信息类管理体系认证规则

KBRZ-GZ-14

北京坤标检验认证有限公司

目 录

1.适用范围 4

2. 引用文件 4

3. 术语和定义 4

4. 总则 5

5.审核类别和审核方式 7

6.审核人员、技术专家、审核组要求 7

7.认证信息公开 7

8. 初次认证 7

8.1 初次认证申请 7
8.2 初次认证的审核方式 10
8.3 初次认证的审核实施 10
8.4 初次认证的纠正措施验证 11
8.5 初次认证的审核报告 11
8.6 初次认证的认证决定 11

9. 监督审核 11

9.1 例行监督审核的方式 11
9.2 例行监督评审的时间间隔 11
9.3 例行监督评审的准备 12
9.4 例行监督审核的实施 12
9.5 例行监督审核的纠正措施验证 12
9.6 例行监督评审的审核报告 12
9.7 例行监督审核的评定 12
9.8 扩大认证范围的审核 12
9.9 非例行监督 12

10. 再认证 12

10.1 再认证申请 13
10.2 再认证的审核方式 13
10.3 再认证审核前准备 13
10.4 再认证的审核实施 13
10.5 再认证的纠正措施验证 13
10.6 再认证的审核报告 13
10.7 再认证的认证决定 13

11. 暂停和撤销认证的规则 13

11.1 暂停认证 13
11.2 撤销认证 14

12. 认证证书及标志使用 15

12.1 认证证书和标志 15
12.2 认证证书和认证标志的使用 15
13. 与其他管理体系的结合审核 16
14. 多场所客户的审核和认证 16
14.1 认证申请与受理 17
14.2 审核 17
14.3 不符合 19
14.4 认证证书 19
15. 申请方、获证组织和 KBRZ 的权利与义务 20
15.1 申请方、获证组织权利 20
15.2 申请方、获证组织义务 20
15.3 KBRZ 的权利 21
16. 受理组织的申诉 22
16.1 申诉 22
16.2 投诉 23
17. 信息通报要求 24
18. 认证收费标准 24
附录 A 信息安全管理体系人天计算表 26
附录 B 信息技术服务管理体系人天计算表 34
附录 C 云服务信息安全管理体系人天计算表 38
附录 D 通用数据保护条例管理体系人天计算表 41
附录 E 公有云个人信息安全管理体系人天计算表 43
附录 F 隐私信息安全管理体系人天计算表 46

北京坤标检验认证有限公司简介

北京坤标检验认证有限公司（以下简称 KBRZ）成立于 2013 年 7 月 31 日，经北京市工商行政管理局朝阳分局登记注册的具有独立法人资格的股份制公司，注册资金 330 万元。

KBRZ 是经中国国家认证认可监督管理委员会批准（批准号：CNCA-R-2015-186）从事质量、环境、职业健康安全、信息安全、信息技术等管理体系认证、服务认证、产品认证等认证活动的第三方认证机构。

根据公司的自身运营特点及维护认证活动的公正性考虑，公司设立了公正性委员会、监督和规范认证行为，维护认证的公正性；处理认证业务中的技术问题，纠正认证活动的偏差，防止认证活动偏离轨道。设置了技术委员会、运营管理部、综合管理部、技术质量部、财务部 5 个管理部门。

总经理要求全体员工“秉承以事实为依据，以标准为准绳开展认证活动，避免任何行政权利、经济利益、人际关系对认证工作的影响是我们的基本要求。遵守诚实守信的认证之本，以严谨科学的态度、一丝不苟的作风、务实求真的精神、公开透明的认证信息，向所有申请认证方提供热情、周到和增值的服务，把履行认证机构的社会责任为己任，提高认证活动的公信力”。保持对顾客的持续关注与沟通，对自身的持续改进与提高是坤标人不懈的追求目标。

KBRZ 致力于打造具有自身优势的认证服务特色，希望与客户建立起长期的战略合作关系，通过认证及其他增值服务工作，来促进客户提高管理体系运行的有效性和效率，实现从优秀到卓越的跨越。

KBRZ 拥有一支实践经验丰富、理论功底深厚、能够胜任工作的审核员队伍。随着认证事业的不断发展，专、兼职审核员队伍将不断壮大，专业结构、知识结构、年龄结构、地域结构将逐步趋于合理。KBRZ 致力于建设一支具有团队精神、敬业精神，良好职业素质，打得了硬仗的审核员队伍，以适应认证事业发展的需要。

地址：北京市朝阳区望京园 601 号楼 26 层 3005

邮编：100102

电话：010-84631655/84622396

传真：010-64780891

网址：http://www.bjkbrz.com/

1.适用范围

1.1 本规则用于规范 KBRZ 的信息类管理体系认证活动，包括：信息安全管理体系、信息技术服务管理体系、云服务信息安全管理体系、GDPR 通用数据保护条例管理体系、公有云个人信息安全管理体系、个人身份信息保护实践管理体系、隐私信息安全管理体系等。

1.2 本规则旨在遵守认证认可相关法律法规及国家技术标准，对信息类安全管理体系认证实施过程作出具体规定，确保 KBRZ 对认证过程的管理和相应责任。

1.3 本规则是对 KBRZ 从事信息类安全管理体系认证活动的基本要求，公司各部门从事该项认证活动应当遵守本规则。

2.引用文件

下列文件中的条款通过本文件的引用而成为本文件的条款。以下引用的文件，注明日期的，仅引用的版本适用；未注明日期的，引用文件的最新版本（包括任何修订）适用。

2.1 信息安全管理体系认证以 ISO/IEC 27001 为认证依据。

2.2 信息技术服务管理体系认证以 ISO/IEC 20000-1 为认证依据。

2.3 云服务信息安全管理体系认证以 ISO/IEC 27001、ISO/IEC27002、ISO/IEC 27017 信息技术 安全技术 基于 ISO/IEC 27002 信息安全控制的云服务-实施要求为认证依据。

2.4 GDPR 通用数据保护条例管理体系认证以 GB/T 22080/ISO/IEC27001、GB/T 22081/ISO/IEC27002、GDPR 通用数据保护条例-要求为认证依据。

2.5 公有云个人信息安全管理体系认证以 ISO/IEC 27001、ISO/IEC 27002、ISO/IEC 27018/ GB/T 41574 为认证依据。

2.6 个人身份信息保护实践管理体系认证以 GB/T 22080/ISO/IEC27001、GB/T 22081/ISO/IEC27002、ISO/IEC 29151 为认证依据。

2.7 隐私信息安全管理体系认证以 GB/T 22080/ISO/IEC27001、 GB/T 22081/ISO/IEC27002、ISO/IEC 27701 安全技术 ISO/IEC27001 和 ISO/IEC27002 的隐私信息管理的扩展-要求和指南为认证依据。

3.术语和定义

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.总则

4.1 KBRZ 依据国家有关法律法规、相关认可规范、规则和国家标准等开展对申请组织的信用评价活动。

4.2 KBRZ 对申请组织的认证活动遵循客观公正、科学规范、权威信誉、廉洁高效和非歧视的原则。

a) 客观性：应对采集到的被评对象信息进行尽职调查，并采取相应方法核实比对，务求真实客观反映其状况。

b) 独立性：应不带有任何偏见、不受任何外来因素影响，独立、公正地反映被评对象的状况。

c) 审慎性：在对被评对象进行分析、评价的过程中，尤其在被评对象提供的信息不完备或不能核实的情况下，应持审慎态度。

d）目的性：评价内容应根据评价目的,选择设计包括能反映本领域服务质量要素和服务质量特性状况的关键信息。

e）可操作性：评价内容应实用,评价方法可行。相关信息要素可采集、可量化,便于操作。

f）全面性：根据评价的目的,选取评价指标时应全面准确反映顾客对服务的需求。

g）回避原则：KBRZ 应对委托方委托事项进行初步判断，再行签订合同。主要判断事项应包括是否需要进行从业回避等。

其中，从业回避主要包括但不限于下列规定：

1）KBRZ 与被评对象存在资产关联或者其他利害关系，可能影响评价活动客观公正性的，KBRZ 不得提供有关该被评对象的评价报告；

2）KBRZ 高级管理人员近 1 年内曾在被评对象任职，或其直系亲属目前在被评对象担任高级管理职务的，KBRZ 不得提供有关该被评对象的评价报告；

3）KBRZ 高级管理人员与被评对象有除评价业务收费之外的其它重大经济利益关系，KBRZ 不得提供有关该被评对象的评价报告；

4）评价人员近 1 年内曾在被评对象任职，或其直系亲属目前在被评对象担任高级管理职务的，该评价人员应予回避；

5）评价人员与被评对象有除评价业务收费之外的其它重大经济利益关系，该评价人员应予回避。

4.3 KBRZ 不对申请认证的组织提供可能影响认证公正性的咨询或其他服务。

4.4 KBRZ 对承诺满足法律法规要求开展经营活动的组织实施认证。

4.5 在认证申请或初次认证评价的任何阶段，若有证据表明服务组织存在欺诈行为、故意提供虚假信息或隐瞒信息，KBRZ 将不予受理。

4.6 KBRZ 对申请认证的组织的申请材料内容、认证评价信息和其他非公开信息保守秘密。在法律法规要求时，KBRZ 有责任将申请组织的相关信息向有关部门通报。

4.7 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的信用评价达到相关标准要求，始终一致地达到认证标准和符合认证要求的责任，在于认证客户而不是 KBRZ。

