中心将在调查核实后的 5 个工作日内暂停其认证证书。

（1）管理体系持续或严重不满足认证要求，包括对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）获证组织被有关执法监管部门责令停业整顿的。

（4）持有的与管理体系范围有关的行政许可证明、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。

（5）主动请求暂停的。

（6）其他应当暂停认证证书的。

6.2.2 认证证书暂停期不得超过 6 个月。但属于 6.2.1 第（4）项情形的暂停期可至相关单位作出许可决定之日。

6.2.3 中心将暂停认证证书的信息上报国家认监委及中心网站，明确暂停的起始日期和暂停期限，并在暂停通知中要求获证组织在暂停期间不得以任何方式使用认证证书或引用认证信息。

6.3 注销、撤销证书

6.3.1 获证组织有以下情形之一的，中心将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）被国家相关部门列入严重失信企业名单的。

（3）拒绝配合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。

（4）出现重大的质量、环保、安全生产或食品安全等问题的，经执法监管部门确认是获证组织违规造成的。

（5）有其他严重违反法律法规行为的。

（6）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。

（7）没有运行管理体系或者已不具备运行条件的。

（8）不按相关规定正确引用和宣传获得的获证信息，造成严重影响或后果，或者认证机构已要求其纠正但超过 1 个月仍未纠正的。

（9）其他应当撤销认证证书的。

6.3.2 撤销认证证书后，中心将按认证合同的要求，收回撤销的认证证书。若无法收回，中心将在中心网站上公布撤销决定。

6.3.3 认证证书注销是撤销的一种特殊形式，获证客户由于自身原因不想保持认证证书可向本中心提出注销认证证书的书面申请，再由中心办理注销手续。

6.4 变更信息报送

中心将暂停、注销或撤销认证证书的相关信息在国家认监委及中心网站上公布。

6.5 认证合同

不得使用无效的认证证书和获证信息，中心将在认证合同中予以明确。

7 认证证书及认证标志要求

7.1 认证证书至少包含以下信息：

（1）获证组织名称、地址和统一社会信用代码。该信息将与其法律地位证明文件的信息一致。

（2）管理体系覆盖的范围。若认证的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。

（3）管理体系符合 ISO22301:2019《安全与韧性 业务连续性管理体系 要求》标准的表述。

（4）证书编号。

（5）中心名称。

（6）有效期的起止年月日。

证书将注明：获证组织必须定期接受监督审核，并经认证合格此证书方继续有效的提示信息。

（7）证书查询方式。认证证书将包括国家认监委或中心网站上的查询方式上的查询方式，以便于社会监督。

备注：证书名称可根据双方协商的结果，进行适当标注。

7.2 初次认证证书有效期最长为 3 年。再认证的认证证书有效期不超过最近一次有效认证证书截止期再加 3 年。

7.3 中心将建立证书信息披露制度。除向申请组织、监管部门等执法监管部门提供认证证书信息外，社会相关方有请求时，可向其提供证书信息，接受社会监督。

7.4 认证标志的使用应符合中心制订的《认证证书和标志的管理程序》以及公开性文件的要求。

8 与其他管理体系的结合认证

中心暂不考虑与其他管理体系的结合认证，将按单独的管理体系进行认证。

9 受理转换认证证书

中心目前暂不进行获得业务连续性管理体系认证证书的组织申请认证证书的转换。

10 受理组织的申诉

申请组织或获证组织对认证决定有异议时，中心将接受申诉并且及时进行处理，在 30 日内将处理结果形成书面通知送交申诉人。若认为中心未遵守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，可以直接向所在地市场监督管理局或其他法律机关投诉。

11 认证记录的管理

11.1 中心将建立认证记录保持制度，记录认证活动全过程并妥善保存，包括电子版记录。

11.2 记录将真实准确以证实认证活动得到有效实施。记录资料将使用中文，保存时间至少应当与认证证书有效期一致。

11.3 以电子文档方式保存记录的，将采用不可编辑的电子文档格式。

11.4 所有具有相关人员签字的书面记录，可以制作成电子文档保存使用，但是原件必须妥善保存，保存时间至少应当与认证证书有效期一致。

12 其他

12.1 本规则内容提及 ISO22301:2019《安全与韧性 业务连续性管理体系 要求》标准时均指认证活动发生时该标准的有效版本。认证活动及认证证书中描述该标准号时，将采用当时有效版本的完整标准号。

12.2 本规则所提及的各类证明文件的复印件应是在原件上复印的，并经审核员签字确认与原件一致。

12.3 中心也将开展管理体系及相关技术标准的宣贯培训，促使组织的全体员工正确理解和执行 ISO22301:2019《安全与韧性 业务连续性管理体系 要求》标准的要求。

附录 A 业务连续性管理体系认证审核时间要求

有效人数	认证时间（人天）
1-100	2
101-500	3
501-1000	4
>1000	根据实际情况予以确认，但将不少于 5 人日

注：有效人数包括认证范围内涉及的所有人员，包括兼职人员、临时人员，但兼职人员、临时人员可根据实际工作小时数予以换算成等效的全职人员数。