公有云个人信息安全管理体系认证规则

KBRZ-GZ-49

北京坤标检验认证有限公司

目录

1. 适用范围及总则

1.1 适用范围和认证依据

1.1.1 本规则适用于 KBRZ 依据 GB/T 41574-2022 MOD ISO/IEC 27018:2019 《信息技术 安全技术 公有云中个人信息保护实践指南》标准开展的公有云个人信息安全管理体系认证活动。

1.1.2 本规则认证依据为 GB/T 41574-2022 MOD ISO/IEC 27018:2019 《信息技术 安全技术 公有云中个人信息保护实践指南》标准，以及相关的技术规范、技术规范强制性要求或者标准。

1.1.3 本规则对公有云个人信息安全管理体系认证实施过程作出具体规定，明确 KBRZ 对认证过程的管理责任，保证公有云个人信息安全管理体系认证活动的规范有效。

1.1.4 本规则是 KBRZ 在公有云个人信息安全管理体系认证活动的基本要求，审核员、认证客户在该项认证活动中应当遵守本规则。

1.2 总则

1.2.1 KBRZ依据国家相关法律法规，国家标准、规范等开展对认证客户的认证活动。

1.2.2 KBRZ对认证客户的认证工作遵循客观公正、科学规范、权威信誉、廉洁高效和非歧视的原则。

1.2.3 KBRZ不对申请认证客户提供可能影响认证公正性的咨询或其他服务。

1.2.4 KBRZ对承诺满足法律法规要求开展经营活动的认证客户实施认证。

1.2.5 在认证申请或初次认证审核的任何阶段，若有证据表明认证客户存在欺诈行为、故意提供虚假信息或隐瞒信息，KBRZ将不予受理。

1.2.6 KBRZ对申请认证的认证客户的申请材料内容、认证审核信息和其他非公开信息保守秘密。在法律法规要求时，KBRZ有责任将认证客户的相关信息向有关部门通报。

1.2.7 KBRZ对认证客户的认证仅表明，KBRZ承认获准认证的认证客户在认证范围内具有相关的管理能力。始终一致地达到实施管理体系标准的预期结果和符合认证要求的责任，在于认证客户而不是KBRZ。

2.引用文件

下列引用文件对本文件的应用是必不可少的。凡是注日期的引用，仅所引用的版本适用。凡是不注日期的引用，所引用文件的最新版本（包括任何修改单）适用。

《认证证书和认证标志管理办法》（2022年9月29日国家市场监督管理总局令第61号第二次修订）

CNAS-CC01《管理体系认证机构要求》

CNAS-CC170《信息安全管理体系认证机构要求》

GB/T 27021《管理体系认证机构要求》

《认证证书和认证标志管理办法》（2022年9月29日国家市场监督管理总局令第61号第二次修订）

3.术语和定义

GB/T 19000 和GB/T 27000中给出的术语和定义、引用文件的术语定义以及下列术语和定义适用于本文件。

3.1 认证审核

由独立于客户和依赖认证的各方的审核组织实施的、对客户的管理体系进行以认证为目的的审核。

3.2 管理体系认证审核时间

审核时间的一部分，包括从首次会议到末次会议之间实施审核活动的所有时间。

3.3 严重不符合

影响管理体系实现预期结果的能力的不符合。

3.4 轻微不符合

不影响管理体系实现预期结果的能力的不符合。

3.5 多场所组织

多场所组织是指组织有一个确定的KBRZ职能机构（以下称作KBRZ办公室，但不一定是组织的总部）来策划、控制或管理某些活动，并且有一个由地方办公室或分支（即场所）组成的网络来实施（或部分实施）这些活动。

3.6 现场审核

KBRZ指派审核组到受审核组织所在地点进行的审核活动。

3.7 远程审核

应用信息和通信技术(ICT)，在受审核活动的实际场所以外任何地点实施的审核。

注1:ICT是应用技术来收集、存储、检索、处理、分析和发送信息，它包括软件和硬 件，例如:智能手机、手持设备、笔记本电脑、台式电脑、无人机、摄像机、可穿戴技术、 人工智能及其他。

注2:远程审核可以是审核人员在受审核方某一场所对其他场所的人员、活动或过程进 行的审核，也可以是审核人员不在受审核方场所对受审核方的人员、活动或过程进行的审 核。

3.8 特殊审核

扩大认证范围或提前较短时间通知的审核。

4.认证人员条件及能力要求

KBRZ依据 ISO/IEC 17021-1（CNAS-CC01）要求，对每个技术领域所需的能力，对相关具体的认证方案、认证活动中的职责和作用进行了确定，对所涉及的认证人员的聘用、初始评价、持续评价等要求执行KBRZ-CX10《认证人员管理程序》，对认证人员岗位资格、行为与能力准则要求执行KBRZ-GL-18 《认证人员能力评价准则》。

审核员及认证决定人员的专业能力根据所申请认证的领域，参考信息安全管理体系专业

评价。

5.初次认证程序

5.1 受理初次认证申请

5.1.1 申请初次认证的认证客户（以下简称申请组织）应具备的基本条件：

1）具有法律地位；

2）从业条件中，有行政许可要求的，应取得相应资格并在有效期内；

3）产品及过程符合国家相关法律法规和标准要求；

4）已依据信息类相关标准进行了内部评价和管理评审；

5）通常情况下，企业建立的评价体系和管理体系运行 3 个月以上；

6）申请认证前未发生误导使用认证标识等行为。

7）ISO27017 认证是在 ISO27001 信息安全管理体系的基础上建立、实施和扩展的，ISO27001 是 ISO27017 认证的基础和前提条件。申请 ISO27017 认证的组织应已经建立信息安全管理体系，且通过了 ISO27001 认证或准备同时申请 ISO27001 认证。