4.8 KBRZ 对认证资格的处理，执行本规则第 11 条。

4.9 获证客户以其他适当方式对外宣传获证信息，执行本规则第 12 条。

4.10 与其他管理体系（评价体系）的结合评价，执行本规则第 13 条。

4.11 KBRZ 对具有多场所认证客户的认证，执行本规则第 14 条。

4.12 申请方、获证组织的权利与义务，执行本规则第 15 条。

4.13 KBRZ 对认证客户的申诉处理，执行本规则第 16 条。

4.14 获证客户应向 KBRZ 通报有关信息。执行本规则第 17 条。

4.15 对认证客户的认证服务收费，执行本规则第 18 条，不接受任何组织或其他认证活动相关利益方的资助。

5.审核类别和审核方式

审核类别分为初次认证审核（包括一阶段和二阶段审核）、监督审核、再认证审核和特 殊审核。

审核方式分为现场审核、远程审核。

6.审核人员、技术专家、审核组要求

审核人员必须取得认证注册资格，并得到 KBRZ 的专业能力评价，以确定其能够胜任所安排的审核任务。

技术专家必须得到 KBRZ 的专业能力评价，以确定其能够胜任所安排的技术支持工作。审核组应由能够胜任所安排的审核任务的审核员组成。必要时可以补充技术专家以增 强审核组的技术能力，技术专家应在审核员的监督下进行工作，可就受审核组织管理中技术充分性事宜为审核员提供建议，但技术专家不能作为审核员。

7.认证信息公开

KBRZ 应向申请认证的社会组织（以下称申请组织)至少公开以下信息：

1) 认证服务项目；

2) 认证工作程序；

3) 认证依据；

4) 证书有效期；

5) 认证收费标准等。

8.初次认证

8.1 初次认证申请

8.1.1 申请认证的条件：

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）。

8.1.2 申请人应提交《认证申请书》及其要求的文件等申请材料。

需要时，申请人还应提供进一步的材料，以便 KBRZ 获得足够的认证客户信息。包括但不限于：

1）组织基本信息，包括业务活动、组织架构、联系人信息、物理位置和体系范围 等基本内容；

2）法律地位资格证明（营业执照、事业单位法人证书或社会团体法人登记证书）；

3）申请认证的范围；

4）涉及的管理体系过程；

5）管理体系正式运行的时间、内审时间、管理评审时间；

6）取得相关法规规定的行政许可文件、相关法律法规要求的其他证明文件(适用时）

7）适用性声明；

8）信息类管理体系申请的其他要求。

以上资料加盖公章。

8.1.3 在提交《认证申请书》时，申请人应按照认证收费标准表交纳认证申请费。

8.1.4 KBRZ 在收到认证申请后,进行申请评审，解决双方在理解上的差异，必要时可对申请人进行访问。

1) 通过申请评审的，KBRZ 将向申请人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

2) 不符合申请条件的，KBRZ 将向申请人发出不受理申请的通知，并阐明理由。

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

KBRZ 应根据认证依据、程序等要求，在三个工作日内对申请组织提交的认证申请书及其

相关资料进行评审并保存评审记录，做出评审结论，以确定：

1) 所需要的基本信息都得到提供；

2) 申请组织的行业类别和与之相对应的业务过程特性和要求；

3) 国家对相应行业的管理要求；

4) 申请组织管理体系运行时间满三个月，已完成内部审核和管理评审；

5) KBRZ 与申请组织之间任何已知的理解差异得到消除；

6) KBRZ 有能力并能够实施所申请的认证活动；

7) 申请的认证范围、申请组织的运作场所、完成审核需要的时间和任何其他影响认证活动的因素；

8) 核算并确定审核人日；

9) 根据申请认证的活动范围及场所、从事活动的影响、员工人数、完成审核所需时间 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，不予受理其认证申请。

KBRZ 应建立审核人日确定准则，根据受审核组织的规模、特性、业务复杂程度、管理涵盖的范围、认证要求和其承担的风险以及采取审核方式等因素核算并确定审核人日，以确保审核的充分性和有效性。确定的人日数记录在审核方案记录中。

8.1.5 建立审核方案

在申请评审后，KBRZ 应针对申请组织建立审核方案（申请组织变更为受审核组织），并由专职人员负责管理审核方案。审核方案的范围与程度应基于受审核组织的规模和性质，以及受审核方服务的性质、功能、复杂程度以及成熟度水平。

审核方案应包括在规定的期限内有效和高效地组织和实施审核所需的信息和资源，应 包括以下内容：

1) 审核方案的目标；

2) 审核的范围与程度、数量、类型、持续时间、地点、日程安排，确定审核范围应考虑如下要求：

a) 初次认证、再认证审核内容为认证依据的全部条款；

b) 监督审核采取抽样的方式进行，两次监督审核必须覆盖标准所有适用条款。

3) 审核准则；

4) 审核方式；

5) 审核组的选择；

6）所需的资源，包括交通和食宿；

7）确定的审核人日；

8）处理保密性、信息安全、健康和安全，以及其它类似事宜。

8.1.6 初次认证审核

8.1.6.1 初次认证的准备

KBRZ 应依据第 6 章中的审核组组建原则，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人。申请人如对评审组组成有异议，可向 KBRZ 提出。。

8.1.6.2 制定审核计划

审核组结合受审核组织的申请材料、审核方案对审核的策划以及上一次审核（如果有）的结果，对审核做出具体安排，包括但不限于审核的目的、内容、具体的时间安排、审核组成员对受审核组织按岗位和活动以何种方式进行审核的安排、高层沟通的安排和会议的安排。审核组长应至少在开展审核三个工作日之前，与受审核组织就审核计划进行充分沟通，确保双方没有异议。

8.2 初次认证的审核方式

初次认证审核应分两个阶段实施：第一阶段和第二阶段。

8.3 初次认证的审核实施

8.3.1 第一阶段

8.3.1.1 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，申请人实施纠正，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。

8.3.1.2 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，并提前通知申请人。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人代表进行沟通确认，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

8.3.1.3 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。

8.3.2 第二阶段

审核组编制二阶段审核计划，并提前通知申请人。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，对申请人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人代表予以确认，并提出不符合报告。

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

8.4 初次认证的纠正措施验证

二阶段审核开出的不符合，严重不符合和轻微不符合受审核方应在 3 个月内完成经纠正措施并验证合格；特殊情况下，严重不符合不超过 6 个月；如逾期未能有效关闭不符合，KBRZ 将按要求对其认证资格进行处置。

8.5 初次认证的审核报告

不符合的纠正措施验证完成后，由审核组长完成审核报告，并提出推荐结论。

8.6 初次认证的认证决定

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

通过认证决定后，KBRZ 为申请人颁发有效期为 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。

9.监督审核

例行监督评审

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

9.1 例行监督审核的方式

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。

9.2 例行监督评审的时间间隔

9.2.1 初次认证后的第一次监督审核应在认证证书签发日起 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。

9.2.2 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。

9.2.3 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。

9.3 例行监督评审的准备

9.3.1 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。

9.3.2 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。

9.4 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。

9.5 例行监督审核的纠正措施验证

例行监督审核中开出的轻微和严重不符合，应在 1 个月内完成纠正措施验证。

9.6 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。

9.7 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。

9.8 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 在受理申请后按有关要求完成审核方案策划、审核组委派和审核实施，工作流程与初次认证中的有关过程相同。审核中开出的轻微不符合和严重不符合在 1 个月内完成纠正措施验证。

9.9 非例行监督

当出现下列情况时，KBRZ 将对获证客户进行非例行监督审核

a) 收到相关方对获证客户的投诉；

b) 获证客户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) 获证客户被有关行政监管部门查处、媒体曝光；

d) KBRZ 认为有必要时。

10. 再认证

10.1 再认证申请

申请人应在认证证书有效期截止 3 个月前向 KBRZ 提出再认证申请，如果认证客户未按时提供齐全的再认证申请材料，造成认证证书有效期到期还未做出认证决定，将导致认证失效。再认证申请过程按本文件初次认证的有关过程实施。

10.2 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。

10.3 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。

10.4 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。

10.5 再认证的纠正措施验证

审核中开出的轻微不符合，应在 1 个月内完成纠正措施验证；或在认证证书到期前完成纠正措施验证；

如果在当前认证证书终止日期前，认证客户未能完成再认证审核或对严重不符合项实施的纠正和纠正措施未能进行验证，则不予以再认证，也不延长原认证证书的有效期。

在当前认证证书到期后，如果认证客户能够在 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。

10.6 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。

10.7 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。

11. 暂停和撤销认证的规则

获证客户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为暂停和撤销认证的，KBRZ 在调查核实后的 5 个工作日内做出决定。

