方圆标志认证集团
China Quality Mark Certification Group

数据安全风险管理认证实施方案

文件编号：CQMS-FN-27-026

发布日期：2021 年 10 月 27 日

修订日期：

实施日期：2021 年 10 月 27 日

CHINA
QUALITY MARK

目　　录

数据安全风险管理认证实施方案

1 适用范围

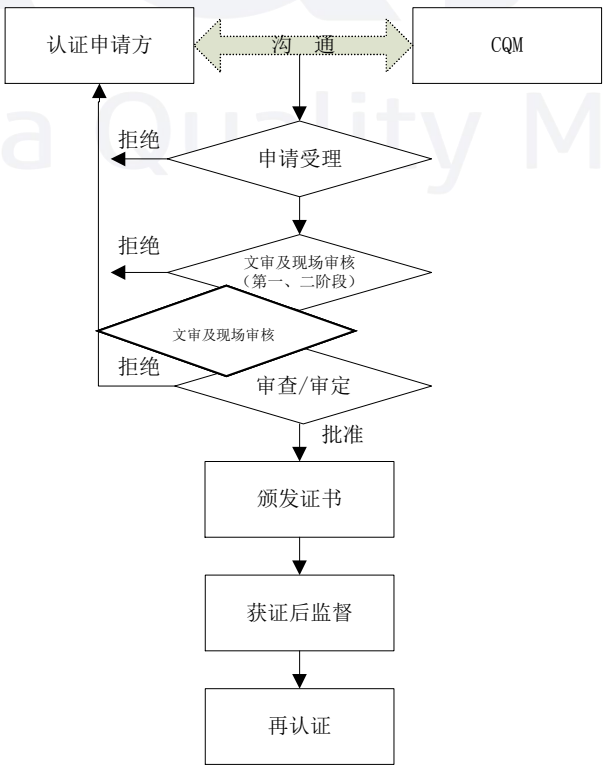
本认证方案适用于方圆标志认证集团有限公司（以下简称：CQM）实施数据安全风险管理认证，满足第三方认证制度要求，作为提供认证服务的规范。必要时，在认证合同中补充相关的技术要求。

本认证方案在认证双方签订合同时予以确认和采用。

2 认证模式

CQM 首先对受审核方的数据安全风险管理进行初次审核，经过评定，确认是否批准认证；通过认证之后，在认证证书的有效期内对获证客户进行监督，确认是否持续满足认证要求。

3 认证过程流程图



4 认证申请

4.1 认证申请的基本条件

a) 认证客户具有明确的法律地位,客户具有企业营业执照、事业单位法人证书、社会团体登记证书、非企业法人登记证书等，可独立申请认证。其他类型的客户，应由具备资格的单位代为申请；

b) 国家、地方或行业有要求时，认证客户具有规定的行政许可文件,其申请认证范围应在法律地位文件和行政许可文件核准的范围内；

c) 认证客户承诺遵守国家的法律、法规及其他要求,承诺始终遵守认证的有关规定，承担与认证有关的法律责任，并有义务协助认证监管部门的监督检查，对有关事项的询问和调查如实提供相关材料和信息；

d) 认证客户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”；

e) 近一年内通过数据安全风险评估检测并提供检测报告；

f) 认证客户承诺获得 CQM 认证后,按规定使用认证证书和认证标志和有关信息，不得擅自利用数据安全风险管理认证证书的文字、符号误导公众认为其产品或服务通过认证按合同支付认证费用，并按规定接受监督；

g) 认证客户承诺获得 CQM 认证后，按照 CQM 要求向 CQM 通报数据安全风险管理变更的信息和其他可能影响数据安全风险管理持续满足认证标准要求的能力的事宜的信息，一般包括：客户及相关方有重大投诉；发生重大事故；相关情况发生变更（包括：法律地位、生产经营状况、组织状态或所有权变更、强制性认证或其他资质证书变更；法定代表人、最高管理者、管理者代表发生变更；生产经营或服务的工作场所变更；数据安全风险管理覆盖的活动范围变更；数据安全风险管理和重要过程的重大变更等）；出现影响数据安全风险管理运行的其他重要情况；