8）ISO27018 认证是在 ISO27001 信息安全管理体系的基础上建立、实施和扩展的，ISO27001 是 ISO27018 认证的基础和前提条件。申请 ISO27018 认证的组织应已经建立信息安全管理体系，且通过了 ISO27001 认证或准备同时申请 ISO27001 认证。

9）相关信息类管理体系运行期间及建立体系前的一年内未受到主管部门行政处罚；或企业受到行政处罚但已整改、执行完毕并提供有效证据。

10）申请范围不超出资质许可范围、不超出信息类相关管理体系的覆盖范围（ISO27001 信息安全管理体系超出的认证范围必须先安排或同时对其 ISO27001 实施专项扩大审核后）。

5.1.2 申请组织应提交《认证申请书》及其要求的文件等申请材料。需要时，申请组织还应提供进一步的材料，以便 KBRZ 获得足够的认证客户信息。

5.1.3 在提交《认证申请书》时，申请组织应按照认证收费标准表交纳认证申请费。

5.2 申请评审

5.2.1 KBRZ 在收到申请组织提交的资料后,进行申请评审，解决双方在理解上的差异，必要时可对申请组织进行访问。

1）为确保认证审核的完整有效，KBRZ 依据 KBRZ-GL-19《确定审核时间管理规定》，基于申请组织管理体系覆盖的有效人数，并考虑活动范围、特性、技术复杂程度、风险程度等情况，核算并拟定完成认证审核工作需要的现场审核人日数，可以增加或减少审核人日数，但应有合理理由并记录。

2）通过申请评审的，KBRZ 将向申请组织发出受理申请的通知，并签署《认证合同》，明确双方的权利和义务，包括信息通报的义务

3）不符合申请条件的，KBRZ 将向申请组织发出不受理申请的通知，并阐明理由。

4）对不予受理有异议的，申请组织可以按《申诉、投诉和争议处理规则》的规定提出申诉。

5.3 方案策划

5.3.1审核方案

5.3.1.1 应对整个认证周期制定审核方案，以清晰地识别所需的审核活动，这些审核活动用以证实客户的管理体系符合认证所依据标准或其他规范性文件的要求。认证周期的审核方案应覆盖全部的管理体系要求。具体执行KBRZ-GL-05《审核策划管理规定》。

5.3.1.2 初次认证审核方案应包括两阶段初次审核（第一阶段和第二阶段）、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。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。审核方案的确定和任何后续调整应考虑客户的规模，其管理体系、产品和过程的范围与复杂程度，以及经过证实的管理体系有效性水平和以前审核的结果。

5.3.1.3 监督审核应至少每个日历年（应进行再认证的年份除外）进行一次。初次认证后的第一次监督审核应在认证决定日期起12个月内进行。

注：为了考虑诸如季节或有限时段的管理体系认证（例如临时施工场所）等因素，可能有必要调整监督审核的频次。

5.3.1.4 如果客户已获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本文件要求提供支持。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。

5.3.1.5 如果客户采用轮班作业，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。

5.3.2 确定审核目的、范围和准则

5.3.2.1 审核目的应由 KBRZ 确定。审核范围和准则，包括任何更改，应由 KBRZ 在与客户商讨后确定，应说明审核要完成什么。

5.3.2.2 审核范围应说明审核的内容和界限，例如拟审核的场所、组织单元、活动及过程。当初次认证或再认证过程包含一次以上审核（例如覆盖不同场所的审核）时，单次审核的范围可能并不覆盖整个认证范围，但整个审核所覆盖的范围应与认证文件中的范围一致。

5.3.2.3 审核准则应被用作确定符合性的依据，并应包括：所确定的管理体系规范性文件的要求；所确定的由客户制定的管理体系的过程和文件。

5.3.3 选择和指派审核组

KBRZ依据审核组组建原则，根据受审核组织的行业、规模和业务复杂程度组建审核组，指派审核组长并通知申请组织。如果仅有一名审核员，该审核员应有能力履行适用于该审核的审核组长职责。审核组应整体上具备KBRZ按照申请评审确定的审核能力，审核组长和审核

员所需的知识和技能可以通过技术专家和翻译人员补充。技术专家和翻译人员应在审核员的指导下工作。申请组织如对审核组组成有异议，可向KBRZ提出。

具体参考人员条件和能力要求章节。

5.3.4 制定审核计划

5.3.4.1 要求

KBRZ应确保为审核方案中确定的每次审核编制审核计划，以便为有关各方就审核活动的日程安排和实施达成一致提供依据。应提前与客户就审核计划进行沟通，并商定审核日期。应向客户提供审核组每位成员的姓名,并在客户请求时使其能够了解每位成员的背景情况。KBRZ应留出足够的时间，以使客户能够对某一审核组成员的任命表示反对，并在反对有效时使KBRZ能够重组审核组。