若信息类管理体系的认证证书暂停或撤销时，KBRZ 认证证书会同时进行暂停或撤销

11.1 暂停认证

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) 获证客户的产品、活动出现安全事故，经确认是获证客户造成的；

f) 被有关执法监管部门责令停业整顿的；

g) 获证客户向 KBRZ 提供的与认证有关的信息或相关证据严重失实的；

h) 获证客户未按《认证合同》规定按期缴纳认证费用的；

i) 获证客户不能再规定时限内接受监督审核或再认证审核的；

j) 获证客户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) 获证客户主动请求暂停的；

n) 其他应当暂停认证证书的。

暂停时间为不超过 6 个月，涉及获证客户全部或部分认证范围。KBRZ 将向获证客户发出《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。获证客户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。

11.2 撤销认证

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，或认证机构已要求其纠正但超过规定时间仍未纠正的；

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。

当获证客户部分认证范围无法满足规定要求时，可缩小部分认证范围；当获证客户全部认证范围无法满足规定要求时，撤销认证证书。KBRZ 向获证客户发出《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。

12. 认证证书及标志使用

12.1 认证证书和标志

a） 认证证书：KBRZ 颁发给获准认证的组织，表明所确定的范围已被认证的一组正式文件，包括符合特定认证标准的证明、相关附件；

b） KBRZ 徽标：代表 KBRZ 本身的图形符号；

c） 注册号：KBRZ 授予已认证组织的唯一性代码；

d） 标志：表明某种状态的图形符号。标志包括认证标志；

e） 认证标志：KBRZ 颁发的、供获准认证组织使用、表示其认证资格的图形符号。KBRZ 徽标与组织的注册号如下图所示共同构成认证标志；

f） 信息类管理体系认证标志

KBRZ 徽标

12.2 认证证书和认证标志的使用

a） 认证客户应对认证证书和认证标志的使用进行管理；

b） 认证证书的正确使用方法：在宣传、投标等活动中展示认证证书，也可在文件、信签、广告和有关宣传材料上影印认证证书，使用必须完整，不得变形使用；

c） 认证证书/标志的使用者必须是认证证书（特别是有主/子证书的情况）所载明的认证组织（即在证书中所列出的获证组织名称），除此之外其他任何单位不得使用该认证证书/标志。拥有认证证书/标志使用权的组织，应在其认证证书限定的“审核地址”、“产品服务”及其过程等认证证书所明示的范围内使用，不得超出认证证书中限定的各自范围。有关方错误使用认证证书/标志带来的一切法律责任由使用者承担；

【案例 1：仅集团公司总部单独获证的，集团公司下属分/子公司无权使用该证书（包括宣传、投标等活动）；同样，集团公司总部和集团公司下属的分/子公司 A 获证，集团公司下

属的分/子公司 B 或其他分/子公司均无权使用该证书（包括宣传、投标等活动）；当集团公司总部与集团公司下属的分/子公司 A 的认证范围不一致时，集团公司总部与分/子公司 A 应仅在认证证书限定的各自范围内使用；】

d) 认证客户不得变造、转让甚至非法买卖认证证书，也不得在知情的前提下容许他人或组织利用本组织的认证证书伪造、变造或冒用认证证书；

e) 获证客户不得利用管理体系认证证书和相关文字、符号，误导公认为其产品、服务通过认证。或者能够组织的管理体系发生重大变化时，应当向 KBRZ 申请变更，未变更或者经 KBRZ 调查发现不符合认证要求的，不得继续使用该认证证书；

f) KBRZ 拥有认证标志的所有权，并授权获证客户在认证范围和认证有效期内按照本文件的规定使用认证标志。获证客户拥有认证标志使用权，使用前须经 KBRZ 对其使用方式进行认证、加以备案，未经 KBRZ 允许，不得转让认证标志使用权；

g) 获证客户可以将认证标志用在报告、证书、文件、办公用品、宣传片、网页等（实验室除外）。可以采用印刷、图文和印章等使用方式；

h) 获证客户在使用认证标志（包括印章和电子图形）时，应保证认证标志的完整，可按比例放大或缩小，但应确保认证标志的颜色与认证机构的徽标颜色一致并清晰可辨；

i) 被暂停或缩小认证资格的组织，在被暂停或缩小的范围内应立即停止任何关于获得 KBRZ 认证的宣传，并应立即停止在证书、报告、文件、宣传品上继续使用认证标志；

j) 被撤销认证资格的组织应立即停止任何关于获得 KBRZ 认证的宣传，并应立即停止在证书、报告、文件、宣传品、办公用品等上继续使用认证标志；

k) 当获证客户因认证标志引起法律诉讼时，应及时通告 KBRZ;

l) 必要时，KBRZ 将与获准认证的组织协商制定对认证标志使用的其他要求，并形成相关文件；

m) 原则上，获证客户不得将认证标志用在产品上，除非按照第 13 条规定使用认证标志；

n) KBRZ 有权对获证组织使用认证证书和认证标志的情况进行监督，一旦发现获证组织有错误使用认证证书和认证标志现象，可以责成其采取纠正措施，并视情节轻重采取暂停直至撤销其认证证书的措施，也可以上报国家认证认可监督管理委员会进行处理；

o) 任何情况下，云计算管理体系获证客户不得使用认证标志或 IAF-MLA 国际互认标志

13.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。

14.多场所客户的审核和认证

14.1 认证申请与受理

14.1.1 申请有多场所认证的初次认证客户，除满足本规则第 8.1 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。

14.1.2 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》。

14.2 审核

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

14.2.1 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。

14.2.2 多场所审核

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。

14.2.2.1 对各场所实施现场审核的原则

14.2.2.1.1 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。

14.2.2.1.2 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下，该信息类管理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。

14.3 不符合

14.3.1 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。

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。

14.4 认证证书

14.4.1 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。

14.4.2 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。

14.4.3 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。

14.4.4 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。

14.4.5 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。

14.4.6　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。

15.申请方、获证组织和 KBRZ 的权利与义务

15.1 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。

15.2 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。

15.3 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）。

16.受理组织的申诉

认证客户或获证组织对认证决定有异议时，KBRZ 接受申诉并且及时进行处理，在 60 日内将处理结果形成书面通知送交申诉人。

书面通知告知申诉人，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 010-82262841。

16.1 申诉

16.1.1 申诉的提出

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，应在 10 个工作日内以书面形式提交综合部。

16.1.2 申诉的受理

综合部接到申诉一周内做出是否受理的决定，并给申诉方发《申诉、投诉和争议受理通知书》。

16.1.3 申诉的处理

(1)如决定受理，将材料转交相关部门，对认证申请的不受理的申诉，由市场部负责处理；中止审核的申诉由审核部负责处理；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的申诉由技术部负责处理，各部门根据申诉事项的具体情况，决定采取相应措施取证， 包括召集会议听取双方证词、现场调查、向专家咨询等方式进行调查并做出有根据的判断。

(2)如采用会议方式应在接到申诉的 20 个工作日内举行，至少提前 5 个工作日通知申诉人会议的时间和地点。

(3)被诉方和申诉方均有权提出证人、证据，所提出的证人、证据，应在不迟于会议召开 / 现场调查 / 向专家咨询前 5 个工作日内以书面形式提出。

(4)裁定

技术部组织相关的人员做出公正判断，提出书面裁定报告，参与做出决定的所有成员均受认可规范及本文件的约束。

对申诉做出的裁定在经本文件职责规定的主管领导批准后，由综合部书面通知有关各方，该裁定具有约束力。申诉方如还有不同意见，可向公正性委员会以至上级管理机关提出申诉。自综合部受理申诉 3 个月内，KBRZ 必须对申诉做出决定，例外情况下可提交 KBRZ 公正性委员会做出最终决定。特殊情况下需延期处理的，由主管领导批准后在 3 个月时效期内提前 10 天告知申诉方。

(5)若重复受理类似的申诉问题，相关部门部长/主管领导应组织制定出文件化的管理制度来回应申诉的过程。

(6)对申诉的决定应由与申诉事项无关的人员做出，或经其审查和批准，并由综合部告知申诉人。

(7)在申诉处理过程结束时，由综合部正式通知申诉人。

16.1.4 费用

申诉处理的合理费用由败诉方承担。如果是由申诉人支付申诉有关的全部或部分费用，将用保证金结清，余款退还申诉人。若保证金不足，申诉人应自处理决定生效之日起 10 日将不足部分支付 KBRZ。

16.2 投诉

16.2.1 投诉的提出

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，关注和重视有关方投诉信息的收集。

16.2.2 投诉的受理

综合部接到投诉一周内做出是否受理的决定，并给投诉方发《申诉、投诉和争议受理通知书》。

16.2.3 投诉的处理

16.2.3.1 综合部依据投诉材料（包括匿名投诉）进行初步调查，收集与核实对投诉进行确认所需的一切信息，经确认后交由相关部门处理，各部将处理的决定及理由（各部门主管签字）回馈给综合部，综合部自受理起 30 个工作日内将处理意见或措施，以书面方式通知投诉人或相关方。

