北京质信认证有限公司

隐私信息安全管理体系
认证实施规则

版 本：A/1

编 号：BQC-GZ-012

编 写：技术部

审 核：王　雷

批 准：杨小涛

发布日期：2023 年 10 月 31 日　　实施日期：2023 年 10 月 31 日　　修改日期：2025 年 8 月 18 日

目 录

1 适用范围

本规则用于规范北京质信认证有限公司（简称 BQC）开展隐私安全管理体系认证活动。

2 认证依据

以国际标准 ISO/IEC 27701:2019《安全技术 隐私信息管理对 ISO/IEC 27001 和 ISO/IEC 27002 的扩展要求和指导方针》为认证依据。

3 术语和定义

3.1 现场审核

BQC 指派审核组到受审核方或获证组织所在办公地点进行管理体系运行的符合性进行审核。

3.2 申请组织/受审核方/获证组织

申请组织：向公司提出认证申请的组织

受审核方：当公司受理后，对申请组织的称呼变更为“受审核方”。

获证组织：当受审核方取得公司证书后，称呼变更为“获证组织”。

4 认证审核类型

认证审核类型分为初次认证，监督审核和再认证。

5 审核人员及审核组要求

认证审核人员必须取得其他管理系注册审核员资格或者取得隐私信息安全管理体系审核员资格（如有相关注册或确认制度），经 BQC 进行能力评价确认后，认为其能够胜任所安排的审核任务。

6 审核组要求

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。

具有与管理体系相关的管理和法规等方面特定知识的技术专家可以成为审核组成员。

技术专家可就受审核方或获证组织管理体系中技术充分性事宜为审核员提供技术支持和指导，但技术专家不能作为审核员独立审核。

7 认证程序

7.1 初次认证

7.1.1 认证申请

BQC 应要求申请组织至少提供以下必要的信息：

a) 认证申请书；

b) 法律地位资格证明，包括但不限于：工商营业执照；事业单位法人证书或社会团体法人登记证书；组织代码证；税务登记证等；

c) 取得相关法规规定的行政许可文件(适用时)；

d) 管理体系所必要的文件；

e) 产品及过程符合国家相关法律法规和标准要求的证据（必要时）；

f) 无未处理结束的重大与拟申请认证领域相关的责任事故；

g) 未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未被列入“严重违法企业名单”；

注意事项：被其他机构暂停、撤销认证证书的申请组织，需在暂停、撤销满一年后，我机构方可受理认证申请。

7.1.2 申请评审

BQC 针对申请组织提交的认证申请书，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：

h) 符合申请组织的行业类别和管理体系要求的文件化管理体系；

i) 申请组织生产/从事的产品/活动符合相关法律、法规的规定；

j) 体系运行满三个月，且至少进行过一次管理体系内部审核与管理评审（标准有要求时），覆盖申请范围内所有的产品、过程、场所。

k) 符合国家及行业对申请组织相应行业的特殊管理要求；

l) BQC 与申请组织之间任何已知的理解差异得到消除；

m) BQC 有能力并能够实施认证活动；

申请组织所提供的资料和信息应确信足以建立审核方案；

评审通过后，双方签订《管理体系认证合同》。

7.1.3 建立审核方案

在申请评审通过后，BQC 应针对申请组织建立审核方案。

审核方案范围与程度的确定应基于受审核组织的规模和性质，以及受审核管理体系的性质、功能、复杂程度以及成熟度水平有关。

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）审核的范围，审核的内容和界限，如审核场所、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（如覆盖不同场所的审核）时，单次审核的范围可以不覆盖整个范围，但整个审核覆盖的范围要与认证文件的范围一致；

2）审核准则和其他规范性文件，客户有效的管理体系过程和文件要求；

3）审核方法、审核时机、审核频次、审核时间；

4）审核组的选择；

5）所需的资源，包括交通和食宿；

6）处理保密性、信息安全、健康和安全，以及其它类似事宜。

7.1.4 确定审核组

BQC 应根据受审核方的行业、规模和业务复杂程度组建审核组，指派审核组长。审核组组建原则见第 5 章。

7.1.5 文件审查

审核组应在第一阶段审核之前进行文件审查，用以评价受审核方提供资料的充分性、适宜性。

由审核组对受审核方提交的文件化的管理体系进行审核，出具《文件审查报告》，并将《文件审查报告》反馈给受审核方。

文件审核需关注以下内容：

- 组织所提交的文件化管理体系是否覆盖了标准要求；
- 受审核方所建立的管理体系应符合组织所在行业相关法律、法规及标准要求，与产品、服务及活动类型相适应。
- 描述业务开展所需的主要过程及关系文件。