5.3.4.2 审核计划应与审核目的和范围相适应。审核计划至少应包括或引用：

a) 审核目的；

b) 审核准则；

c) 审核范围，包括识别拟审核的组织和职能单元或过程；

d) 拟实施现场审核活动（适用时，包括对临时场所的访问和远程审核活动）的日期和场所；

e) 预计的现场审核活动持续时间；

f) 审核组成员及与审核组同行的人员（例如观察员或翻译）的角色和职责。

注：审核计划的信息可以包含在一个以上的文件中。

5.4 初次认证的审核实施

5.4.1 第一阶段

5.4.1.1 通常情况下，现场审核前，审核组实施初步文件评审，对发现的问题开出不符合。针对文件评审提出的不符合，申请组织实施纠正，审核组验证后，实施现场审核。在下列情况，第一阶段审核可以不在认证客户现场进行：

（1）申请客户已获 KBRZ 颁发的其他有效认证证书，KBRZ 已对申请组织管理体系有充分了解。

（2）KBRZ 有充足的理由证明认证客户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。

5.4.1.2 一阶段非现场审核，文件审核的结果须在二阶段审核前验证；一阶段现场审核，文件评审提出的不符合可在一阶段现场验证。审核组编制审核计划，并提前通知申请组织。审核通常从首次会议开始，就一阶段的要求和安排等事项与申请组织代表进行沟通确认，一阶段主要与管理层、管理体系推进部门沟通管理体系的策划及确认申请的相关事宜等。现场巡视等。

5.4.1.3 审核结束时，审核组与认证客户代表召开末次会议，报告评审情况、审核组将第一

阶段审核情况形成书面文件告知认证客户。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，要及时提醒认证客户特别关注。在确保一阶段不符合充分的整改时间下，与客户商定二阶段的审核时间。

5.4.2 第二阶段

审核组编制二阶段审核计划，并提前通知申请组织。审核通常从首次会议开始，审核过程中，审核组可以通过面谈、查阅文件、抽查质量记录以及调查有关现场活动等方式收集证据。

审核组对所获取的相关信息和证据进行分析，对申请组织的能力及其运作的符合性和有效性进行综合评价。对不符合事实将要求申请组织代表予以确认，并提出不符合报告。

审核结束时，审核组与申请组织代表召开末次会议，报告审核情况、审核发现和审核结论，向申请组织提出有关不符合的纠正措施验证的要求和方式。

5.5 初次认证不符合项的纠正和纠正措施及其结果的验证

对审核中发现的不符合项，KBRZ要求受申请组织分析原因，并提出纠正和纠正措施。对于严重不符合和一般不符合，应要求申请组织在3个月内采取纠正和纠正措施。KBRZ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。特殊情况下，对于严重不符合，如果未能在第二阶段结束后6个月内验证对严重不符合实施的纠正和纠正措施，KBRZ将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，或者按照5.4.2条重新实施第二阶段审核。

注：验证活动由审核组成员完成。

5.6 初次认证的审核报告

5.6.1 审核组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）认证客户的名称和地址。

2）认证客户活动范围和场所。

3）审核的类型、准则和目的。

4）审核组组长、审核组成员及其个人注册信息。

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 5.4 条列明的程序及各项要求的审核工作情况，其中：对 5.4.2 条的各项审核要求逐项描述或引用审核证据、审核发现和审核结论；对信息类目标和过程及其绩效实现情况进行评价。

7）识别出的不符合项。

8）审核组对是否通过认证的意见建议。

5.6.2 KBRZ 保留用于证实审核报告中相关信息的证据。

5.7 初次认证的认证决定

KBRZ根据审核报告、审核记录、申请组织提交的资料和所获得的相关信息做出认证决定。必要时，可继续向申请组织调阅必要的补充信息。

通过认证决定后，KBRZ为申请组织颁发有效期为3年的认证证书。

同时，KBRZ在网站上向社会发布认证公告，并将认证名录上报认监委。

注： KBRZ 网站 （www.bjkbrz.com）,认监委网站www.cnca.gov.cn

6.监督审核程序

6.1 例行监督审核的方式

在认证证书有效期内，KBRZ按一定时间间隔对获证组织实施例行监督审核，以确认其持续符合认证标准及KBRZ认证规则。

例行监督审核通常采用现场审核的方式。

当认证客户管理体系文件发生重大变更时，监督审核还将包括对认证客户管理体系文件的评审。

6.2 例行监督评审的时间间隔

6.2.1 初次认证后的第一次监督审核应在认证决定日期起 12 个月内进行。此后，监督审核应至少每个日历年（应进行再认证的年份除外）进行一次，且两次监督审核的时间间隔不得超过 15 个月。

6.2.2 认证客户发生重大变更或 KBRZ 认为必要时，可缩短对认证客户例行监督评审的时间间隔。

6.2.3 认证客户的产品在产品质量国家监督抽查中被查出不合格时，自国家质检总局发出通报起 30 日内，KBRZ 对该客户实施监督审核。

6.3 例行监督评审的准备

6.3.1 例行监督审核实施前，认证客户应按要求及时向 KBRZ 提供准确的信息，以便 KBRZ 完成例行监督审核方案策划。对于需实施文件评审的，认证客户应按照要求向 KBRZ 报送管理体系文件。

6.3.2 KBRZ 确定例行监督审核方案后，组建审核组并通知认证客户，认证客户如有异议，可向 KBRZ 提出。审核组长负责编制审核计划，并提前通知认证客户。

6.4 例行监督审核的实施

对于需实施文件评审的，审核组应在现场审核实施前完成文件评审。

现场审核的实施与初次认证的二阶段审核实施过程相同。

6.5 例行监督审核不符合项的纠正和纠正措施及其结果的验证

在例行监督审核中发现的不符合，KBRZ应要求获证组织分析原因，并提出纠正和纠正措

施。一般不符合，获证组织应在3个月内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，严重不符合，应在1个月内完成纠正和纠正措施，KBRZ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，特殊情况下，对于不符合，要求申请组织在最多不超过6个月期限内采取纠正和纠正措施。如果未能在审核结束后6个月内验证对不符合实施的纠正和纠正措施，则评定该申请组织不符合认证要求，或者重新实施审核，并采取暂停、撤销等相应措施。

