**附件7**

****

CNAS-CC1XX

**业务连续性管理体系审核及认证的能力要求**

**Competence Requirements for Auditing and Certification of Business Continuity Management Systems**

**（征求意见稿）**

中国合格评定国家认可委员会

目 次

[前 言 2](#_Toc482988750)

[引 言 3](#_Toc482988751)

[1 范围 4](#_Toc482988752)

[2 规范性引用文件 4](#_Toc482988753)

[3 术语和定义 4](#_Toc482988754)

[4 通用能力要求 4](#_Toc482988755)

[5 业务连续性管理体系审核员、复核审核报告并做出认证决定的人员的能力要求 4](#_Toc482988756)

[5.1 总则 4](#_Toc482988757)

[5.2 业务连续性管理（BCM）术语 5](#_Toc482988758)

[5.3 组织环境 5](#_Toc482988759)

[5.4 适用法律法规和其他要求 5](#_Toc482988760)

[5.5 业务连续性管理过程中的关系 5](#_Toc482988761)

[5.6 业务影响分析和风险评估 5](#_Toc482988762)

[5.7 业务连续性策略 5](#_Toc482988763)

[5.8 事件管理 6](#_Toc482988764)

[5.9 业务连续性计划 6](#_Toc482988765)

[5.10 业务连续性演练 6](#_Toc482988766)

[5.11 业务连续性管理体系绩效评价 6](#_Toc482988767)

[6 实施申请评审以确定所需的审核组能力、选择审核组成员并确定审核时间的人员的能力要求 6](#_Toc482988768)

[6.1 总则 6](#_Toc482988769)

[6.2 业务连续性管理术语 6](#_Toc482988770)

[6.3 组织环境 6](#_Toc482988771)

[6.4 业务连续性管理过程中的关系 7](#_Toc482988772)

[附录 A（资料性附录）](#_Toc482988773)[业务连续性管理体系审核及认证的知识 8](#_Toc482988774)

[参考文献 9](#_Toc482988775)

前 言

本文件等同采用ISO/IEC TS 17021-6:2014《合格评定 管理体系审核与认证机构要求 第6部分：实施业务连续性管理体系审核及认证的能力要求》（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），本文件是CNAS对业务连续性管理体系认证机构的专用认可准则。本文件与管理体系认证机构的基本认可准则CNAS-CC01:2015《管理体系认证机构要求》共同构成CNAS对业务连续性管理体系认证机构的认可准则。

本文件附录A为资料性附录。

本文件对ISO/IEC TS 17021-6:2014进行了编辑性修改，包括：

1.删除了ISO/IEC TS 17021-6引言中

“本技术规范中使用下列助动词：

——“应”表示要求；

——“宜”表示建议；

——“可以”表示允许；

——“能”表示能够。

进一步内容参见ISO/IEC指令第2部分。

为了研究的目的，鼓励使用者分享他们对本技术规范的观点以及在他们认为在后续版本变化中优先考虑的事项。点击以下链接参加在线调查：

<https://www.surveymonkey.com/s/tptvjcl>”；

2.本文件中将对ISO/IEC 17021:2011的引用更新为对CNAS-CC01:2015的引用；

3.本文件中将对ISO 9000的引用调整为对GB/T 19000的引用，对ISO 19011的引用调整为对GB/T 19011的引用，对ISO 22301:2012的引用调整为对GB/T 30146-2013的引用，对ISO/IEC 17000的引用调整为对GB/T 27000的引用；