当文件审查结果确信不影响现场审核时，才能安排现场审核。

7.1.6 一阶段审核

审核组应对受审核方开展一阶段审核，以了解组织对审核准备的状态，为策划第二阶段审核提供关注要点，确定是否具备进入二阶段审核的条件。

一阶段审核计划应在一阶段审核前，提交受审核方确认。

一阶段审核应关注以下内容：

（1）结合现场情况，确认申请组织实际情况与管理体系成文信息描述的一致性，特别是体系成文信息中描述的产品和服务、部门设置和职责与权限、生产或服务过程等是否与申请组织的实际情况相一致；

（2）结合现场情况，审核申请组织有关人员理解和实施标准要求的情况，评价管理体系运行过程中是否实施了内部审核与管理评审（标准有要求时），确认管理体系是否已有效运行并且超过 3 个月；

（3）确认申请组织建立的管理体系覆盖的活动内容和范围、申请组织的员工人数、活动过程和场所，遵守相关法律法规及技术标准的情况；

（4）结合管理体系覆盖活动的特点识别对目标的实现具有重要影响的关键点，并结合其他因素，科学确定审核关注点；

（5）与申请组织讨论确定第二阶段审核安排。

一阶段审核可分为非现场审核或现场审核，非现场审核的条件参照认监委和公司相关文件要求执行，一阶段审核可包括对文件审核的进一步确认。

在第一阶段审核中，如发现组织存在违反审核依据的情况，审核组应该填写《一阶段审核问题清单》。在问题清单中问题没有得到有效处理前，不得进行第二阶段审核。

一阶段审核结束前，审核组将与受审核方进行沟通，通报第一阶段审核结论，出《一阶段审核报告》。

7.1.7 二阶段现场审核计划

审核组应结合受审核方的申请材料、审核方案以及文件审核结果、一阶段审核的结果对现场审核做出具体二阶段计划安排。

一二阶段审核时间间隔不宜超过 6 个月，超过该期限的，BQC 应调整审核方案。

制定审核计划应考虑受审核方申请认证范围内的产品、过程和职能部门，并覆盖标准所有条款。

如果管理体系覆盖范围包括在多个场所进行相同或相近的活动，且这些场所都处于申请组织授权和控制下，可以在审核中对这些场所进行抽样，但应根据相关要求实施抽样以确保对所抽样本进行的审核对管理体系包含的所有场所具有代表性。如果不同场所的活动存在明显差异、或不同场所间存在可能对管理有显著影响的区域性因素，则不能采用抽样审核的方法，应当逐一到各现场进行审核。

