



# 中华人民共和国国家标准

GB/T 27021.6—2020/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 审核认证能力要求

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

(ISO/IEC TS 17021-6:2014, IDT)

2020-03-31 发布

2020-10-01 实施

国家市场监督管理总局 发布  
国家标准化管理委员会

## 目 次

前言 .....	III
引言 .....	IV
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 BCMS 审核员、复核审核报告人员和做出认证决定人员的能力要求 .....	1
5.1 总则 .....	1
5.2 业务连续性管理(BCM)术语 .....	2
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 .....	3
5.9 业务连续性计划 .....	3
5.10 业务连续性演练 .....	3
5.11 BCMS 绩效评估 .....	3
6 实施申请评审人员的能力要求,以确定审核组能力需求、选择审核组成员和确定审核时间 .....	3
6.1 总则 .....	3
6.2 BCM 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

GB/T 27021《合格评定 管理体系审核认证机构要求》分为以下7个部分：

- 第1部分：要求；
- 第2部分：环境管理体系审核认证能力要求；
- 第3部分：质量管理体系审核认证的能力要求；
- 第4部分：大型活动可持续性管理体系审核和认证能力要求；
- 第5部分：资产管理体系审核和认证能力要求；
- 第6部分：业务连续性管理体系审核认证能力要求；
- 第7部分：道路交通安全管理体系审核认证能力要求。

本部分为GB/T 27021的第6部分。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分使用翻译法等同采用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认证能力要求》。

与本部分中规范性引用的国际文件有一致性对应关系的我国文件如下：

- GB/T 27000 合格评定 词汇和通用原则(GB/T 27000—2006,ISO/IEC 17000:2004,IDT)
- GB/T 30146 公共安全 业务连续性管理体系 要求(GB/T 30146—2013,ISO 22301:2012, IDT)

本部分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。

本部分起草单位：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、中国认证认可协会、东风咨询有限公司、上海安言信息技术有限公司、奇安信科技集团股份有限公司、广东互能信息科技有限公司、云天弈(北京)信息技术公司、广东康云科技有限公司、平安科技(深圳)有限公司。

本部分主要起草人：尤其、魏军、杨哲、王轶亮、王曙光、石磊、王茜、钱英杰、史吉建、鲍旭华、苏云凤、秦峰、张明状、金利杰、李家康。

## 引 言

本部分是对 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 章的指导原则是本部分中要求的基础。

认证机构对相关方(包括认证机构的客户和获得管理体系认证的组织的顾客)负有相应的责任,即确保被证实具备相应能力的审核员,才能实施业务连续性管理体系(Business Continuity Management System;BCMS)审核。

BCMS 认证人员需要具有 ISO/IEC 17021:2011 所述的通用能力,也具有本部分所述的 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。本部分中使用下列助动词:

- “应”表示要求;
- “宜”表示建议;
- “可以”表示允许;
- “能够”表示一种可能性或能力。

ISO/IEC 工作导则第 2 部分中对这些助动词做了更详细的说明。



# 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

### 审核认证能力要求

#### 1 范围

GB/T 27021 的本部分对 ISO/IEC 17021:2011 的现有要求进行了补充。本部分包含了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 17000 合格评定 词汇和通用原则(Conformity assessment—Vocabulary and general principles)

ISO/IEC 17021:2011 合格评定 管理体系认证机构要求(Conformity assessment—Requirements for bodies providing audit and certification of management systems)

ISO 22300 公共安全 术语(Societal security—Terminology)

ISO 22301 公共安全 业务连续性管理体系 要求(Societal security—Business continuity management system—Requirement)

#### 3 术语和定义

ISO 22300、ISO 22301、ISO/IEC 17000 和 ISO/IEC 17021:2011 界定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,以及本部分第 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资料性摘要。

注 2: ISO 19011 提供了审核原则的信息。

#### 5 BCMS 审核员、复核审核报告人员和做出认证决定人员的能力要求

##### 5.1 总则

所有 BCMS 审核员、复核审核报告人员和做出认证决定人员均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,以及本部分 5.2~5.11 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: 尽管这些知识要求的基本要素都一样,但可以认识到对审核员、复核审核报告人员和做出认证决定人员而言,知识要求的详略程度可能不尽相同。这由各认证机构负责确定。

## 5.2 业务连续性管理(BCM)术语

审核组、复核审核报告人员和做出认证决定人员应具备 BCM 及风险的术语、定义和概念的知识。

## 5.3 组织环境

审核组、复核审核报告人员和做出认证决定人员应具备组织运行所处环境的知识。

## 5.4 适用法律法规和其他要求

审核组、复核审核报告人员和做出认证决定人员应具备相关知识,以确定组织是否识别并评价了适用法律和其他要求的符合性。

注 1: 行政规章和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定。

## 5.5 业务连续性管理过程中的关系

审核组、复核审核报告人员和做出认证决定人员应具备 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、复核审核报告人员和做出认证决定人员应具备业务影响分析(BIA)的知识,包括:

- 方法学和技术;
- 对产品和服务交付活动的识别;
- 对时间推移产生的影响进行评估,识别何时会变为不可接受;
- 为重启设置优先级;
- 对依赖及支持资源的识别。

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知识,包括:

- 方法学和技术;
- 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、复核审核报告人员和做出认证决定人员应具备降低中断事件影响和可能性的策略和方法学方面的知识,包括:

- 策略制定;
- 准备措施;
- 替代策略的选择;
- 连续性策略的成本收益分析;
- 和外部相关方的协调方法;
- 事件响应;
- 沟通;
- 命令和控制;

- 响应组织的协调；
- 恢复和重建。

## 5.8 事件管理

审核组、复核审核报告人员和做出认证决定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、复核审核报告人员和做出认证决定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、复核审核报告人员和做出认证决定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、开发、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、复核审核报告人员和做出认证决定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、技巧以及评价组织满足其恢复优先级别与恢复目标的能力的准则。

## 5.11 BCMS 绩效评估

审核组、复核审核报告人员和做出认证决定人员应具备 BCMS 绩效评价的知识,包括指标和绩效测量的知识,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 实施申请评审人员的能力要求,以确定审核组能力需求、选择审核组成员和确定审核时间

## 6.1 总则

其他认证职能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,以及本部分 6.2 和 6.3 描述的 BCMS 知识。

## 6.2 BCM 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 BCMS 审核及认证所需知识的摘要,该表是资料性的,因为仅识别了特定认证功能所需的知识域。

每个认证职能的能力要求见本部分正文。

表 A.1 中,“√”表示认证机构宜对知识的准则和程度进行确定。

表 A.1 知识表

知识	认证职能		
	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	复核审核报告并做出认证决定	审核及领导审核组
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)
业务连续性和恢复策略		√(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)

审核组宜具有专业的知识和技能,或在必要时由技术专家补充。当审核由一个审核组实施时,宜由审核组整体具备所需的技能水平相应程度的必备技能,而不必要求组内每个成员具备这些技能。



参 考 文 献

- [1] ISO 19011 Guidelines for auditing management systems
  - [2] ISO 22313 Societal security—Business continuity management system—Guidance
  - [3] ISO 22398 Societal security—Guidelines for exercises
  - [4] ISO 31000 Risk management—Principles and guidelines
  - [5] ISO Guide 73 Risk management—Vocabulary
  - [6] IEC 31010 Risk management—Risk assessment techniques
-