4.修正6.1条中对后续条款号（6.2至6.4）的引用，修正附录A的表A.1中对5.4、5.7条款名称的引用。

本文件与CNAS适用认可规则、认可准则等规范文件共同构成对业务连续性管理体系认证机构的认可要求。

本文件为首次发布。

引 言

本文件是对CNAS-CC01的补充，特别是明确了CNAS-CC01:2015附录A所述的认证过程涉及人员的能力要求。

CNAS-CC01:2015的第4章的指导原则是本文件中要求的基础。

对于相关方（包括认证机构的客户和获得管理体系认证的组织的顾客），认证机构有责任确保业务连续性管理体系（BCMS）认证是可靠的、仅使用相关能力得到证实的认证人员。

BCMS认证人员需要具有CNAS-CC01:2015所述的通用能力，也具有本文件所述的BCMS特定知识。

认证机构需要针对每个BCMS审核的范围识别审核组所需的特定能力。

**业务连续性管理体系审核及认证的能力要求**

**1 范围**

本文件对CNAS-CC01:2015的现有需求进行了补充。本文件包括对业务连续性管理体系（BCMS）认证过程中所涉及人员的特定能力要求。

**2 规范性引用文件**

本文件中涉及的以下文件的部分或全部内容组成了此文件的要求。凡是注日期的引用文件，仅注日期的版本适用于本文件。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。

CNAS-CC01:2015管理体系认证机构要求

GB/T 27000 合格评定 词汇和通用原则（ISO/IEC 17000，IDT）

GB/T 30146 公共安全 业务连续性管理体系 要求（ISO 22301，IDT）

ISO 22300 公共安全-术语

**3 术语和定义**

CNAS-CC01:2015、ISO 22300、GB/T 30146和GB/T 27000中给出的术语和定义适用于本文件。

**4 通用能力要求**

认证机构应对CNAS-CC01:2015表A.1中的每一项认证职能定义能力要求。在定义这些能力要求时，认证机构应考虑CNAS-CC01:2015中规定的所有要求，以及本文件第5章至第6章中规定的所有要求。

注1：附录A提供了对特定的认证职能所涉及人员能力要求的信息摘要。

注2：GB/T 19011提供了审核原则的信息。

**5** **业务连续性管理体系审核员、复核审核报告并做出认证决定的人员的能力要求**

## 5.1 总则

所有BCMS审核员、复核审核报告并做出认证决定的人员应具备一定程度的能力，包括CNAS-CC01:2015中所描述的通用能力，以及本文件5.2到5.11所描述的BCMS知识。