h) 认证审核期间，认证客户能够提供与拟认证范围相关的活动或过程。

4.2 不予受理认证申请的情形

a) 认证客户申请的认证范围超出法律地位文件和行政认可文件核准的范围内的；

b) 认证客户不满足 4.1 中其他相关要求或近一年内发生其他违反国家法律法规、行业规定的情形。

5 审核实施

5.1 审核准则

认证双方确认的审核依据标准如下：

CQM/S-RZ-ZY-21-001《数据安全风险管理 要求》

审核准则还包括受审核方所适用的方针、程序、标准、法律法规、数据安全风险管理相关要求、合同要求或行业规范。

上述标准更新时，使用更新版本。

5.2 审核过程

5.2.1 初次认证审核

初次认证审核目的是评价认证组织的数据安全风险管理实施情况，审核组通过收集客观证据，综合评价认证组织是否符合标准要求及相关要求，运行是否有效。

初次认证审核具体关注：

a) 受审核方规定的数据安全风险管理过程的有效性和控制方法；

b) 自我评估和自我改进实施情况等。

5.2.2 监督活动

5.2.2.1 监督活动的方式

监督活动包括监督审核与日常监控。监督审核的主要内容：

a) 自上次审核以来与组织数据安全风险管理有关的重要变更（如资源、过程、组织结构、已识别的关键控制点等）；

b) 持续的运作控制数据安全管理目标的实现情况；

c) 对上次审核中提出问题的改进情况的验证；

d) 自我评估和自我改进实施情况等。

5.2.2.3 监督审核的频次

在证书有效期内，获证客户须接受监督审核，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。初审/再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。

获证客户因未在规定的时间内实施监督审核而暂停认证证书的，监督审核恢

复后，下次审核时间应按原计划时间计算。

5.2.3 再认证

再认证审核的主要内容：

a） 上一认证周期组织数据安全风险管理的持续有效性；

b） 数据安全风险管理有关的重要变更对数据安全风险管理的影响；

c） 数据安全风险管理目标的实现情况；

d） 对上次审核中提出问题的改进情况的验证；

自我评估和自我改进实施情况等。

5.3 现场审核活动实施

审核组在现场审核前与受审核方沟通，确认审核安排，说明首末次会议议程。

审核组按照审核计划中日程安排实施审核，通过查阅受审核方的文件和记录、与过程和活动的岗位人员面谈、座谈、观察产品、服务形成过程和活动等适当方法，抽样收集并验证有关的信息，形成审核发现，确认不符合情况。

在审核过程中，审核组及时与受审核方沟通，通报审核进程，确认审核证据，解决分歧。当审核发现表明不能达到审核目的时，应说明理由，商定后续措施。如果需要改变审核目的和范围或终止审核时，应经审核派出机构评审和批准后实施。

审核组长在现场审核结束前，与受审核方沟通现场审核的信息，审核组编制审核报告并提交受审核方。

审核报告属 CQM 所有，如果在审核后续活动中（含 CQM 进行认证决定期间）有所更改，CQM 将重新向受审核方提供审核报告。请受审核方妥善保管审核报告等相应材料。