16.2.3.2 若投诉表明 KBRZ 的质量管理体系存在的问题，则由主管部门分析不符合原因，采

取必要的措施予以纠正。

16.2.3.3 如果投诉与获证客户有关，在调查投诉时应考虑获证管理体系的有效性。对于针对获证客户的投诉，综合部还应在适当的时间将投诉告知该客户。

16.2.3.4 对投诉的决定应由与投诉事项无关的人员做出，或经其审查和批准，并由综合部告知投诉人。

16.2.3.5 投诉人需要时，综合部应向投诉人提供投诉处理的进展报告和结果。在投诉处理过程结束时，由综合部正式通知投诉人。

16.2.3.6 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。

17.信息通报要求

17.1 获证客户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）

17.2.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。

18.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	

审核基础人日按附录中所列计算，未列明的参考类似管理体系结果项目风险计算。

附录 A 信息安全管理体系人天计算表

1.审核人天

表 B.1 中所引用的“审核时间”，是根据审核中花费的“审核人天”来阐述的。附录 B 的计算基础是一个 8 小时的工作日。

2.临时场所

临时场所是认证文件所注明的场所之外的位置，其活动在认证范围内并在规定的时间周期内实施。此类场所范围可从大项目管理场所到较小的服务或安装场所。在确定对这些场所的访问需求及其抽样范围时，宜基于在临时场所发生的不符合而导致没能满足信息安全目标的风险的评价。所选择的场所样本宜考虑活动的规模与类型和项目进展的不同阶段，并体现组织的能力需求和服务差异的范围。对于一般的抽样，见本文件的 9.1.5.1。

3. 确定初次认证审核时间的程序

3.1 总则

审核时间的计算,应遵从文件化的程序。

3.2 远程审核

如果使用了远程审核技术（例如:基于网络的交互式协作、网络会议、电话会议和/或电子验证组织的过程)与客户组织接触，这些活动宜在审核计划中加以识别（见 9.2.3)，可以考虑将其作为现场审核时间的一部分。

如果认证机构制定的审核计划中远程审核活动占据了大于 30%的现场审核时间，认证机构宜证实审核计划的合理性，并在审核计划实施前得到认可机构的专门批准。

注:现场审核时间是指分配给单个场所的现场审核时间。对远程场所的电子审核被视为远程审核,即使电子审核是在组织的物理场所进行。

3.3 审核时间的计算

表 B.1 给出了初次审核天数平均值的起点(在此处及后面的内容中，这个数值包括一次初次审核（第一阶段和第二阶段）的天数)。经验表明，对于一个覆盖了给定数量的、在组织控制下工作的人员的 ISMS 范围来说，这一数值是适当的。经验还表明，对于相似规模的 ISMS 范围，有些需要多的审核时间,有些需要少的审核时间。

表 B.1 提供了审核策划应使用的框架。该表基于在组织控制下工作的、所有班次的

人员的总数来识别审核时间的起点，然后根据适用于所审核的 ISMS 范围的重要因素来调整它，并对每一个因素赋予增、减权重以修正基数。使用表 B.1 时应考虑促成因素和最大偏移的限制（见 B.3.4 和 B.3.5)。B.2 解释了表 B.1 中所使用的术语，附录 C 提供了如何计算审核时间的示例。

表B.1 审核时间表

在组织控制下工作的人员的数量	QMS初次审核审核时间（审核人日）	EMS初次审核审核时间（审核人日）	ISMS初次审核审核时间（审核人日）	增加或减少的因素	总审核时间
1～10	1.5-2	2.5-3	5	见本附录B.3.4	
11～15	2.5	3.5	6	见本附录B.3.4	
16～25	3	4.5	7	见本附录B.3.4	
26～45	4	5.5	8.5	见本附录B.3.4	
46～65	5	6	10	见本附录B.3.4	
66～85	6	7	11	见本附录B.3.4	
86～125	7	8	12	见本附录B.3.4	
126～175	8	9	13	见本附录B.3.4	
176～275	9	10	14	见本附录B.3.4	
276～425	10	11	15	见本附录B.3.4	
426～625	11	12	16.5	见本附录B.3.4	
626～875	12	13	17.5	见本附录B.3.4	
876～1175	13	15	18.5	见本附录B.3.4	
1176～1550	14	16	19.5	见本附录B.3.4	
1551～2025	15	17	21	见本附录B.3.4	
2026～2675	16	18	22	见本附录B.3.4	
2676～3450	17	19	23	见本附录B.3.4	
3451～4350	18	20	24	见本附录B.3.4	
4351～5450	19	21	25	见本附录B.3.4	
5451～6800	20	23	26	见本附录B.3.4	
6801～8500	21	25	27	见本附录B.3.4	
8501～10700	22	27	28	见本附录B.3.4	
＞ 10700	沿用以上规律		沿用以上规律	见本附录B.3.4	

3.4 调整审核时间的因素

不能孤立地使用表B.1。所安排的时间，还应考虑以下因素。这些因素与ISMS复杂程度相关,并因此与ISMS审核工作量相关。

a）ISMS 的复杂程度（例如，信息的关键程度、ISMS 的风险状况）；b）ISMS 范围内所开展的业务的类型;

c)以往已证实的 ISMS 绩效;

d)在 ISMS 各部分的实施过程中，所应用的技术的水平和多样性[例如，不同 IT 平台的数量、隔离网络的数量];

e） ISNS 范围内所使用的外包和第三方安排的程度;f)信息系统开发的程度;

g）场所的数量和灾难恢复场所的数量;

h)对于监督或再认证审核:符合 CNAS-CC013.5.3 条款的、与 ISMS 相关的变更的数量和程度。

附 C 提供了在计算审核时间时如何考虑这些不同因素的示例。需要增加审核时间的其他因素，例如:

a)复杂的后勤，在 ISMS 范围中涉及不止一处建筑物或地点:;

b)员工所说的语言超过一种（需要翻译或审核员个人无法独立工作)，提供的文件使用了一种以上的语言;

c)为了确认管理体系认证范围内永久场所的活动，需要访问临时场所的活动;d)适用于 ISMS 的标准和法规数量很多;

允许减少审核时间的因素，例如:

a)没有风险或者低风险的产品/过程;

b)过程只涉及单一的常规活动（例如，只有服务);c)在组织控制下工作的雇员大部分是从事相同的任务;

d)对组织已经有些了解（例如，如果组织获得了同一个认证机构的、另一个标准的认证);

e)客户的认证准备情况较好（例如，已经获得了另一个第三方认证方案的认证或承认);

f)高度成熟的管理体系。

在认证客户或被获证组织在临时场所提供其产品或服务时,将对这类场所的评价纳入到认证审核和监督方案中是十分重要的。

宜考虑上述因素，并根据这些因素对审核时间做出调整。这些因素可证实一次有效审核所需更多或更少的审核时间的合理性。增加时间的因素可被减少时间的因素冲抵。在任何情况下，对审核时间表中的时间的调整，应保持足够的证据和记录来证实其变化的合理性。

3.5 对审核时间偏离的限制

为了确保能够实施有效的审核并确保可靠和可比较的结果，对表 B.1 中审核时间的减少，不应超过 30%。

应确定偏离审核时间表的适当理由，并形成文件。B.3.6 现场审核时间策划和编制报告一起所用的时间，通常不宜使总的现场“审核时间”减少到表 B.1 中“总审核时间”的 70%以下。当策划和/或编制报告需要增加时间时，这不应成为减少现场审核时间的理由。审核员旅途时间未计在内，这应在表中所给出的审核时间的基础上另外增加。

注:70%是一个基于 ISMS 审核经验所考虑的系数。

4 监督审核的审核时间

在初次认证审核周期，对一个组织的监督时间宜与初次审核时间成比例，每年用于监督审核的时间总量大约是初次审核时间的 1/3。宜时常评审所策划的监督审核时间，以考虑影响审核时间的变更。为审核 ISMS 的变更[例如,审核新的或发生变更的控制),应增加监督审核的时间。

5 再认证的审核时间

用于再认证审核的全部时间,应取决于本文件的 9.4.3 和 CNAS-CC01 的 9.6.3 所规定的、任何以往审核的结果。再认证审核所需的时间，宜与同一组织的初次认证审核所用的时间成比例，宜至少是同一组织初次认证审核时间的 2/3。

6 多场所的审核时间

应针对每个场所计算每个场所(包括总部）的审核人天数。

可以考虑因部分审核与总部或分场所无关而减少审核时间。认证机构应记录这类减少的合理理由。

附 C(资料性附录)

审核时间计算方法

C.1 总则

本附录为获得一个审核时间计算公式提供了进一步的指南。C.2 给出了一个对因数进行分类的示例，它可用作审核时间计算的基础。C.3 提供了一个审核时间计算的示例。c.2 审核时间计算因数的分类。

如 B.3.4 中 a)-h)所列举的，表 C.1 给出了对主要的审核时间计算因数进行分类的示例。认证机构可以使用该分类来获得一个符合 9.1.4.1 的审核时间计算方案。

