全国认证认可标准化技术委员会

国认标委函 〔2019〕13 号

关于征求国家标准《合格评定 管理体系审核认证机构要 第 6 部分：业务连续性管理体系审核和认证能力要求》（征求意见稿）意见的函

各位委员、观察员及有关单位：

全国认证认可标准化技术委员会（SAC/TC 261）正在实施国家标准化管理委员会下达的《合格评定 管理体系审核认证机构要 第 6 部分：业务连续性管理体系审核和认证能力要求》国家标准制定项目（计划编号：20170456-T-469）。现将《合格评定 管理体系审核认证机构要 第 6 部分：业务连续性管理体系审核和认证能力要求》（征求意见稿）、编制说明以及意见反馈表提供给你们，望认真研究并提出宝贵意见。请于 2019 年 5 月 22 日以前将意见反馈表以电子文本发送至标准起草组。

联系人：王轶亮

电话： 13701230219

电子邮件：wangyl@isccc.gov.cn

附件：1.《合格评定 管理体系审核认证机构要 第 6 部分：业务连续性管理体系审核和认证能力要求》（征求意见稿）

2.编制说明

3.意见反馈表

国认标委

2019年4月22日

附件 1

ICS 点击此处添加 ICS 号
点击此处添加中国标准文献分类号

GB/T XXXXX—XXXX

中 华 人 民 共 和 国 国 家 标 准

合格评定 管理体系审核认证机构要求

第 6 部分：业务连续性管理体系审核和认证能力要求

Conformity assessment — requirements for bodies providing audit and certification of management systems — part 6: conpetence requirements for auditing and certification of business continuity management systems

点击此处添加与国际标准一致性程度的标识

（征求意见稿）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前言.....II
引言.....III
1　范围..... 1
2　规范性引用文件..... 1
3　术语和定义..... 1
4　通用能力要求..... 1
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..... 1
5.1　总则..... 1
5.2　业务连续性管理（BCM）术语..... 1
5.3　组织环境..... 2
5.4　适用法律法规和其他要求..... 2
5.5　业务连续性管理过程中的关系..... 2
5.6　业务影响分析和风险评估..... 2
5.7　业务连续性策略..... 2
5.8　事件管理..... 2
5.9　业务连续性计划..... 3
5.10　业务连续性演练..... 3
5.11　业务连续性管理体系绩效评价..... 3
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..... 3
6.1　总则..... 3
6.2　业务连续性管理术语..... 3
6.3　组织环境..... 3
6.4　业务连续性管理过程中的关系..... 3
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..... 4
参考文献..... 5

前　言

本标准按照GB/T 1.1-2009和GB/T 20000.2-2009给出的规则起草。

本标准使用翻译法等同采用国际标准ISO/IEC TS 17021-6:2014 《合格评定 管理体系审核认证机构要求 第6部分：业务连续性管理体系审核和认证能力要求》。

本标准由全国认证认可标准化技术委员会（SAC/TC 261）提出并归口。

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这些专利的责任。

本标准起草单位：中国网络安全审查技术与认证中心、中国合格评定国家认可中心、山东省标准化研究院、海关总署、中国认证认可协会、广东康云科技有限公司、广州海关信息中心、中国兵工物资集团有限公司、广州云润大数据服务有限公司、四川省电子产品监督检验所、广东鸿威展览集团、广东联结电子商务有限公司、上海安言信息技术有限公司、广东智信信息科技股份有限公司、南方电网传媒有限公司

本标准主要起草人：王轶亮、魏军、尤其、杨哲、王曙光、张芳、王茜、李家康、茶国吉、曲晖、晋彤、王照云、陶宇、冯丽、蔡立群、王永基、石磊、秦峰

引　言

本标准是对ISO/IEC 17021:2011的补充，特别是明确了ISO/IEC 17021:2011附录A所述的认证过程涉及人员的能力要求。

ISO/IEC 17021:2011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ISO/IEC 17021:2011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。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。

合格评定 管理体系审核认证机构要求 第6部分:业务连续性管理体系审核和认证能力要求

1 范围

本文件对ISO/IEC 17021:2011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

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，仅所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。

ISO/IEC 17021:2011 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

ISO/IEC 17021:2011、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ISO/IEC 17021:2011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ISO/IEC 17021:2011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ISO/IEC 17021:2011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ISO/IEC 17021:2011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5.7）
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] GB/T 31595-2015 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