注1：审核组中的每位审核员不必具备同样的能力，然而审核组的整体能力需要足以实现审核目标。

注2：尽管知识要求的基本要素都一样，但应该承认对审核员、复核审核报告并做出认证决定的人员而言，知识要求的细节程度可能不尽相同。这由每个独立的认证机构负责确定。

## 5.2 业务连续性管理（BCM）术语

审核组、复核审核报告并做出认证决定的人员应具备BCM及风险的术语、定义和概念的知识。

## 5.3 组织环境

审核组、复核审核报告并做出认证决定的人员应具备组织运行所处相关环境的知识。

## 5.4 适用法律法规和其他要求

审核组、复核审核报告并做出认证决定的人员应具备相关知识，以确定组织是否识别并评价了其与适用法律法规和其他要求的符合性。

注1：法律法规要求可以表述为法律要求。

注2：其他要求可以包括自愿性的国家、国际和特定行业的协议。

## 5.5 业务连续性管理过程中的关系

审核组、复核审核报告并做出认证决定的人员应具备BCM各要素间相互关系的知识。

## 5.6 业务影响分析和风险评估

审核组、复核审核报告并做出认证决定的人员应具备业务影响分析（BIA）的知识，包括：

——方法学和技巧；

——对产品和服务交付活动的识别；

——时间上的影响评估，当影响变得不可接受时应能予以识别；

——对重启设定具有优先排序的时间表；

——对附属及支持资源的识别。

审核组、复核审核报告并做出认证决定的人员应具备风险评估和风险管理的知识，包括：

——方法学和技巧；

——中断事件相关风险的识别、分析和评价；

——现有控制措施的有效性；

——对适当的风险处置的识别。

## 5.7 业务连续性策略

审核组、复核审核报告并做出认证决定的人员应具备策略和方法学的知识，以降低中断事件的影响及其发生的可能性，包括：

——策略制定；

——已准备措施；

——对可选性策略的选择；

——连续性策略的成本收益分析；

——和外部股东的协调方法；

——事件响应；

——沟通；

——命令和控制；

——协调响应部门；

——恢复和重建。

## 5.8 事件管理

审核组、复核审核报告并做出认证决定的人员应具备事件管理措施的知识，以确定组织是否识别了对中断事件的适当响应，包括预警和沟通需求。

审核组、复核审核报告并做出认证决定的人员应具备相关知识以评价组织测试其事件管理能力的有效性。

## 5.9 业务连续性计划

审核组、复核审核报告并做出认证决定的人员应具备业务连续性计划的知识，包括业务连续性计划的建立、更新、维护、目的、格式、结构以及程序细节。

## 5.10 业务连续性演练

审核组、复核审核报告并做出认证决定的人员应具备策划和执行业务连续性演练的知识，包括业务连续性演练的类型、过程、技巧以及组织满足其恢复优先级别与恢复目标的能力的评价准则。

## 5.11 业务连续性管理体系绩效评价

审核组、复核审核报告并做出认证决定的人员应具备BCMS绩效评价的知识，包括指标和绩效标准的知识，以确定组织的BCMS绩效是否实现其管理层确定的目的和目标。

**6 实施申请评审以确定所需的审核组能力、选择审核组成员并确定审核时间的人员的能力要求**

## 6.1 总则

其他认证职能涉及的小组或个人应具备的能力包括CNAS-CC01:2015中描述的通用能力，以及本文件6.2到6.4描述的BCMS知识。

## 6.2 业务连续性管理术语

其他认证职能涉及的小组或个人应具备BCM术语的知识。

## 6.3 组织环境

其他认证职能涉及的小组或个人应具备组织运行所处相关环境的知识。

## 6.4 业务连续性管理过程中的关系

其他认证职能涉及的小组或个人应具备BCM要素间相互关系的知识。

# 附录 A（资料性附录）

# 业务连续性管理体系审核及认证的知识

表A.1提供了一个BCMS审核及认证所需知识的摘要，该表是资料性的，仅标明了特定认证功能所需的知识范围。

每个认证职能的能力要求见本文件正文。

表A.1中，“√”表示认证机构宜对知识的准则和程度进行定义。

表 A.1 知识表

|  |  |
| --- | --- |
| **知识** | **认证职能** |
| **实施申请评审，以确定审核组的能力要求、选择审核组成员并决定审核时间** | **复核审核报告并做出认证决定** | **审核和领导审核组** |
| 业务连续性管理术语 | √（见6.2） | √（见5.2） | √（见5.2） |
| 组织环境 | √（见6.3） | √（见5.3） | √（见5.3） |
| 适用法律法规和其他要求 |  | √（见5.4） | √（见5.4） |
| 业务连续性管理过程中的关系 | √（见6.4） | √（见5.5） | √（见5.5） |
| 业务影响分析和风险评估 |  | √（见5.6） | √（见5.6） |
| 业务连续性策略 |  | √（见5.7） | √（见5.8） |
| 事件管理 |  | √（见5.8） | √（见5.8） |
| 业务连续性计划 |  | √（见5.9） | √（见5.9） |
| 业务连续性演练 |  | √（见5.10） | √（见5.10） |
| BCMS绩效评价 |  | √（见5.11） | √（见5.11） |

审核组宜具有专门知识和技能，或在必要时由技术专家补充。当审核由一个审核组实施时，宜由审核组整体具有相应程度的必备技能，而不必由组内每位独立成员具有。

**参考文献**

1. GB/T 19011 管理体系审核指南
2. ISO 22313 公共安全-业务连续性管理体系-指南
3. ISO 22398 公共安全-演练指南
4. ISO 31000 风险管理-原则和实施指南
5. ISO Guide 73 风险管理-词汇
6. IEC 31010 风险管理-风险评估方法

——