表 C.1 审核时间计算因数的分类

对工作量的影响 / 因数（见 B.3.4）	减少工作量	正常工作量	增加工作量
a）ISMS 的复杂性： ● 信息安全要求[保密性、完整性和可用性，(CIA)] ● 关键资产的数量 ● 过程和服务的数量	● 只有少量的敏感信息或保密信息，可用性要求低； ● 很少的关键资产（根据 CIA）； ● 只有一个关键业务过程，该过程的接口和涉及的业务单	● 较高的可用性要求或若干敏感/保密信息； ● 若干关键资产； ● 2-3 个简单的业务过程，这些过程的接口和涉及的业务单元很少	● 比较多的保密信息或敏感信息（例如，健康、个人可识别信息、保险、银行），或可用性要求高； ● 很多关键资产 ● 超过 2 个复杂的过程，这些过程的接

c.3 审核时间计算的示例

以下示例阐述了认证机构如何使用 B.3 中的因数来计算审核时间。该示例中的审核时间计算，是按照以下方法进行的:

第一步:确定与业务和组织相关的(非 IT)因数。识别表 C.2 中每个类别的适宜分值,并对结果求和;

第二步:确定与 IT 环境相关的因数。识别表 C.3 中每个类别的适宜分值，并对结果求和;

第三步:基于以上第一步和第二步的结果，通过选择表 C.4 中的适宜条目，识别这些因数对审核时间的影响;

第四步:最终计算。将由审核时间表（表 B.1）所确定审核人天数乘以第三步中得出的系数。

当利用多场所抽样时，要根据执行多场所抽样计划所需的工作量增加所计算出的审核人天。

d）在 ISMS 各部分的实施过程中，所应用的技术的水平和多样性[例如,不同 IT 平台的数量、隔离网络的数量]；	● 高标准化、低多样性的环境（很少的 IT 平台、服务器、操作系统、数据库、网络等）；	● 标准化且多样性的 IT 平台、服务器、操作系统、数据库和网络；	● 高多样性或复杂的 IT 环境（例如，很多不同的网段、服务器或数据库的类型、关键应用的数量）

e）ISMS 范围内所使用的外包和第三方安排的程度；	● 没有外包且对供应商的依赖较小，或， ● 对外包协议进行了明确的规定、良好的管理与监视； ● 外包方获得了 ISMS 认证； ● 可获得相关的独立担保报告；	● 多个管理不充分的外包协议；	● 高度依赖外包或供应商，它们对重要业务活动有很大影响；或， ● 对外部的数量或程度不清楚； ● 多个未得到管理的外包协议；
f） 信息系统开发的程度；	● 没有内部的系统开发 ● 使用标准化的软件平台	● 使用标准化的、具有复杂配置/参数化的平台； ● （高度）定制软件； ● 若干开发活动（内部的或外包的）	● 大量的内部软件开发活动，有若干针对重大业务目的的、持续进行的项目。
g） 场所的数量和灾难恢复场所的数量；	● 较低的可用性要求，且没有或有一个可选的灾难恢复场所；	● 中等或高的可用性要求，且没有或有一个可选的灾难恢复场所；	● 高可用性要求，例如 7×24 服务； ● 若干个可选的灾难恢复场所； ● 若干个数据中心；
h） 对于监督或再认证审核：符合 CNAS-CC01 8.5.3 条款的、与 ISMS 相关的变更的数量和程度。	● 自上次再认证审核后未发生变化；	● ISMS 的范围或 SoA 有微小的变化，例如，一些策略、文件发生变化； ● 以上因素有微小变化；	● ISMS 的范围或 SoA 有重大变化，例如，新的过程，新的业务单元，风险评估管理方法、策略，文件、风险处置。 ● 以上因素有重大变化；

c.3 审核时间计算的示例

以下示例阐述了认证机构如何使用 B.3 中的因数来计算审核时间。该示例中的审核时间计算，是按照以下方法进行的:

第一步:确定与业务和组织相关的(非 IT)因数。识别表 C.2 中每个类别的适宜分值，并对结果求和;

第二步:确定与 IT 环境相关的因数。识别表 C.3 中每个类别的适宜分值，并对结果求和;

第三步:基于以上第一步和第二步的结果，通过选择表 C.4 中的适宜条目，识别这些因数对审核时间的影响;

第四步:最终计算。将由审核时间表（表 B.1)所确定审核人天数乘以第三步中得出的系数。当利用多场所抽样时，要根据执行多场所抽样计划所需的工作量增加所计算出的审核人天。

这个结果是最终需要调整的审核人天数。

表 C.2 与业务和组织（非 IT）相关的因数

类别	分值
业务类型和法规要求	1. 组织所处的是一个非关键业务领域，且不受管制的领域。[a] 2. 组织的客户处于关键业务领域；[a] 3. 组织处于关键业务领域；[a]
过程与任务	1. 一般的过程，涉及一般的且重复性的任务；大量在组织控制下工作的人员从事相同的任务；很少的产品或服务； 2. 一般的但不重复的过程，涉及大量的产品或服务。 3. 复杂的过程，大量的产品和服务，许多业务单元包含在认证范围内（ISMS 涉及复杂性高的过程，或数量相对较大的活动，或独特的活动）。
管理体系的建立水平	1. 已经很好地建立了 ISMS，和（或）存在其他管理体系； 2. 其他管理体系的要素，有些已经实施，有些没有实施； 3. 根本没有实施其他管理体系，ISMS 是新且没有建立。
a：关键业务领域是可以影响关键公共服务的领域，这些公共服务将引起健康、安全、经济、形象和政府运行能力的风险，从而可能对国家造成非常重大的负面影响。	

表 C.3 与 IT 环境相关的因数

类别	分值
IT 基础设施的复杂程度	1. 很少的或高度标准化的 IT 平台、服务器、操作系统、数据库、网络等； 2. 多个不同的 IT 平台，服务器、操作系统、数据库、网络； 3. 很多不同的 IT 平台、服务器、操作系统、数据库、网络。
对外包和供应商（包括云服务）的依赖程度	1. 很少或不依赖外包或供应商； 2. 有些依赖外包或供应商，这些外包或供应商与某些重要业务活动相关，但不是与所有的重要业务活动相关； 3. 高度依赖外包或供应商，外包或供应商对重要业务活动有着很大影响。
信息系统开发	1. 没有或非常有限的内部系统/应用开发； 2. 有一些服务于某些重要业务目的的、内部的或外包的系统/应用开发； 3. 有大量服务于重要业务目的的、内部的或外包的系统/应用开发。

表 C.4 因数对审核时间的影响

IT 复杂性 / 业务复杂性	低（3-4）	中（5-6）	高（7-9）
高（7-9）	+5%～+20%	+10%～+50%	+20%～+100%
中（5-6）	-5%～-10%	0%	+10%～+50%
低（3-4）	-10%～-30%	-5%～-10%	+5%～+20%

示例 1:

受审核的组织有 700 人，因此根据表 B.1，其初次认证审核需要 17.5 人天。该组织不属于关键业务领域，从事高度标准化和重复性的任务且刚建立 ISMS。根据表 C.2，可以得出与业务和组织相关的因子为 1+1+3=5。该组织具有非常少的 IT 平台和数据库，但大量地使用外包。该组织没有内部的或外包的开发活动。根据表 C.3，可以得出与 IT 环境相关的因子为 1+3+1=5。利用表 C.4，可以得出该审核时间无需调整。

示例 2:

还是示例 1 中的这个组织，但其已有多个管理体系且已较好地建立了 ISMS。根据表 C.2，与业务和组织相关的因子将变为:1+1+1=3。根据表 C.4，将得出需要减少 5%~10%的审核时间，即:审核时间将减少 1 到 1.5 人天，变为 16 到 16.5 人天。

附录 B 信息技术服务管理体系人天计算表

1.确定初次审核的审核时间

认证机构应使用客户的有效人数作为计算初次认证审核时间的基础。在确定审核时间时，认证机构应使用表 1。表 1 是基于每天工作 8 小时的。如果每天工作时间低于或超过 8 小时的，可对该表进行相应调整。

客户的有效人数应根据全职等效人数(FTE)来计算。在计算有效的客户人员时，应基于 SMS 范围内的人员。认证机构应能够证实支持客户 SMS 和服务的有效人数与审核时间之间的关系的合理性。

如果支持 SMS 和服务的客户的有效人数超过了 1175，认证机构计算审核时间的程序应一致地沿用表 1 的递进规律，并通过推断来确定表 1 以外的人天数。
无论客户人员数量是多少，调整后的初次审核时间应不低于 2.5 天。

管理体系认证审核时间不应低于 80%的审核时间。如果策划或编制报告需要额外的时间，这不应减少管理体系认证审核时间。

表 1 客户的有效人数与调整前的审核时间（初次审核）之间的关系

客户的有效人数	审核时间：1 阶段+2 阶段（天）
1 ~ 15	3.5
16 ~ 25	4.5
26 ~ 45	5.5
46 ~ 65	6
66 ~ 85	7
86 ~ 125	8
126 ~ 175	9
176 ~ 275	10
276 ~ 425	11
426 ~ 625	12
626 ~ 875	13
876 ~ 1175	15