受审核方逾期未能有效关闭不符合，KBRZ将按认证规则要求对其认证资格进行处置。

6.6 例行监督评审的审核报告

例行监督审核方案所要求的审核活动全部完成后，由审核组长完成审核报告。监督审核的审核报告，除满足5.6.1条款1）~7）条内容外，还应有对下列内容的描述：

1）上次审核以来信息类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）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。

3）对与相关信息安全法律法规的符合性进行定期评价与评审的规程的运行情况。

4）信息类目标及其绩效是否达到信息类管理体系确定值。如果没有达到，获证组织是否运行内审机制识别了原因、是否运行管理评审机制确定并实施了改进措施。

5）获证组织对认证标志的使用或对认证资格的引用是否符合《认证认可条例》及其他相关规定。

6）信息类管理体系在实现客户信息安全方针的目标方面的有效性；

7）是否有投诉，如果有接受和处理投诉是否及时。

8）审核组对是否保持认证、变更的意见建议。

6.7 例行监督审核的评定

KBRZ根据例行监督审核的材料，由具备能力的人员对审核报告实施复核，符合要求的，保持认证资格；对于涉及缩小认证范围或者暂停/撤销认证资格的，经认证评定后，做出缩小认证范围/暂停/撤销认证资格的决定并通知认证客户。

6.8 扩大认证范围的审核

获认证后申请增加或变更认证范围时，KBRZ应对扩大认证范围的申请进行评审，并确定任何必要的审核活动，以做出是否可予扩大的决定。这类审核活动可以和监督审核同时进行。审核中发现的任何不符合应在规定时间内完成纠正和纠正措施的验证。

6.9 非例行监督

当出现下列情况时，KBRZ将对获证组织进行非例行监督审核

a) 收到相关方对获证组织的投诉；

b) 获证组织的管理体系和过程发生重大变更，可能影响体系正常运行；

c) 获证组织被有关行政监管部门查处、媒体曝光；

d) KBRZ 认为有必要时。

对于为调查投诉，或对国家/地方监督检查出现认证范围相关的不符合进行核实等，可能需要在提前较短时间通知获证组织后或不通知获证组织就对其进行审核的特殊审核项目，所开具的不符合，应在最多不超过1个月期限内采取纠正和纠正措施，或按《审核任务书》要求执行。

受审核方逾期未能有效关闭不符合，KBRZ将按认证规则要求对其认证资格进行处置。

7.再认证程序

7.1 再认证申请

申请组织应在认证证书有效期截止3个月前向KBRZ提出再认证申请，如果在当前认证的终止日期前成功完成了再认证活动，新认证的终止日期可以基于当前认证的终止日期。新证书上的颁证日期应不早于再认证决定日期。

7.2 再认证的审核方式

通常采用文件评审和现场审核相结合的方式。

7.3 再认证审核前准备

受理再认证申请后，KBRZ策划审核方案并确定审核组组成后通知认证客户，认证客户如有异议，可向KBRZ提出。审核组长负责编制审核计划，并提前通知认证客户。

7.4 再认证的审核实施

审核组应在现场审核实施前完成文件评审。

现场审核的实施与初次认证的二阶段审核实施过程相同。

7.5 再认证的不符合项的纠正和纠正措施及其结果的验证

对再认证审核中发现的不符合，KBRZ应要求获证组织分析原因，对于一般不符合，KBRZ要求获证组织在3个月内实施纠正与纠正措施，对于严重不符合，KBRZ要求获证组织在1个月内实施纠正与纠正措施，并在当前认证证书到期前完成对纠正与纠正措施的验证；特殊情况下，对于不符合，应要求申请组织在最多不超过6个月期限内采取纠正和纠正措施。如果未能在审核结束后6个月内验证对不符合实施的纠正和纠正措施，则应评定该申请组织不符合认证要求，或者重新实施审核，并采取暂停、撤销等相应措施。

受审核方逾期未能有效关闭不符合，KBRZ将按认证规则要求对其认证资格进行处置。

如果在当前认证终止日期前，KBRZ未能完成再认证审核或不能验证对严重不符合实施的纠正和纠正措施，则不推荐再认证，也不延长认证的效力。KBRZ会告知客户并解释后果。

在当前认证证书到期后，如果获证组织能够在6个月内完成未尽的再认证活动，则可以恢复认证，否则应至少进行一次第二阶段审核才能恢复认证。认证证书的生效日期应不早于再认证决定日期，终止日期应基于上一个认证周期。