第二阶段审核计划应至少包括以下内容：

●具体的时间安排

●审核组成员及分工

●对受审核方职能/岗位/场所的具体审核安排

审核计划应至少在实施现场审核前交受审核方确认，并与受审核方就审核计划进行充分沟通，确保双方在理解上没有歧义。

7.1.8 二阶段现场审核

审核组按照审核计划的安排对受审核方进行现场审核。

二阶段现场审核应考虑一阶段审核结果，对受审核方的管理过程和控制措施的运行情况进行评价。

现场审核依据认证标准的要求进行，收集、评价客观证据。

内容可包括但不限于：

a) 组织环境；

b) 领导；

c）策划；

d) 支持；

e) 运行；

f）绩效评估；

g) 改进。

7.1.9 初次认证的审核结论

审核组应该对现场审核中收集的所有信息和证据进行汇总分析，评价审核发现并就审核结论达成一致。

如果现场审核发现不符合项和观察项应开具不符合项报告，不符合事实应得到受审核方的认可。现场审核结束，审核组应形成是否推荐认证注册的结论。

现场审核结束后，审核组长完成审核报告编制工作，BQC 将与受审核方进行沟通，确保双方对报告的理解上没有歧义。

7.1.10 认证决定

认证决定人员负责对受审核方的认证申请及认证过程的符合性和有效性进行评定，根据评定结果做出以下决定：

a）同意认证注册，颁发认证证书；

b）补充认证决定所需的信息，包括但不限于申请材料、审核材料，再行决定；

c）不同意认证注册，并将理由通知受审核方。

认证决定人员实施认证决定时应以认证过程中收集的信息和其他相关信息为基础，以充分的证据证实受审核方建立管理体系得到了建立、实施、运行、监视、评审、保持和改进。

注 1：参加审核的人员不能再作为认证决定人员实施认证决定。

注 2：受审核方获得认证注册资格后变更为获证组织。

7.1.11 审核方案记录与变更

审核方案管理人员应收集现场审核和认证决定的信息，特别是形成的结论和变化的信息，记录到审核方案中，并确定审核方案是否需要进行变更，如需要则更新相应项目内容。

7.2 监督审核

7.2.1 监督频次

认证证书有效期通常为三年，证书有效期内，BQC 需对获证组织进行两次监督审核。

第一次监督审核自初次认证二阶段审核结束日期/再认证审核结束日期后的 8-12 个月内进行；

第二次监督审核在第一次监督审核后 12 个月内进行；适当时，第二次监督最长可延长到第一次监督审核后的 15 个月内进行。

当获证组织管理体系发生重大变更，或发生重大问题、业务中断事故、客户投诉等情况时，BQC 可视情况增加监督的频次。

认证证书有效期内的两次监督审核必须覆盖管理体系认证范围内的所有业务活动。

由于获证组织业务运作的时间(季节)特点及其内部审核安排等原因，可以合理选取和安排监督周期及时机。

7.2.2 监督信息收集

在进行监督审核之前，BQC 需要收集获证组织的管理体系相关信息，以确定获证组织的管理体系相关信息是否发生变化。需确认的信息包括单不限于以下几个方面：

a. 基本信息，包括组织名称、地址、联系人、法人等信息的变化情况；

b. 组织信息：包括范围、组织架构、人员数量等信息的变化情况；

c. 管理体系相关信息，关键文件化信息的变化情况。

申请评审人员及审核组应该对变化信息进行确认，以确定是否需修订审核方案。

7.2.3 监督审核要求

单次监督审核可不覆盖标准所有条款，安排监督审核条款时，应以下列原则进行：

1) 对过程控制有决定作用的条款每次监督审核都必须审核；

2) 上次审核问题较多的条款在本次监督审核中需实施审核；

监督审核的内容可包括以下方面：

1) 内部审核和管理评审（标准有要求时）；

2) 对上次审核中确定的不符合采取的措施（标准有要求时）；

3) 投诉的情况及处理（标准有要求时）；

4) 管理体系在实现目标和各管理体系的预期结果方面的有效性；

5) 为持续改进而策划的活动的进展；

6) 持续的运作控制；

7) 任何变更；

8) 标志的使用和（或）任何其他对认证资格的引用

由于监督审核并不要求覆盖体系的所有方面，因此在监督审核的策划过程中，如果获证组织的认证范围信息有变化，应对变化的方面进行关注，必要时重新确认审核范围。

7.2.4 监督审核结论

审核组应该对现场审核中收集的所有信息和证据进行汇总分析，评价审核发现并就审核结论达成一致。

现场审核发现不符合项和观察项应开具不符合项报告，且获得获证组织认同。

当两次审核均不能覆盖认证范围内所有产品/服务时，可根据监督审核结果，做出保持、暂停、撤销认证证书和缩小认证范围的决定。

7.2.5 认证决定

BQC 认证决定人员对获证组织的监督审核实施认证决定，以决定：

a．同意保持认证注册，颁发认证标志；

b．补充认证决定所需的信息，包括但不限于申请材料、审核材料，再行决定；

c．不同意保持认证注册，做出暂定或撤销的决定，并将理由通知获证组织。

认证决定人员实施认证决定时应以认证过程中收集的信息和其他相关信息为基础，以充分的证据证实获证组织建立管理体系得到了建立、实施、运行、监视、评审、保持和改进。

7.2.6 审核方案记录与变更

审核方案管理人员应收集变更信息、现场审核和认证决定的信息，特别是形成的结论和变化的信息，同时记录到审核方案中。 并确定审核方案是否需要进行变更，如需要则更新相应项目内容。

7.3 再认证

认证证书有效期满前，BQC 根据获证组织的申请对获证组织实施再认证，以保证管理体系认证证书持续有效。再认证审核的形式和过程与初次认证保持一致，但再认证的一阶段审核可以与二阶段审核一起进行，但当获证组织或其管理体系的运作环境（如法律的变更）有重大变更时，再认证审核活动可能需要有单独的第一阶段审核。

再认证审核将包括针对下列方面的现场审核

1) 上个认证周期内管理体系的有效性，以及认证范围的持续相关性和适宜性；

2) 经证实的对保持管理体系有效性并改进管理体系，以提高整体绩效的承诺；

3) 管理体系在实现获证客户的目标和管理体系预期结果方面的有效性。

7.4 管理体系结合审核

当申请组织在运行隐私信息安全管理体系的同时还运行了其他管理体系，若其他管理体系在 BQC 的认证业务范围内，BQC 可以根据申请组织的需求对管理体系进行单独的审核，或者对多个管理体系进行结合审核，但 BQC 需确保在结合审核的情形下，对诸如审核范围的界定、审核时间的确定、审核方案的策划等进行有效的管理。