注:审核时间是指策划并完成一次完整和有效的客户管理体系审核所需的时间。审核时间包括在客户场所(物理的或虚拟的)现场的所有时间和在非现场进行的策划、文件评审、与客户人员沟通和撰写报告所花费的时间。管理体系认证审核时间是指用于实施一次从首次会到末次会的审核活动所用的那部分审核时间。

有效人数，由认证范围内所涉及的所有人员（包括倒班人员)组成。在认证范围内的人员，还应包括非永久雇员（例如合同工)和兼职人员。根据其所工作的小时数，可减少或增加兼职人数和部分工作包含在认证范围内的员工,并转化为等效的全职员工数量。当大量员工从事重复性的活动或任务时，允许减少认证范围内的员工数量。这种减少要有条理，要根据每个客户的情况进行一致地应用。

2.调整审核时间

应考虑客户 SMS 和服务的所有属性,并根据这些因素对初次审核时间做出调整。该调整可以证明更多或更少的审核时间是合理的。无论考虑了何种调整因素，认证机构应确保分配了充足的审核时间，以完成一次对客户 SMS 完整且有效的审核。认证机构应对审核时间的增加或减少形成文件，并能够说明其合理性。

表 2 和表 3 显示了相关因素是如何影响表 1 中的审核时间。倒班是指在一个连续工作周期内运营的多个地点和（(或)小组之间的工作交接或协同工作。

对表 1 中审核时间的减少不应超过 30%。

表 2 减少审核时间的因素

序号	潜在的减少因素
1	SMS 和服务很少发生变化；
2	以往已证实了 SMS 的有效实施，例如：以前获得了另一家已认可的认证机构的认证；
3	对 SMS 和一个或多个其他相关管理体系进行结合审核；
4	事先已了解组织，例如：组织已获得了同一家认证机构的其他标准的认证；
5	单一的、简单的服务；
6	所有班次实施完全相同的活动，并有适宜证据表明所有班次中具有同等的绩效；如服务台；
7	大部分参与服务管理的人员从事相似的单一职能；
8	人数少的单一场所；
9	对参与服务提供的其他方的依赖程度低，例如供方、内部团体或作为供方的顾客；

表 3 增加审核时间的因素

序号	潜在的增加因素
1	复杂的后勤，包括多重管理、多个工作场所、处于在同一时区或横跨多个时区；
2	不同地点之间语言差异的复杂性，例如员工说一种以上的语言（需要翻译或使得审核员无法独立工作）；
3	SMS 范围大或复杂，例如大量的服务、人员或地点，不易理解和维持的专业化服务；
4	影响客户 SMS 的法律法规要求高，例如：知识产权、隐私、食品、药品、航空、核；
5	不同的班次实施不同的活动；
6	特定审核的 SMS 范围中包含临时场所；
7	SMS 范围内有复杂的业务过程；
8	高度依赖参与服务提供的其他方，例如供方、内部团体或作为供方的顾客；
9	经常有增加新服务、服务移除、服务转换或服务发生重大变更；

3.其他管理体系标准认证对审核时间调整

如果客户通过了其他相关管理体系标准的认证，如 ISO 9001 和（或)ISO/IEC27001，认证机构可以减少初次审核时间。

仅在满足以下条件时，方可根据获得了其他相关管理体系标准的认证而减少审核时间:

a)其他管理体系标准的认证是与所审核的 SMS 相关的;

b）任何现有的证书是有效的,且已认可的认证机构在最近的 12 个月内对其至少实施了一次审

核;

c)其他管理体系标准的认证范围，是等同于或大于 ISO/IEC 20000-1 认证的范围;

审核时间的减少量，应取决于客户服务管理体系与其他管理体系整合的程度。无论客户是获得了何种其他相关管理体系标准的认证,认证机构应确保为对客户 SMS 实施完整有效的审核分配了充足的时间。

注:当同时审核两个或多个不同领域的管理体系时，叫做“结合审核”;当这些管理体系被整合到一个单一的管理体系时，审核的原则和程序与结合审核相同。

4. 确定监督审核和再认证审核的审核时间

在确定实施监督审核和再认证审核所需的时间时，应考虑以下因素:

a)管理体系认证审核时间不低于总审核时间的 80%;

b)年度监督审核，可以是一次审核或多次审核，其审核时间应不少于初次审核的 1/3;

c)再认证审核的审核时间，不应少于初次审核的 2/3;

d)调整后的监督审核时间应不低于 1 天;

e)调整后的再认证审核时间应不低于 2 天。

5.远程审核

审核不是在同一个地点面对面的进行而是在其他地点进行的，叫做远程审核。审核计划中应识别出审核中将使用的远程审核技术。

表 4 描述了使用远程审核时的可接受的和不可接受的做法。认证机构不应使用表 4 中不可接受的做法，可以使用可接受的做法。

远程审核不应将审核时间减少到低于根据表 1 并考虑了适当调整之后所计算出的审核时间。

如果在认证机构制定的审核计划中,远程审核活动所占时间超过了所策划的现场审核时间的 30%时，认证机构应将相应理由形成文件。

表 4 可接受和不可接受的远程审核实践

	可接受
1	电话会议：视频和音频、网络会议、交互式网络通信；
2	远程访问用于支持 SMS 的工具；
3	远程访问 SMS 文件和记录的资料库；
	不可接受
4	仅仅依赖文件；
5	假设所有场所的职能是相同的，但没有支持该假设的证据；
6	实施审核时没有与人员进行面谈；

附录 C 云服务信息安全管理体系人天计算表

LOW RISK Table(低风险表)	
组织是： • 不负责设计开发系统或软件 • 极少的IT基础设施 • 没有行业特定的风险或特定的法律和法规 • 低的信息敏感度（如没有处理客户或公共信息）	
Effective Number of Personnel 有效员工数	Audit days(stage1+stage2) 审核人天（一阶段+二阶段）
1-10	2
11-25	3
26-45	3.5
46-65	4
66-85	4.5
86-125	5.5
126-175	6
176-275	6.5
276-425	7.5
426-625	8
626-875	8.5
876-1175	9.5
1176-1550	10.5
1551-2025	11
2026-2675	12
2676-3450	12.5
3451-4350	13
4351-5450	14
5451-6800	14.5
6801-8500	16
8501-10700	18
>10700	按照以上进阶计算

Mormal RISK Table(正常风险表)	
组织是： • 负责设计开发系统或软件 • 负责IT基础设施管理 • 没有适用的行业特定法律和法规，但是适用行业特定的风险 • 有处理客户的信息	
Effective Number of Personnel 有效员工数	Audit days(stage1+stage2) 审核人天（一阶段+二阶段）
1-10	3
11-25	4
26-45	4.5
46-65	5.5
66-85	6
86-125	7.5
126-175	8
176-275	9
276-425	10
426-625	11
626-875	12
876-1175	13
1176-1550	14
1551-2025	15
2026-2675	16
2676-3450	17
3451-4350	18
4351-5450	19
5451-6800	20
6801-8500	21
8501-10700	22
>10700	按照以上进阶计算

High RISK Table(高风险风险表)	
组织是： • 负责设计开发系统或软件 • 有大量的IT基础设施管理 • 有适用的行业特定法律和法规及适用的行业特定的风险 • 有处理高敏感的信息（如国家安全、犯罪记录等）	
Effective Number of Personnel 有效员工数	Audit days(stage1+stage2) 审核人天（一阶段+二阶段）
1-10	4
11-25	5
26-45	6
46-65	7
66-85	8
86-125	10
126-175	11
176-275	12
276-425	13
426-625	14.5
626-875	16
876-1175	17
1176-1550	18
1551-2025	19.5
2026-2675	21
2676-3450	22
3451-4350	24
4351-5450	25
5451-6800	26
6801-8500	27
8501-10700	29
>10700	按照以上进阶计算

注：云服务信息安全管理体系审核人天的确定，在初次审核、监督审核、再认证审核时的计算方法参照如下要求。

1 初审人天确定标准

基于云服务信息安全管理体系有效员工人数，计算审核需要的人天表（以下简称附表 1）。人天表适用于初审审核人天包括一阶段和二阶段的审核人天的计算。总审核人天包括现场审核人天和非现场审核人天，非现场审核人天工作内容通常包括审核策划和准备审核报告，这些工作可以在非现场完成。二阶段审核应在现场进行，二阶段审核不应少于 1 人天。二阶段以评估客户是否符合 ISO/IEC 27017 标准所有要求。

2 审核人日计算与调整

2.1 员工有效人数

员工有效人数包括:

1） 在认证范围内涉及到的所有全职员工，包括每个班工作的员工。

2）在审核时出现的可等同于全职员工计算的非永久性员工（如季节性员工、临时工和合同工）以及兼职员工。

2.2 审核人日计算的调整因素

审核时间表是基于有效员工数计算审核人天的。应将组织分为三类风险水平：低风险、正常风险和高风险。风险水平依赖的因素如下：

- IT 基础设施的多少
- 管理信息的敏感度
- 行业特定风险
- 行业特定的法律法规
- 有设计职责

下面一个或多个行业 code 会基于 ISMS 认证范围被分配。

- ISMS 01 IT 信息技术
- ISMS 02 银行和金融服务
- ISMS 03 通信
- ISMS 04 医疗保健
- ISMS 05 教育
- ISMS 06 航空
- ISMS 07 所有以上没有规定的其他行业