7.6 再认证的审核报告

审核方案所要求的审核活动全部完成后，由审核组长完成审核报告。

7.7 再认证的认证决定

KBRZ根据再认证的审核材料，对认证客户做出更新认证资格的决定，换发新的认证证书。

8.认证证书及认证标志要求

8.1 认证证书应至少包含以下信息：

a）每个获证客户的名称和地理位置（或多场所认证范围内总部和所有场所的地理位置）；

b）授予认证、扩大或缩小认证范围、更新认证的生效日期，生效日期不应早于相关认证决定的日期；

注：当证书失效一段时间时，KBRZ在满足下列条件时，可以在证书上保留原始的认证日期：－清晰标示了当前认证周期的开始时间和截止时间；－ 把上一认证周期截止时间连同再认证审核的时间一起标示。

c）认证有效期或与认证周期一致的应进行再认证的日期；

d）唯一的识别代码；

e）审核获证客户时所用的管理体系标准和（或）其他规范性文件，包括发布状态的标示（例如修订时间或编号）；

f）与活动、产品和服务类型等相关的认证范围，适用时，包括每个场所相应的认证范围，且没有误导或歧义；

g）KBRZ的名称、地址和认证标志；可以使用其他标识（如认可标识、客户的徽标），但不能产生误导或含混不清；

h）认证用标准和（或）其他规范性文件所要求的任何其他信息；

i）在颁发经过修改的认证文件时，区分新文件与任何已作废文件的方法。

j）证书查询方式。KBRZ 除公布认证证书在 KBRZ 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”类似描述，以便于社会监督。

8.2 认证证书的有效期

初次认证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。

8.3 认证证书信息公开

KBRZ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，还根据社会相关方的请求向其提供证书信息，接受社会监督。

8.4 认证证书及认证标志的使用

执行KBRZ-GKWJ 公开文件中“认证证书及认证标志使用规则”。

9.暂停和撤销认证的规则

获证组织超过期限而未能实施监督审核的；审核组实施监督审核的审核结论及认证决定结论为暂停或撤销认证的，及其他经暂停、撤销的，KBRZ将发放《认证证书暂停通知书》或《认证证书撤销通知书》通知到客户，信息上报人员将暂停/撤销信息2日内上报认监委并在网上公布。

9.1 发生下列情况之一，暂停认证

a) 持有的行政许可证明、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；

b) 在前后两次认证的审核中，同样类型的严重不符合重复出现的；

c) 对于认证审核中提出的不符合，未在 KBRZ 规定时间内完成纠正措施和（或）纠正的；

d) 被认证监管部门发现体系运行存在问题或被投诉，经调查体系运行存在问题，但尚未构成撤销认证资格的；

e) 获证组织的产品、活动出现安全事故，经确认是获证组织造成的；

f) 被有关执法监管部门责令停业整顿的；

g) 获证组织向 KBRZ 提供的与认证有关的信息或相关证据严重失实的；

h) 获证组织未按《认证合同》规定按期缴纳认证费用的；

i) 获证组织不能再规定时限内接受监督审核或再认证审核的；

j) 获证组织发生对体系造成影响的重大事故、重大投诉及相关变更未及时报告 KBRZ 的；

k) 错误使用认证证书、认证标志，使用认证标志或国际互认标志；

l) 不接受 KBRZ 非定期监督审核和/或认证行业管理部门监督检查的；

m) 获证组织主动请求暂停的；

n) 其他应当暂停认证证书的。

暂停时间为不超过6个月，涉及获证组织全部或部分认证范围。KBRZ将向获证组织发出《暂停注册资格通知书》、同时向行业管理部门上报相关信息并向社会公告。获证组织应按通知书规定的有关要求执行，暂停使用认证证书及认证标志。

9.2 发生下列情况之一，撤销认证

a) 暂停期限内，未就存在问题采取有效纠正措施的（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）；

b) 对获证组织投诉，经调查存在严重问题，构成撤销认证资格的；

c) 发生重大事故，经执法监管部门确认是获证组织违规造成的；

d) 被注销或撤销法律地位证明文件的，或被相关行政部门撤销产品生产或服务提供资格的，或有其他严重违反法律法规行为的；

e) 在 KBRZ 非定期监督审核、认证行业管理部门监督检查中被发现存在严重问题，构成撤销

认证资格的；或拒绝配合 KBRZ、认证行业管理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；

f） 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 KBRZ 已要求其纠正但超过规定期限仍未纠正的；

g） 获证组织没有运行相应管理体系或者已不具备运行条件的；

h） 其他应当撤销认证证书的。

当获证组织部分认证范围无法满足规定要求时，可缩小部分认证范围；当获证组织全部认证范围无法满足规定要求时，撤销认证证书。KBRZ向获证组织发出《撤销认证注册资格通知书》，并以公告形式公布，组织应交回认证证书。被撤销的认证证书信息，KBRZ将及时上报至国家认监委；KBRZ网站证书查询栏中将同步公示被撤销的组织名录。

9.3 发生下列情况之一，注销认证

a） 获证组织主动请求注销的；

b） 换发新证书注销旧证书的；

c） 其他应当注销认证证书的。

被注销的认证证书信息，KBRZ将及时上报至国家认监委；KBRZ网站证书查询栏中将同步公示被注销的组织名录。

10.与其他管理体系的结合审核

对信息类管理体系和其他管理体系实施结合审核时，通用或共性要求应满足本规则要求，审核报告中应清晰，并易于识别。

11.多场所客户的审核和认证

11.1 认证申请与受理

11.1.1 申请有多场所认证的初次认证客户，除满足本规则第 5.1 条中申请认证应具备的基本条件外，还应符合以下条件：

1） 多场所认证客户应对设立、授权和管理多场所以及对多场所获得 KBRZ 认证等活动建立和实施相关程序；

2） 多场所认证客户的总部和每个分场所应已按相关认证标准的要求建立和运行其管理体系，并已实施覆盖所有程序的内审和管理评审；

3） 与申请事项有关的所有场所应至少已实施过经总部授权的活动，并在认证客户最近一次的内部审核和管理评审中覆盖了授权范围的活动。

11.1.2 多场所认证客户的总部在向 KBRZ 提交《认证申请书》及相关材料时，应按要求提供多场所有关的材料。需要时，认证客户还应提供进一步的材料，以便 KBRZ 获得足够的认证客户信息，具体内容见《认证申请书》。