6 认证的批准、拒绝、保持、扩大、缩小、暂停、恢复和撤销的条件和程序

6.1 批准认证范围的条件和程序

6.1.1 批准认证注册的条件

a） 认证客户的申请材料真实、准确、有效；

b） 认证客户申请认证范围在法律地位文件和资质规定的范围内；认证客户在认证申请范围覆盖的经营活动不存在重大风险；

c）国家或地方或行业有要求时，认证客户申请认证范围内的组织单元、产品、服务及其过程和活动已满足适用的法律法规的要求；

d）审核中发现的不合格在规定期限内已经采取纠正/纠正措施，经 CQM 验证有效。

e）至少近一年来，认证客户申请认证范围内未发生失信行为或国家检查不合格；

f）认证客户已与方圆签署认证合同，承诺始终遵守认证的有关规定，并按照认证合同规定缴纳认证费用。

6.1.2 批准认证资格的程序

a）CQM 向认证客户提供认证有关信息的公开文件，使其知悉并理解；

b）认证客户向 CQM 正式提交认证申请书和相关附件；

c）CQM 根据客户申请信息进行申请评审，并已确认受理认证申请；

d）满足 6.1.1 批准认证资格的条件，经 CQM 审定，认为认证客户在认证范围内已满足批准认证资格的条件，同意批准认证；

e）CQM 向认证客户颁发认证证书，要求获证方按规定使用认证标志。

6.2 拒绝认证注册的条件和程序

6.2.1 拒绝认证资格的条件

a）认证客户信息未通过 CQM 的申请评审，评审为不予受理认证申请；

b）认证客户的数据安全风险管理有重大缺陷，不符合认证标准的要求，CQM 审核组现场审核结论为“不推荐认证注册”；

c）认证客户的数据安全风险管理有重大缺陷，不符合认证标准的要求，CQM 的审定结论为不予认证注册。

6.2.2 拒绝认证注册的程序

a）符合 6.2.1 条件之一，经 CQM 评审为不予受理认证或认证客户的数据安全风险管理不满足批准认证资格条件；

b）CQM 向认证客户发出《不予认证注册通知》。

6.3 保持认证资格的条件和程序

6.3.1 保持认证资格的条件

a）获证客户的法律地位、行政许可文件持续符合国家的最新要求，并且认证

范围在法律地位文件和行政许可文件规定的范围内；

b）获证客户持续遵守认证有关的规定，包括变更的规定；

c）获证客户在认证范围内的组织过程和活动持续满足适用的最新法律法规的要求，如发生不满足时及时采取有效的措施；

d）获证客户于获证期内，认证范围内涉及的过程或活动未发生重大事故和国家检查不合格；

e）获证客户在获证期间未发生误用认证证书和认证标志，如有发生能及时有效地采取纠正和纠正措施，并将误用产生的影响降至最小程度；

f）获证客户对顾客或相关方的重大投诉和关切能及时有效地处理；

g）获证客户能按照 CQM 要求及时通报重要过程变更等信息；

h）按时接受监督审核，经现场审核获证客户的数据安全风险管理持续符合认证标准/规范性文件要求，审核组结论为“保持认证”；

i）获证客户履行与 CQM 签署认证合同中规定的责任和义务，并按照认证合同规定缴纳认证费用。

6.3.2 保持认证资格的程序

a）满足 6.3.1 保持认证资格的条件，监督审核后，经 CQM 派出的审核组长确认和 CQM 审查后认为获证客户在认证范围内能持续满足保持认证资格的条件，同意保持认证资格，由 CQM 签发确认证书并向获证客户发放；

b）在认证证书有效期内如有认证要求变更，获证客户接受变更的认证要求，并经 CQM 验证在认证范围内数据安全风险管理满足变更的要求，可保持认证资格。

6.6 变更认证信息的条件和程序

6.6.1 变更认证信息的条件和分类

6.6.1.1 变更认证信息的条件

在认证证书有效期内，获证客户因信息发生变更，导致与认证证书信息不一致时，应予以更新。

6.6.1.2 变更认证信息的分类

a）获证客户名称、住所变更；

b）认证地址变更；

c）地名变更；

d）证书范围中的过程或活动的变更。

6.6.2 变更认证信息的程序

6.6.2.1 认证信息的变更需提交的资料

6.6.2.1.1 获证客户名称、住所变更应提交的资料

a） 获证客户的书面变更申请；

b） 获证客户是企业的，提供工商行政主管部门的变更核准证明及新营业执照复印件；其他性质的获证客户提供允许其设立的政府行政主管部门的相关文件；

c） 对于因改制、企业重组引起的名称变更，获证客户不能获得名称变更核准证明时，应提交组织以原名称和现名称名义的更名申请、政府有关部门的批文和原名称注销证明；并需因数据安全风险管理发生重大变更接受 CQM 的一次监督审核和审定；