附件 2

国家标准《合格评定 管理体系审核认证机构要求 第 6 部分：业务连续性管理体系审核和认证能力要求》编制说明

一、任务来源

本标准的制定由中国网络安全审查技术与认证中心提出，中国合格评定国家认可中心、山东省标准化研究院等机构共同参与编制，本标准列入国家标准委 2018 年国家标准制修订计划，项目编号 20170456-T- 469，项目名称为《合格评定 管理体系审核认证机构要求 第 6 部分：业务连续性管理体系审核和认证能力要求》。

二、目的和意义

ISO/IEC TS 17021-6:2014《合格评定 管理体系审核认证机构要求 第 6 部分：业务连续性管理体系审核和认证能力要求》国际标准已于 2014 年 12 月 1 日发布，该标准是对已发布的国际标准 ISO/IEC 17021:2011 的补充，特别是明确了 ISO/IEC 17021:2011 附录 A 所述的，在业务连续性管理方面的认证过程涉及人员的能力要求。为了使我国业务连续性管理体系认证审核活动能够与国际要求保持一致，我们特申请将该标准等同转化为国家标准，以对国内实施业务连续性管理体系认证审核的机构提供一致性要求，同时，该标准也可适用于认可、同行评审或其他审核过程，作为实施或评价的准则。

三、起草工作组的组成

中国网络安全审查技术与认证中心负责本标准的制订工作。标准起草工作组的组成考虑了认证机构、认可机构、标准使用单位等方面。主要起草单位和人员包括：

中国网络安全审查技术与认证中心：王轶亮、魏军、尤其

中国合格评定国家认可中心：杨哲

山东省标准化研究院：王曙光

海关总署：张芳

中国认证认可协会：王茜

广东康云科技有限公司：李家康

广州海关信息中心：曲晖

中国兵工物资集团有限公司:茶国吉

广州云润大数据服务有限公司：晋彤

四川省电子产品监督检验所：冯丽

广东鸿威展览集团：王照云

广东联结电子商务有限公司：陶宇

上海安言信息技术有限公司：石磊、秦峰

广东智信信息科技股份有限公司:蔡立群

南方电网传媒有限公司:王永基

四、编制原则

1）本标准的编写遵守国家标准 GB/T 1.1—2009《标准化工作导则 第 1 部分：标准的结构和编写》。

2）本标准编制依据 ISO/IEC 导则第 1 部分附录中对管理体系标准框架结构一致性的最新要求。

3）本标准中的术语和定义尽可能与我国现行相关国家标准保持一致和连贯。

五、标准的编制过程

中国网络安全审查技术与认证中心在 2015 年提出《合格评定 管理体系审核认证机构要求 第 6 部分：业务连续性管理体系审核和认证能力要求》国家标准起草项目，并列入国家标准委 2018 年国家标准制修订计划，具体过程如下：

1）2014 年 5 月，在全国认证认可标准化技术委员会秘书处的正式确立下，成立了 ISO/CASCO/JWG 40 国际标准对口工作组，开始跟踪 ISO/IEC TS 17021—6 国际标准的制修订过程，并针对 ISO/IEC DTS 17021—6 提出了我国的修订意见。

2）2015 年 3 月，在前期国际标准跟踪的基础上，完成了《合

格评定 管理体系审核认证机构要求 第6部分:业务连续性管理体系审核和认证能力要求》草案的编制,同时正式向全国认证认可标准化技术委员会秘书处提出该标准立项申请。

3)2018年12月,标准起草组对《合格评定 管理体系审核认证机构要求 第6部分:业务连续性管理体系审核和认证能力要求》(草案)进行了第一次公开征求意见。

4)2019年3月,根据标准草案征求意见修订情况进行研究,形成国家标准公开征求意见稿草案。

六、有关问题的说明

1)标准的适用范围:

本标准为要求类标准,适用于按照GB/T 30146《公共安全 业务连续性管理体系 要求》开展以业务连续性管理体系(BCMS)审核和认证为目的认证机构,也可适用于认可、同行评审或其他审核过程,作为实施或评价的准则。

2)标准的技术特点:

本标准为等同采用国际标准ISO/IEC TS 17021-6:2014,在标准的起草过程中仅做了编辑性的修改,除此之外,未对原国际标准进行任何修改。

标准起草组

二〇一九年四月十日

附件 3

《合格评定 管理体系审核认证机构要 第 6 部分：业务连续性管理体系审核和认证能力要求》国家标准意见反馈表

序号	标准条款号	意见或建议	修改原因
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			

填写单位：_____ 姓名：_____联系方式：_____Email：_____

抄送：国家市场监督管理总局认可检测司，存档（2）。

全国认证认可标准化技术委员会　　2019 年 4 月 22 日印发