11.2 审核

11.2.1 要求

KBRZ对多场所认证客户的认证审核将覆盖认证范围内的认证客户总部和场所。KBRZ将根据具体情况，采取文件评审、现场评审中的一项或多项组合的方式并综合运用抽样的方法对多场所认证客户实施审核。

满足下列条件，可实施抽样

所有场所的过程应实质上属于同一类，并按照相似的方法和程序运作。如果其中某些场所实施的过程与其他场所相似，但过程的数量少于其他场所，那么在实施大多数过程或关键过程的场所要接受完整审核的前提下，可以对上述过程数量较少的场所采用多场所认证。

当组织通过位于不同地点但相互关联的过程开展业务时，如果满足本文件的所有其他规定，也可以进行抽样。如果各个地点的过程虽不相似，但明显相互关联，那么抽样计划应至少包括组织实施的每个过程的一个样本（例如，组织在一个地点生产电子元器件，在其他几个地点组装这些电子元器件）。

组织的管理体系应处于一个受到集中控制和管理的计划之下，并接受集中的管理评审。组织的内部审核方案应包括所有相关的场所（包括KBRZ管理职能），并应在认证机构审核开始前按照内部审核方案对所有相关的场所进行了审核。

应证实组织的KBRZ办公室已按照审核所依据的相关管理体系标准建立了管理体系，且整个组织满足该标准的要求。该证实应考虑相关法律法规的要求。

组织宜证实其有权且有能力从所有场所（包括KBRZ办公室）收集数据（包括但不限于下列方面）并进行分析，并宜证实其有权并有能力在必要时实施组织变更

12.2.2 文件评审

若分场所拥有自己的管理体系文件，除对总部统一的管理体系文件实施文件评审外，KBRZ还将对分场所自己的管理体系文件实施文件评审。

12.2.3 多场所审核

12.2.3.1 对各场所实施现场审核的原则

对多场所认证客户的现场审核，包括对总部和分场所的现场审核。当总部或被抽样的分场所拥有多个与认证活动相关的办公地点（如：总部将生产活动的记录存放在核心办公地点以外的地点、实验室与管理职能分处不同地点等）时，KBRZ将到所有办公地点实施审核。

12.2.3.1.1 对总部实施现场审核的原则

对多场所认证客户初次认证、监督和再认证时，应安排对认证客户总部的现场审核；已获认证客户增加场所时，无论是否与监督或再认证结合进行，均应安排对总部的现场评审。

12.2.3.1.2 对场所实施现场审核的原则

KBRZ在选取多场所的样本时，有目的地选取一部分样本，同时随机选取另一部分样本，从而使样本相对于接受抽样的不同场所既具有代表性，又包含随机抽样的成分。

至少25％的样本宜随机选取

1） 抽样方法

当客户组织有很多现场满足下面三个准则，审核必须使用多现场认证抽样方法:

a） 所有现场运行在同一个信息类管理体系体系下，该信息类管理体系体系被集中管理和内部审核、并集中统一进行管理评审;

b） 所有现场被包括在客户组织的内部信息类管理体系审核方案和程序中;

c） 所有现场被包括在客户组织的内部信息类管理体系管理评审方案和程序中;

尽最大可能，初次认证合同评审必须识别现场间的差异以满足确定的适宜的抽样水平。

2）抽样准则

认证机构抽取一个有代表性数量的现场需要考虑：

a） 总部和各分现场的内审结果,

b） 管理评审的结果,

c） 各现场规模的变化,

d）各现场经营目的的变化,

e） 信息类管理体系体系的复杂度,

f） 在不同现场信息安全体系的复杂度,

g） 工作惯例的变化,

h） 所从事活动的变化,

i） 关键信息系统或信息系统处理的敏感信息间的潜在相互影响,

j） 任何不同的法规要求.

有代表性的样本是从客户组织的 信息类管理体系 认证范围内的所有现场挑选出来的;这种抽样选择是基于在反映以上因素的判断选择并考虑了随机抽样原理基础上做出的。

3）样本大小

样本大小计算是基于KBRZ使用的多现场组织抽样的基本程序。

如果发现了不符合项，无论是在总部还是在单独现场，纠正措施程序适用于证书覆盖的总部和所有现场。

审核必须评审客户组织的总部活动，确保单一的信息类管理体系体系适用于所有现场和在运营层面传递总部管理要求。审核必须评审以上要点的所有内容。

通常情况下，按下述比例实施抽查

初次审核：样本的数量宜为分场所数量的平方根（$y=\sqrt{X}$），计算结果向上取整为最接近的整数。

监督审核：每年的抽样数量为分场所数量的平方根乘以0.6（$y=0.6\sqrt{X}$）），计算结果向上取整为最接近的整数。

再认证审核：样本的数量宜与初次审核相同。但是，如果证明管理体系在三年的周期中是有效的，样本的数量可以乘以0.8（$y=0.8\sqrt{X}$），计算结果向上取整为最接近的整数。