d） 有行政许可、资质等要求的获证客户，还应提供按新名称变更后的有关文件。

6.6.2.1.2 认证地址变更需要提交的资料

a） 获证客户的书面变更申请；

b） 有行政许可、资质等要求的获证客户，还应提供按新地址变更后的法规要求的有关文件。

6.6.2.1.3 地名变更需要提交的资料

a） 获证客户的书面变更申请；

b） 当地政府的相关证明；

c） 对有行政许可、资质等要求的获证客户，还应提供按新地址变更后的有关文件。

6.6.2.1.4 证书范围中的过程或活动的变更需要提交的资料

a） 获证客户的书面变更申请；

b） 对有行政许可、资质等要求的认证范围，还应提供相应文件复印件。

6.6.2.2 认证信息变更的办理流程

a） 获证客户根据 6.6.1 要求向 CQM 正式提交满足 6.6.2.1 要求的申请和相关

文件资料；

b）需要时，获证客户应接受 CQM 的审核；

c）经 CQM 审定，认为获证客户满足认证信息变更的条件，同意批准认证信息变更；

d）CQM 收回原认证证书，换发认证证书或附件，认证证书的有效期保持不变。

6.7 暂停认证资格的条件和程序

6.7.1 暂停认证资格的条件

符合下列条件之一的获证客户，CQM 将暂停其认证证书：

——获证客户数据安全风险管理持续或严重不满足认证要求。

a） 获证客户的数据安全风险管理生重大变更，不能持续符合认证标准/规范性文件要求；

b） 获证客户监督审核期间发生严重影响体系运行的情况；

c） 获证客户在认证范围内的过程和活动不能满足适用的最新法律法规和标准的要求，并未采取措施或措施无效；

d） 获证客户未按照认证要求的变更做出相应调整，或调整不满足变更要求；

——获证客户不承担、履行认证合同约定的责任和义务。

a） 获证客户未能在规定的期限内接受监督或再认证审核；

b） 获证客户未履行与 CQM 签署认证合同中规定的责任和义务，并对保持认证资格产生重大影响；

c） 获证客户未按照认证合同规定缴纳认证费用；

d） 获证客户在获证期间发生误用认证证书和认证标志，并未能及时有效地采取纠正和纠正措施，以将产生的影响降至最少程度。

——获证客户在证书有效期间受到相关执法监管部门处罚。

a） 获证客户未按要求对信息进行通报。

——获证客户被地方认证监管部门发现体系运行存在问题。

a） 获证客户于获证期间在认证范围内发生国家抽检不合格，并未查明原因和采取补救措施。

——获证客户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。

a） 获证客户的法律地位、资质不再符合国家的最新要求；

b） 获证客户的认证范围已不在现行有效的法律地位文件和资质规定的范围内，但仍有可能在短期内符合规定要求。

——获证客户主动请求暂停。

——获证客户发生了与违反国家法律法规的重大事故，反映出获证客户的体系建立及运行存在重大缺陷。

a） 获证客户于获证期间在认证范围内发生重大事故被媒体曝光、或未查明原因和采取补救措施；

——其他原因需要暂停证书。

6.7.2 暂停认证资格的程序

a） CQM 提出对获证客户暂停全部或部分认证范围内认证资格的建议，并提供理由和证据,或由获证客户向 CQM 提出暂停认证资格的申请；

b） 必要时，CQM 与获证客户沟通，核实证据；

c） 经 CQM 审定，认为获证客户在认证范围内全部或部分不再持续满足认证要求，但仍然有可能在短期内采取纠正措施的，同意批准暂停全部或部分认证范围的认证资格，并确定暂停期限，向获证客户颁发《认证处置决定通知书》并公告；

d） 获证客户按照《管理体系认证证书和认证标志、认可标识使用规则》停止使用认证证书和认证标志，在暂停期间，客户的数据安全风险管理认证暂时无效。

6.8 恢复认证资格的条件和程序

6.8.1 恢复认证资格的条件

获证客户已针对暂停认证资格的原因采取了有效的纠正措施，产生原因已经消除，认证资格的恢复符合相关的认证要求，同时已证实在暂停期内没有使用、引用认证资格（如广告宣传）和使用认证标志。

6.8.2 恢复认证资格的程序

a） 在确定的认证资格暂停限期结束前，根据暂停原因，获证客户在规定期限内向 CQM 提出恢复认证资格的《恢复使用认证证书和认证标志的申请书》；

b） 需要时，获证客户应提交相关纠正措施和有效性验证材料；

c）经 CQM 审定，确认获证客户在暂停认证资格的认证范围内已恢复符合相关的认证要求，作出同意恢复认证资格的结论，颁发《恢复使用认证证书和标志的通知》并公告。

6.9 撤销认证资格的条件和程序

6.9.1 撤销认证资格的条件

符合下列条件之一的获证客户，CQM 将撤销其认证证书：

——获证客户审核未通过。

——获证客户被注销或撤销法律地位证明文件。

——获证客户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。

a）被国家行政主管部门列入信用严重失信企业名单。

——被相关政府主管部门认定存在严重违法失信行为的。

——获证客户出现重大事故，经执法监管部门确认是获证客户违规造成。

a）获证客户于获证期间在认证范围内发生国家抽检不合格，并造成严重影响。

b）拒绝接受国家行政主管部门监督抽查的。

——获证客户在证书有效期间有其他严重违反法律法规行为，受到相关执法监管部门处罚。

——获证客户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（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）。