对于结合审核，必须以审核活动满足体系认证所有要求为前提，并且审核的质量不应由于结合审核而受到负面影响。在审核报告中，应清晰体现所有与管理体系有关的重要要

素的描述并易于识别。

7.5. 特殊审核

7.5.1 变更或扩大认证范围

获证组织申请变更或扩大认证范围时，BQC 申请评审人员应针对变更信息进行评审，做出是否同意变更或扩大认证注册范围的决定。变更或扩大认证范围的审核活动可单独进行，也可和对获证组织的监督审核或再认证同时进行。

7.5.2 BQC 在调查投诉、对变更做出回应或对被暂停认证资格的获证组织进行追踪时，应指派审核组提前较短时间通知获证组织后对其进行特殊审核。特殊审核以现场审核方式进行，同时应向获证组织明示实施特殊审核的缘由，应根据审核结论作出认证决定。

7.5.3 审核方案记录与变更

审核方案管理人员应收集特殊审核的信息，特别是形成的结论和变化的信息，并记录到审核方案中。同时确定审核方案是否需要进行变更，如需要则更新相应项目内容。

7.6 暂停、撤消认证或缩小认证范围

7.6.1 BQC 制定暂停、撤消认证或缩小管理体系认证范围的政策和形成文件的规定，并按规定实施。

7.6.2.发生以下情况(但不限于)时，BQC 应暂停获证组织的管理体系认证资格：

a.获证组织的管理体系持续地或严重地不满足认证要求，包括对管理体系有效性的要求；

b.获证组织不允许按要求的频次实施监督或再认证审核，不承担、履行认证合同约定的责任和义务的；

c.获证组织不接受或不配合认证认可监督管理部门的监督管理；或被有关执法监管部门责令停业整顿的。

d.持有的与管理体系范围有关的行政许可证明、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。

e.获证组织主动请求暂停或其他应当暂停认证证书的。

7.6.3.认证资格暂停期最长不超过 6 个月。

7.6.4.在暂停认证期间，获证组织的管理体系认证证书暂时无效。BQC 以书面的形式告知获证组织证书暂停信息。

7.6.5.如果获证组织未能在 BQC 规定的时限内解决造成暂停认证的问题，BQC 应撤消其管理体系认证或缩小其相应的认证范围，BQC 以书面的形式告知获证组织证书的撤销或缩小认证范围的信息。

7.6.6.如果获证组织在认证范围的某些部分持续地或严重地不满足认证要求，BQC 应缩小其管理体系认证范围，以排除不满足要求的部分。认证范围的缩小应与认证标准的要求一致。

7.6.7 在相关方提出请求时，BQC 应正确说明获证组织的管理体系认证被暂停、撤消或缩小的情况。

7.6.8 获证组织有以下情形之一的，技术部应在获得相关信息并调查核实后 5 个工作日内撤销其认证证书。

（1）被注销或撤销法律地位证明文件的。

（2）被国家质量监督检验检疫总局列入质量信用严重失信企业名单。

（3）拒绝配合认证监管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。

（4）拒绝接受国家产品质量监督抽查的。

（5）出现重大的产品和服务等质量安全事故，经执法监管部门确认是获证组织违规造成的。

（6）有其他严重违反法律法规行为的。

（7）暂停认证证书的期限已满但导致暂停的问题未得到解决或纠正的（包括持有的与质量管理体系范围有关的行政许可证明、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）。

（8）没有运行管理体系或者已不具备运行条件的。

（9）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，或者认证机构已要求其纠正但超过 2 个月仍未纠正的。