中心办公室在初次认证审核和每次再认证审核中都应接受审核，并至少每年在监督中审核一次。

11.3 不符合

11.3.1 如果在任何一个场所发现了轻微不符合，不论该不符合是在组织内部审核还是 KBRZ 审核中发现的，应进行调查，以确定其他场所是否也受到影响。因此，KBRZ 要求组织对不符合进行检查，以确定体系是否存在影响其他场所的整体性问题。如果发现体系存在整体性问题，在 KBRZ 办公室和每个受到影响的场所采取纠正措施并进行验证。如果没有发现整体性问题，组织能够向 KBRZ 证实有正当理由不对其他场所采取纠正措施。

11.3.2 在认证过程中，KBRZ 不允许组织为克服由于某个场所存在不符合造成的问题，而从认证范围中删除存在问题的场所。只有当认证机构和组织在实施认证前就删除达成一致时，才能进行删除。

11.4 认证证书

11.4.1 如果 KBRZ 对认证范围内的每个场所都进行了审核，或使用本部分文件规定的抽样方法对认证范围内的场所进行了审核，那么颁发的认证文件可以覆盖认证范围内的每个场所。

11.4.2 认证证书包含组织 KBRZ 办公室的名称和地址，以及该认证文件涉及的所有场所的清单。认证证书的范围或文件上的其他索引信息应明确由清单中的多场所网络实施的获证活动。如果场所的认证范围只是整个组织认证范围的一部分，认证证书应明确说明每个场所的适用范围。如果认证范围包含临时场所，认证证书中应注明该场所为临时场所。

11.4.3 KBRZ 可以为组织认证范围内的每个场所颁发认证证书，但前提条件是每个场所的认证证书应含有相同的范围，或该范围的一个分范围，并应明确地引用主认证证书。

11.4.4 如果组织的 KBRZ 办公室或任何场所不满足保持认证的必要条件，KBRZ 应撤销所有认证证书。

11.4.5 认证客户在关闭认证所覆盖的任何场所时告知 KBRZ。组织未能提供上述信息，将被 KBRZ 认为是误用认证，此时 KBRZ 按照其程序采取措施。

11.4.6 作为监督审核或再认证活动的结果，或扩大认证范围的结果，KBRZ 可以在现有认证范围中增加新的场所。如果对已认证的多场所网络增加一组新的场所，那么每组新增加的场所宜作为一个单独的总体来确定抽样数量。在新场所纳入证书后，新场所宜和原有场所合并起来确定未来监督或再认证审核的抽样数量。

12. 申请方、获证组织和 KBRZ 的权利与义务

12.1 申请方、获证组织权利

a) 有权自我决策是否提出云计算管理体系认证申请和自由选择认证机构；

b） 向 KBRZ 了解认证程序与要求；

c） 与 KBRZ 协商确定认证采用的标准与审核时间；

d） 对不适宜参加本方审核的人员提出异议；

e） 获证组织有权正确使用认证证书和认证标志，证明其具有证书标明的云计算管理体系的能力，或将认证合格的细节通知用户和/潜在的顾客；也可以在广告上宣传认证资格，展示认证证书和认证标志；

f） 享有申诉与投诉的权利，详见《申诉、投诉处理规则》；

g） 在认证证书有效期内，因产品变化、区域或标准变更，获证组织有权提出扩大、缩小、撤销认证的申请；

h） 在认证证书有效期内，对因 KBRZ 原因（如审核失效或因 KBRZ 被暂停、撤销认证证书等而影响获证组织使用认证证书的），免费享有 KBRZ 的补救措施。

12.2 申请方、获证组织义务

a） 应始终遵守本《认证规则》的有关规定；

b） 为进行认证审核、监督审核、再认证和解决投诉和申诉，申请方应作出必要的安排，包括提供文件、容许 KBRZ 相关人员进入必要区域、调阅必要记录（包括内审报告、相关方投诉记录）和访问有关人员；

c） 获证至应确保不采取误导的方式使用认证文件、标志和《审核报告》中的一部分，不能用认证来暗示其产品或服务得到了 KBRZ 的批准，证书与标志的使用详见《认证证书及标志使用规则》

d） 获证组织在宣传认证结果时，不得损害 KBRZ 的声誉，不允许做使用 KBRZ 认为误导或未授权的生命；

e） 获证组织如接到暂停或撤销认证通知，发生暂停时，暂停期内应立即停止涉及及认证内容的广告，并应暂停使用认证证书、认证标志（包括认证牌匾）或声称取得认证资格；发生撤销/注销情况时，应立即停止及认内容标志，不得以任何借口拖延或无故保留认证证书；

f） 获证组织因扩大、缩小或企业信息变更需换证，均应在新证书换发的同时交回原认证证书；

g） 当管理体系发生变更，或获证组织自出现重大问题时（如发生事故或因上述原因被顾客（相关方）投诉、主管部门查处、媒体曝光等），应即时通报 KBRZ，并将事情的经过、拟采取的措施和措施实施后的结果等内容在规定的期限内书面报告 KBRZ，执行《获证组织管理体系信息通报程序和要求》；

h） 应接受 KBRZ 非定期监督审核和/或配合认证行业管理部门的监督检查等。

12.3 KBRZ 的权利

a） 在拟开展的云计算管理体系认证领域范围内，制定《认证规则》，实施认证和作出认证

决定；

b） 要求申请方、受审核方和获证组织提供有关认证审核、监督和再认证所必须的资料；

c） 要求获证组织提供鼓励体系变更信息和报告重大事故；并要求获证组织在规定期限内提供其所采取措施的资料；对于其不能提供的，KBRZ 将根据认证认可有关文件规定，实施非例行检查或对认证证书作出暂停、撤销处理；