2.3 调整因素

调整因素可考虑应用于初次审核人天计算，以增加或减少审核时间。需考虑客户的体系、过程、产品和服务特性与复杂程度。按照以上审核人天表，最大减少审核时间不超过 30%。

2.4 判定和记录

审核人天的判定步骤记录在模板“合同评审表”中。

3 监督审核人天

初次认证证书发放后 12 个月内要执行第一次现场监督审核，以后每日历年至少进行一次现场监督审核（再认证审核年除外），以评估认证客户的云服务信息安全管理体系是否持续满足 ISO 27017 标准的要求，但不一定是完整体系审核。

在最初的认证周期中，每年监督审核时间为初审时间的 1 /3。最少的监督审核时间为 1 天。如果每六个月进行一次监督审核，年度监督审核的人天除以 2，小数点后位圆整升到下一整数位。

每一次制定监督审核计划时，组织认证信息如有重大变化，需要提供更新的客户组织信息。

4 再认证审核人天

再认证审核计划应当在第三年进行，保证客户认证的连续性。再认证审核的合同评审应考虑到组织的申请信息（考虑到以往认证周期中发生的所有变化）。审核时间的计算与初次审核相似。再认证审核的人天时间通常是本次认证审核人天计算结果的 2/3，如果上一周期有重大的不符合提出（严重不符合或重复发生的不符合项），认证人天可以增加。

5 转证审核人天

转证审核的目的是评价一个客户是否持续符合 ISO 27017 的所有要求，为客户提供另一个认证机构的认证证书。需要提供云服务信息安全管理体系的有效人数、风险级别、组织认证申请表、并进行转证合同评审、签订认证合同，转证审核时间的计算采用附表 1 中初次审核的认证人天表进行计算。

6.云服务信息安全管理体系的人天涉及多现场时，在初次审核、监督审核、再认证审核时，多现场的抽样方法与人天计算方法参照 14.2.2.1.2 对场所实施现场审核的原则要求。

附录 D 通用数据保护条例管理体系人天计算表

表 1　通用数据保护条例人天计算表

Effective number of personnel	Evaluation time (auditor days)
01-10	5
11-15	6
16-25	7
26-45	8,5
46-65	10
66-85	11
86-125	12
126-175	13
176-275	14
276-425	15
426-625	16,5
626-875	17,5
876-1175	18,5
1176-1550	19,5
1551-2025	21
2026-2675	22
2676-3450	23
3451-4350	24
4351-5450	25
5451-6800	26
6801-8500	27
8501-10700	28
>10700	Same progression as above

注:通用数据保护条例的人天涉及多现场时，在初次审核、再认证审核时，必须覆盖多现场的所有现场。一个认证周期的监督审核方案必须覆盖多现场的所有现场，不需要每个监督审核每年覆盖所有现场。按照所有现场的员工总数计算总审核人天。

审核人天的确定

1.初审人天确定标准

基于通用数据保护条例有效人员，计算审核需要的人天表（以下简称附表 1）。审核人天包括现场审核人天和非现场时间，非现场包括审核策划，文件评审和审核报告的时间。一阶段审核人天通常为整个初审人天的 20%-25%。一、二阶段审核之间的间隔不得超过 6 个月，

即二阶段的第一天审核不应该在一阶段审核结束 180 天之后进行。

2.审核人日计算的调整因素

审核人天的增加或减少需要考虑客户特定的复杂程度(是否多地址、体系、过程、产品和服务)。

3. 监督审核人天

每年至少进行一次现场监督审核。在最初的认证周期中，每年监督审核时间为初审时间的 1/3。最少的监督审核时间为 1 天。如果每六个月进行一次监督审核，年度监督审核的人天除以 2。每一次制定监督审核计划时，需要考虑更新的客户组织信息。

4.再认证审核人天

再认证审核/策划应当在证书到期日前三个月安排。再认证审核的合同评审应考虑到组织的简介信息(考虑到以往认证周期中发生的所有变化)。再认证审核的人天时间需要重新计算，通常为初次认证的 2/ 3。如果上一周期有显著的不符合提出(严重不符合或显著的不符合项)，认证人天可以增加。

5.转证审核人天

转证审核的目的是评价一个客户是否持续符合 GDRP 的所有要求，为客户提供另一个认证机构的认证证书。转证审核时间及过程按照 KBRZ 程序安排。

附录 E 公有云个人信息安全管理体系人天计算表

LOW RISK Table(低风险表)	
组织是： • 不负责设计开发系统或软件 • 极少的IT基础设施 • 没有行业特定的风险或特定的法律和法规 • 低的信息敏感度（如没有处理客户或公共信息）	
Effective Number of Personnel 有效员工数	Audit days(stage1+stage2) 审核人天（一阶段+二阶段）
1-10	2
11-25	3
26-45	3.5
46-65	4
66-85	4.5
86-125	5.5
126-175	6
176-275	6.5
276-425	7.5
426-625	8
626-875	8.5
876-1175	9.5
1176-1550	10.5
1551-2025	11
2026-2675	12
2676-3450	12.5
3451-4350	13
4351-5450	14
5451-6800	14.5
6801-8500	16
8501-10700	18
>10700	按照以上进阶计算

Mormal RISK Table(正常风险表)	
组织是： • 负责设计开发系统或软件 • 负责IT基础设施管理 • 没有适用的行业特定法律和法规，但是适用行业特定的风险 • 有处理客户的信息	
Effective Number of Personnel 有效员工数	Audit days(stage1+stage2) 审核人天（一阶段+二阶段）
1-10	3
11-25	4
26-45	4.5
46-65	5.5
66-85	6
86-125	7.5
126-175	8
176-275	9
276-425	10
426-625	11
626-875	12
876-1175	13
1176-1550	14
1551-2025	15
2026-2675	16
2676-3450	17
3451-4350	18
4351-5450	19
5451-6800	20
6801-8500	21
8501-10700	22
>10700	按照以上进阶计算

High RISK Table(高风险风险表)	
组织是： • 负责设计开发系统或软件 • 有大量的IT基础设施管理 • 有适用的行业特定法律和法规及适用的行业特定的风险 • 有处理高敏感的信息（如国家安全、犯罪记录等）	
Effective Number of Personnel 有效员工数	Audit days(stage1+stage2) 审核人天（一阶段+二阶段）
1-10	4
11-25	5
26-45	6
46-65	7
66-85	8
86-125	10
126-175	11
176-275	12
276-425	13
426-625	14.5
626-875	16
876-1175	17
1176-1550	18
1551-2025	19.5
2026-2675	21
2676-3450	22
3451-4350	24
4351-5450	25
5451-6800	26
6801-8500	27
8501-10700	29
>10700	按照以上进阶计算

注：公有云个人信息安全管理体系审核人天的确定，在初次审核、监督审核、再认证审核时的计算方法参照如下要求。

1 初审人天确定标准

基于公有云个人信息安全管理体系有效员工人数，计算审核需要的人天表（以下简称附表 1）。人天表适用于初审审核人天包括一阶段和二阶段的审核人天的计算。总审核人天包括现场审核人天和非现场审核人天，非现场审核人天工作内容通常包括审核策划和准备审核报告，这些工作可以在非现场完成。二阶段审核应在现场进行，二阶段审核不应少于 1 人天。二阶段以评估客户是否符合 GB/T 41574-2022 标准所有要求。

2 审核人日计算与调整

2.1 员工有效人数

员工有效人数包括:

1） 在认证范围内涉及到的所有全职员工，包括每个班工作的员工。

2)在审核时出现的可等同于全职员工计算的非永久性员工（如季节性员工、临时工和合同工）以及兼职员工。

2.2 审核人日计算的调整因素

审核时间表是基于有效员工数计算审核人天的。应将组织分为三类风险水平：低风险、正常风险和高风险。风险水平依赖的因素如下：

- IT 基础设施的多少
- 管理信息的敏感度
- 行业特定风险
- 行业特定的法律法规
- 有设计职责

下面一个或多个行业 code 会基于 ISMS 认证范围被分配。

- ISMS 01 IT 信息技术
- ISMS 02 银行和金融服务
- ISMS 03 通信
- ISMS 04 医疗保健
- ISMS 05 教育
- ISMS 06 航空
- ISMS 07 所有以上没有规定的其他行业

2.3 调整因素

调整因素可考虑应用于初次审核人天计算，以增加或减少审核时间。需考虑客户的体系、过程、产品和服务特性与复杂程度。按照以上审核人天表，最大减少审核时间不超过 30%。

2.4 判定和记录

审核人天的判定步骤记录在模板“合同评审表”中。

3 监督审核人天

初次认证证书发放后 12 个月内要执行第一次现场监督审核，以后每日历年至少进行一次现场监督审核（再认证审核年除外），以评估认证客户的公有云个人信息安全管理体系是否持续满足 GB/T 41574-2022 标准的要求，但不一定是完整体系审核。