——获证客户没有运行数据安全风险管理要求或者已不具备运行条件。

——获证客户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。

——获证客户因换发新证而撤销旧证书。

——获证客户不承担、履行认证合同约定的责任和义务。

——获证客户主动放弃认证。

——其他原因需要撤销证书。

6.9.2 撤销认证资格的程序

经 CQM 核实与审定，确认获证客户在认证范围内的管理体系不再满足认证要求，作出撤销认证资格的结论，发放《认证处置决定通知书》并公告，收回认证证书，认证客户不得再使用认证证书和认证标志。

7 认证证书

7.1 认证证书

数据安全风险管理认证证书有效期为 3 年；通常情况下，获证客户应在当前认证证书截止期前至少 3 个月接受再认证审核或已做好接受再认证审核的准备。否则，因获证客户接受再认证审核时间过晚或因不符合的关闭导致 CQM 的认证决定无法在原认证证书到期前作出时，再认证证书有效期将不足 3 年。

7.2 认证证书的使用

获证客户应建立认证证书的使用方案，获证后按照《管理体系认证证书、标志标识使用规则》正确使用认证证书。

7.3 认证证书的误用

获证客户误用认证证书，可能导致认证资格的暂停或撤销，具体见《管理体系认证证书、标志标识使用规则》中规定。

获证客户一旦发现误用认证证书或认证标志，应立即采取纠正措施，并报告方圆审核管理部门。

8 获证客户的信息通报

获证客户应建立向方圆通报最新信息的程序，并及时通报其重大投诉、国家监督检查结果、重大事故及获证客户变更的各种信息等。变更信息包括（但不限于）以下：

a) 组织名称，组织法人，隶属关系；

b) 联系人，联系方式(包括：电话、传真、手机)；

c) 组织地址(包括：注册地址、认证地址)；

d) 体系覆盖人数；

e) 认证范围变化；

f） 组织机构和职能分配；

g） 证书表述的组织认证场所。

当上述信息发生变更时，获证客户应填写《获证组织认证信息变更沟通单》，并及时反馈给 CQM。变更信息反馈渠道及联系信息详见《获证组织认证信息变更沟通单》中的联系。

9 认证要求变更的条件和程序

9.1 认证要求变更的条件

a） 获证客户保持认证资格有效；

b） 认证要求变更应在规定的时间前完成；

c） 申请认证要求变更的获证客户应提交认证要求变更需求申请，并提交按新的认证要求进行体系调整的证据；

d） 获证客户的体系已满足新的认证要求，且已正常运行。

9.2 认证要求变更的程序

a） 在认证要求变更转换期结束前，获证客户向 CQM 提出认证要求变更申请；提出申请日期宜在转换期截止前至少 90 天；

b） CQM 通过对获证客户实施年度监督审核或再认证审核，或应获证客户要求安排的认证要求变更的专项审核，评审调整后的数据安全风险管理对认证要求的符合性、适宜性和有效性；

c） 经 CQM 审定，认为获证客户已满足批准认证资格的条件，同意批准认证范围，换发认证证书或附件，收回原证书，认证证书的注册号和有效期保持不变。

10 保密

CQM 承诺为认证客户保密（提前告知认证客户的需公开信息除外）。对认证客户的保密信息如需公开或向第三方提供时，将拟提供的信息提前通知认证客户（法律限制除外）。

如有证据表明，CQM 因认证接触受审核方的商业、技术秘密，而泄露给第三者（法律规定除外），承担相应法律责任。

11 申诉/投诉、争议及处理

对 CQM 或审核人员违反国家认证法律、法规、认可机构有关规定、缺乏公正性及对认证的评价结果等有异议时，可以向 CQM 提出申诉、投诉。

CQM 将在 30 日内答复处理情况。

对 CQM 申诉/投诉和争议的处理有异议时可向中国合格评定国家认可委员会、中国国家认证认可监督管理委员会等有关部门进一步申诉/投诉。

12 费用

实施本方案的费用，按《数据安全风险管理认证收费管理规则》执行。

13 公告

对获得认证、暂停、恢复或撤销的认证客户，在 CQM 网站上公布。

14 附则

本方案由方圆标志认证集团有限公司负责解释。