d） 对获证组织管理体系的运行情况进行定期监督审核或非定期监督审核；对不接受或不配合监督检查（或确认审核、稽查）的，KBRZ 将根据认证认可有关文件规定，有权对认证证书作出暂停、撤销处理；

e） 对获证组织错误使用认证证书与标志的行为，KBRZ 将根据有关文件规定，有权对认证证书作出暂停、撤销处理；

f） 对获证组织因变更需换证或证书失效不交回原证书时，KBRZ 将根据有关文件规定，有权对认证证书作出暂停、撤销处理；

g） 处理来自申请方、受审核方、获证组织或其他有关方面对 KBRZ 的投诉和/或申诉；

h） 调阅获证组织的顾客投诉和所采取措施的记录；

i） 根据认证合同向申请方、获证组织收取认证费用。

j） 对认证过程中的利益冲突加以管理，确保认证活动的公正性；认证要求更改时，及时修改《认证规则》并通知申请方和获证组织；

k） 对足够的客观证据进行评价，并在此基础上作出认证决定；

l） 对申请方、受审核方和获证组织提供的信息与资料进行保密；

m） 除政策、法规要求保密的组织以外，通过公司官方网站（www.bjkbrz.com）公布获证组织名录，包括组织名称、地址、获证日期、证书有效期、证书编号和认证范围等信息；公布获证组织证书状态；

n） 根据政策、法规要求，向国家认监委、地方认监部门和中国认证认可协会上报获证组织信息；当上述单位需要调阅获证组织资料时，将拟提供的资料提前通知获证组织；

o） 解答申请方、受审核方和获证组织就管理体系认证提出的疑义，提供的信息应准确且不使人产生误解；

p） 当申诉、投诉表明认证过程出现错误、疏忽或不合理行为时，采取必要的措施并通报申（投）诉组织（人员）。

13.受理组织的申、投诉

13.1 申、投诉受理及处理

组织对认证申请的不受理、中止审核、拒绝认证、撤销认证或缩小已获得的认证范围等有关的决定提出重新考虑的请求、认证客户或获证组织对认证决定有异议时，可让KBRZ提出申诉；

任何人员或相关的机构对KBRZ可能涉及认证政策、认证运作过程和认证结果及认证人员的表现等的不满，对获证方可能涉及产品及认证证书与认证标志使用等的不满，均可随时向KBRZ的综合部提出投诉，其投诉可以书面信函、来人反映或以其它渠道的方式进行；

KBRZ接受申、投诉并且及时进行处理，申投诉的处理具体按KBRZ-CX15 《申诉投诉处理程序》执行；与客户及投诉人共同决定是否将投诉事项公开，并在决定公开时，共同确定公开的程度。

若认为KBRZ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。

坤标认证投诉电话：010-84631655，认监委投诉010-56738610

13.2 费用

申、投诉处理的合理费用由败诉方承担。

14.信息通报要求

14.1 获证组织发生可能影响管理体系运行的重大变化，应于决定之日起 10 日内报送 KBRZ。（如：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、最高管理者变更；认证联系人变更；生产经营或服务的工作场所变更；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）

14.2.获证组织发生客户及相关方有重大投诉；生产、销售的产品或提供的服务质量或市场监管部门认定不合格；发生产品和服务的质量事故、安全事故、环境污染；应在发生之日起十日内，将相关资料和自查结论报送 KBRZ。

15.认证收费标准

KBRZ严格执行《中国认证认可行业自律公约》和《认证机构诚信经营规范》（2015-5-1实施），制定了KBRZ管理体系认证收费标准，确保认证收费符合要求。

基本收费项目

序号	收费项目	收费标准	备注
1.	申请费	1500元	
2.	审核费	3500元/人日	按所需人日数执行
3.	审定与注册费	2000元	含证书正本一套
4.	换证费	200元	证书内容变更，换发证书。
5.	证书副本	200元	每张100元
6.	翻译费	200元	
7.	差旅费	根据实际支出收取	

16.认证记录的管理

16.1 KBRZ 对所有客户（包括所有提交申请的组织、接受审核的组织和获得认证或被暂停或撤销认证的组织）保持审核及其他认证活动的记录。

16.2 获证组织记录包括以下内容：

a）申请资料及初次认证、监督和再认证的审核报告；

b）认证协议；

c）适用时，多场所抽样方法的理由；

注：抽样方法包括为审核特定管理体系和（或）在多场所审核中选取场所而做的抽样。

d）确定审核时间的理由；

e）纠正与纠正措施的验证；

f）投诉和申诉及任何后续纠正或纠正措施的记录；

g）适用时，技术委员会的审议和决定；

h）认证决定的文件；

i）认证文件，包括与产品（包括服务）、过程相关的认证范围，适用时，包括每个场所相应的认证范围；

j）建立认证的可信度所需的相关记录，如审核员和技术专家能力的证据；

k）审核方案。

16.3 KBRZ 建立文件 KBRZ-CX12《记录和档案管理程序》，记录认证活动全过程并妥善保存。

16.4 记录真实准确以证实认证活动得到有效实施。记录资料使用中文，保存期限为两个认证周期。

16.5 以电子文档方式保存记录的，采用不可编辑的电子文档格式。

16.6 所有具有相关人员签字的书面记录，制作成电子文档上传到认证信息管理系统，纸质版原件由 KBRZ 存档管理，保存时间期限为两个认证周期。