在最初的认证周期中，每年监督审核时间为初审时间的 1 /3。最少的监督审核时间为 1 天。如果每六个月进行一次监督审核，年度监督审核的人天除以 2，小数点后位圆整升到下一整数位。

每一次制定监督审核计划时，组织认证信息如有重大变化，需要提供更新的客户组织信息。

4 再认证审核人天

再认证审核计划应当在第三年进行，保证客户认证的连续性。再认证审核的合同评审应考虑到组织的申请信息（考虑到以往认证周期中发生的所有变化）。审核时间的计算与初次审核相似。再认证审核的人天时间通常是本次认证审核人天计算结果的 2/3，如果上一周期有重大的不符合提出（严重不符合或重复发生的不符合项），认证人天可以增加。

5 转证审核人天

转证审核的目的是评价一个客户是否持续符合 GB/T 41574-2022 的所有要求，为客户提供另一个认证机构的认证证书。需要提供公有云个人信息安全管理体系的有效人数、风险级别、组织认证申请表、并进行转证合同评审、签订认证合同，转证审核时间的计算采用附表 1 中初次审核的认证人天表进行计算。

6.公有云个人信息安全管理体系的人天涉及多现场时，在初次审核、监督审核、再认证审核时，多现场的抽样方法与人天计算方法参照 14.2.2.1.2 对场所实施现场审核的原则要求。

附录 F 隐私信息安全管理体系人天计算表

审核人日数的确定

1. 审核人日数的确定标准

审核时间确定基于隐私信息安全管理体系有效员工人数，计算审核的人日数

- 每个产品的特定规则
- 客户现场和流程的复杂性

Effective number of personnel	A - ISO 27001 or ISO 27701 Evaluation time (auditor days)	B - IS
0		
01-10	5	
11-15	6	
16-25	7	
26-45	8,5	
46-65	10	
66-85	11	
86-125	12	
126-175	13	
176-275	14	
276-425	15	
426-625	16,5	
626-875	17,5	
876-1175	18,5	
1176-1550	19,5	

2. 审核人日数的计算与调整

2.1 员工有效人数:

- 涉及认证范围的所有专职人员，包括所有班次的人员。
- 全职人员在轮班和/或重复或类似过程中工作（信息安全的最终用户控件）
- 部分时间的兼职人员和员工
- 以季节性/工作量为基础的工人

雇员的有效人数应根据以下考虑因素计算:

人员类别	采用的方法	有效人数估算
所有班次的员工=全职及管理人员	这些人主要负责政策制定，战略决策，管理和治理信息安全控制和全面控制管理系统实施情况和有效性。通常是高层管理人员，过程负责人/部门负责人。	100%
所有班次的全职人员，从事重复或相似过程(用户信息安全控制的终端用户)	这种人员采取轮班制，从事的过程和操作是相似且连续的。 最终用户通常会包括那些在监督下工作，参与技术活动，执行类似的＆重复性任务，例如软件开发，测试， 等，使用信息安全的最终用户控制，没有任何决策权。这个人手可能是流动岗位人员或根据涉及的工作量来指定的。	人数平方根， 四舍五入到更高的整数。
兼职人员 雇员 部分范围	取决于工作时间，兼职人员人数和部分雇员 可能会减少或增加并转化为同等数量的专职人员。（例如 30 名每天工作 4 小时的兼职人员相当于 15 个全职人员）。	人数/8 小时数/实际小时 结果数字四舍五入到下一个 视为的最高整数 1 FTE(基于 100%)。
季节性/基于工作量工人	这些是工作量或季节性工人在高峰时期受雇于某些行业（例如为特定项目租用的资源 能力，基于交付的紧迫性项目等)。 这些可能会或可能不会轮班在审核当天可能不可用。因此，根据部署周期，采用 50%的系数。	季节/项目总数 人 x 他们的月数 雇用/ 12 x 50%。 以 100%为基础的 1 FTE。

示例:对于拥有 500 名员工的软件开发组织，人力的分工为:

• 管理人员 - 50

• 软件开发人员和测试人员-400

• 共用人力资源，他们也为不在范围内的其他项目工作 - 50 人，每天 3 个小时因此，计算的工时将基于:

100%的管理人员+做重复性工作（开发人员和测试人员）的人力平方根+FTE 那将是 50 + √400+(((50X3)/ 8)= 70 + 19 =89。要分配审核人天为 12。对于 ISO 27701（公司已通过 ISO 27001 认证）的扩展，额外时间将为两天（2)。

2.1 单一现场组织

所有轮班在组织控制下工作的总人数是确定审核时间的起始点。

在组织控制下从事工作的兼职人员增加了在组织控制下工作的人数，与全职员工相比，组织的控制与工作时间成比例，这一决定应取决于与全职相比的工作小时数。

在偏远地区工作的员工（如在家工作）应被视为总部人数。为 DC/DR 等无人值守现场增加 0.5 人天。

2.2 多现场组织

所有现场的过程必须基本相同，并且必须按照类似的方法程序操作。如果考虑其中的一些现场执行类似的操作，但过程比其他现场少，则它们可能是有资格加入多现场认证方案的，但是前提这些现场是进行大多数过程的关键场所。

所有流程都要经过全面审核。

在不同地点通过关联流程开展业务的组织也有资格进行抽样（如果全部）满足本文件的其他规定。如果每个位置的流程不相似，但有明确的关联，则抽样计划应至少包括组织实施的每个过程的一个示例（例如，设计/开发软件在一个位置，其他支持在多个其他位置)。
组织的管理体系应在一个集中控制和管理的计划之下，并服从中央管理评审。所有相关场所(包括中央管理职能）应遵守本组织的内部审核计划，并且所有内部审核都应在认证机构审核之前按照该计划进行审核。

应证明组织的中央办公室以及整个组织都能满足审核的相关管理体系标准。这应包括对相关法规的考虑。组织应证明其有收集和分析数据（包括但不限于下列项目)的能力。
所有网站，包括中央办公室及其权威，并展示其权威性和发起组织变革的能力如果需要:

- 系统文件和系统变更；
- 管理评审；
- 事件；
- 纠正措施评估；
- 内部审核计划和结果评估；
- 风险管理
- 不同的法律要求。

并非所有符合多现场组织定义的组织都有资格进行抽样，例如:

- 所有现场执行显著不同的活动；
- 客户要求对每个现场进行审核；
- 有一个行业计划或监管要求，规定每个现场都要进行系统审核。

2.3 审核时间计算表

审核时间图作为根据有效员工人数计算审核持续时间的起点。

Column B 仅适用于已经通过 ISO 27001 认证并获得 KBRZ 认证的公司。ISO 27001 认证范围应至少涵盖 ISO 27701 认证范围。

在所有其他情况下，应使用 A 列。

分配的时间还考虑到以下因素，这些因素与 PIM 的复杂性有关，因此也与工作有关，需要审核 PIM:

a) PIMS 的复杂性（如信息的关键性、PIMS 的风险状况等)；

b) 在 PIMS 范围内开展的业务类型；

c) 先前证明 PIMS 的性能；

d) 实施 PIMS 各组成部分所用技术的范围和多样性（例如不同 IT 平台、隔离网络的数量)；

e) PIMS 范围内使用的外包和第三方安排的程度；

f) 信息系统开发程度；

g) 现场数量和灾难恢复（DR）现场数量；

符合资格标准的组织可以由可取样的场地、不能取样的场地或两者的结合。审核时间必须足以进行有效的审核。

每个抽样地点的审核时间减少不得超过 50%。

例如，30%是 IAF MD 5 允许的最大审核时间减少，而 20%则被视为最大减少由中央职能部门执行的单一管理体系过程和任何潜在的集中化流程（如采购)。如果使用翻译器，则增加 20%。不能对列 B 进行人天减少。

2.4 调整因素

2.5 增加审核时间:

需要额外审核时间的其他因素包括:

• 涉及 PIMS 范围内多个建筑物或地点的复杂物流；

• 会说一种以上语言的工作人员（需要翻译或阻止个别审核员工作）或以一种以上语言提供的文件；

• 需要访问临时现场以确认其管理的永久现场的活动系统须经认证；

• 处理敏感的个人数据

• 行业或处理高敏感度的额外或异常数据保护方面或监管条件信息（例如国家安全、犯罪记录等)

2.6 缩短审核时间:

允许缩短审核时间的其他因素包括:

• 无/低风险产品/流程；

• 涉及单一一般活动的过程（例如仅服务)；

• 在组织控制下从事相同任务的人比例很高；

• 客户对认证的高度准备（例如，已经通过另一个第三方计划认证或认可)；

• 不负责系统/软件的设计和开发

• 不是面向 B 到 C

• 仅限国内/本地业务（没有与个人身份信息/隐私相关的若干规定)

• 经主管当局批准的行为准则或公司约束性规则；

6.隐私信息安全管理体系的人天涉及多现场时，在初次审核、监督审核、再认证审核时，多现场的抽样方法与人天计算方法参照 14.2.2.1.2 对场所实施现场审核的原则要求。