（10）其他应当撤销认证证书的。

7.6.9 撤销认证证书后，市场部应及时收回撤销的认证证书。若无法收回，技术部及时在相关媒体和网站上公布或声明撤销决定。

7.6.10 暂停或撤销认证证书，公司在官方网站上公布相关信息，同时按规定报国家认监委。

7.6.11 证书恢复的办理

7.6.11.1 如果造成暂停的问题已解决，应恢复被暂停的认证证书。根据不同的暂停原因，本着“谁办理谁跟踪”的原则，暂停恢复应由暂停提出部门办理。

a. 由技术部提出暂停的，其恢复由技术部提出，需要安排现场审核的，待审核结束现场审核资料交回后，技术部认证决定通过，管理者代表审批，予以恢复。

b. 对因欠费暂停的，获证组织在规定的时间内缴费的，由市场部直接办理恢复手续；

c. 对因资质过期等原因暂停的，获证组织上交有效资质后，由市场部直接办理恢复手续；

d. 除本条 a、b、c 外的，由审核部安排审核组长现场确认是否具备恢复条件。如具备，由审核组长告知技术部，由技术部办理恢复手续。

e. 综合部负责制作和发放“恢复认证证书和标志通知书”并将证书状态变更情况上报认监委。

7.6.11.2 暂停提出部门和综合部要与认证暂停客户保持信息沟通、联系，了解该客户采取纠正措施进展的动态情况，以便对暂停的恢复做出及时安排。

8 认证证书

8.1 证书内容

8.1.1 认证证书内容应以中文书写，至少包括以下方面：

（1）认证证书名称；

（2）证书编号；

（3）获证组织名称、注册地址、获证地址和邮政编码；

（4）符合本规则 2 项的认证依据；

（5）通过认证的业务范围/类别；

（6）发证日期、证书有效期、换证日期等相关日期；

（7）BQC 的名称及其标志；

（8）BQC 的印章和法定代表人代表或其授权人的签字；

（9） 认可标识及认可注册号(获得 CNAS 认可时适用)；

8.1.2 如果认证所覆盖业务(或服务)的类别及其所涉及的过程和覆盖的场所较多，需在证书附件上加以注明。

8.2 证书编号

8.2.1 对同一个受审核方实施的同一个管理体系认证，赋予一个认证证书编号。

8.2.2 证书编号规则由 BQC 确定。

8.2.3 同一个组织的认证范围覆盖多个场所并需要颁发子证书时，在子认证证书编号后加上“-”和序号，如-1(-2，-3，…)。

8.2.4 有效期内换发证书，认证证书编号中的机构注册号、年份号、顺序号和认证的有效期保持不变，应注明换证日期。

8.2.5 撤销证书后，原认证证书编号废止，废号不得占用。

8.2.6 认证证书上的 BQC 名称应与相应的 BQC 批准书上的名称一致。

8.3 对获证组织正确宣传认证结果的控制

BQC 应采取授权使用标识的方式来要求获证组织在认证结果的宣传和使用中采用本规则确定的认证依据，同时注明通过认证的业务类别和认证证书编号。

在认证证书被暂停期间或撤销后，应收回相应的授权。

9 信息通报及响应

为确保获证组织的管理体系持续有效，BQC 应向获证组织传达建立信息通报的机制，及时向 BQC 通报以下信息：

（1）业务、地点、组织机构变化等情况的信息(及时通报)；

（2）顾客投诉的相关信息；

（3）组织的体系文件和业务重大变化时进行通报；

（4）触发了紧急中断事件(及时通报)；

（5）其他重要信息。(视情况通报)

BQC 应对上述信息以及收集到的相关公共信息进行分析，视情况采取相应措施，包括增加监督审核频次以及暂停或撤销认证资格的措施等。

在发生重大客户投诉等严重情况时,BQC 需立即采取相应处理措施。

10 本规则未尽事宜，参照认监委及公司相关文件的规定执行。

附录 A：审核人日

下表为初次认证的审核人日基数，具体审核时间需要考虑受审核方的规模、特性、业务复杂程度、认证范围、认证要求和其承担的风险等因素。根据受审核方的特点在项目方案制定过程中可以在人日基数上进行增减。

审核人日包括所有审核阶段、现场审核的总时间以及）），以及在现场以外实施策划、文件审查、与客户人员之间的相互活动和编写报告等活动的时间。

当与其他管理体系结合审核时，审核时间可根据结合审核的其他管理体系的特点进行减少。

监督审核的人日数约为初次认证人日数的三分之一，再认证的人日数约为初次认证人日数的三分之二，上述原则仅限于获证组织的认证范围和组织规模未发生变化的情况。

基本人日数计算表

<table>
<tr><th>有效人数</th><th>初次审核时间（人日）</th><th>有效人数</th><th>初次审核时间（人日）</th></tr>
<tr><td>1-5</td><td rowspan="6">2</td><td>876-1175</td><td rowspan="2">6</td></tr>
<tr><td>6-10</td><td>1176-1550</td></tr>
<tr><td>11-15</td><td>1551-2025</td><td rowspan="2">7</td></tr>
<tr><td>16-25</td><td>2026-3450</td></tr>
<tr><td>26-45</td><td>3451-4350</td><td rowspan="2">8</td></tr>
<tr><td>46-65</td><td>4351-5450</td></tr>
</table>

66-85	3	>5450	遵循上述递进规律
86-125			
126-175	4		
176-275			
276-425	5		
426-875			